ITUPublications

Cloud computing: From paradigm to operation


NEWS
sms
02
NEWS
sms
+1
02
NEWS

Foreword

Cloud services provide on-demand access to advanced ICT resources, enabling innovators to gain new capabilities without investing in new hardware or software. Cloud concepts are also fundamental to the evolution of ICT networking, helping networks to meet the requirements of an increasingly diverse range of ICT applications.

As innovation accelerates in fields such as IMT-2020/5G and the Internet of Things and digital transformation takes hold in every industry sector, the cloud ecosystem will continue to grow in importance to companies large and small, in developing as well as developed countries.

ITU standards provide the requirements and functional architectures of the cloud ecosystem, covering inter- and intra-cloud computing and technologies supporting 'XaaS' (X as a Service).

These standards enable consistent end-to-end, multi-cloud management and the monitoring of services across different service providers' domains and technologies – they were developed in view of the convergence of telecoms and computing technologies that characterizes the cloud ecosystem.

Recent years have seen software coming to play a key role in network management and orchestration. Concepts rooted in datacentre networking are transforming telecoms operations, with notable examples found in software-defined networking and network function virtualization.

This convergence of telecoms and computing technology is in full flight, with our networks coming to depend heavily on cloud and very modern computing, transport and datacentre technologies.

Our networks are transforming to become agile all-round players able to perform a wide array of specialized functions. Cloud is central to this agility, enabling the automated provisioning of virtualized resources to meet the needs of any ICT application.

ITU standards are supporting industry in navigating this transformation. This compendium of ITU cloud standards will provide ICT industry players with a valuable point of reference as they transform networking operations to take full advantage of cloud capabilities.

Chaesub Lee
Director
ITU Telecommunication Standardization Bureau

Introduction

As stated in Recommendation ITU-T Y.3500, the cloud computing is a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with on-demand self-service provisioning and administration. Users have quick access to such resources as for example hardware and software platforms or applications in the context of the different cloud deployment models as public, private and hybrid. Furthermore, investments in own hardware and software are reduced, in particular, when considering their rapid changes because of high pace of innovations. Aside from cost savings and promoting innovation, the integration of cloud computing changes architecture and management of telecommunication networks. Cloud computing is considered to be one of the key capabilities of currently deploying IMT2020/ 5G networks.

ITU-T has been developing Recommendations on cloud computing since 2011.

Given that cloud computing is based on the concurrence of a variety of resources of telecommunication networks and IT infrastructure, ITU-T standards enabling consistent end-to-end, multi-cloud management and monitoring of services exposed by and across different service providers' domains and technologies have been and are still published. ITU-T Study Group 13 (SG13) has published to this day 24 ITU-T standards related to cloud computing. In addition, other 14 cloud computing standards have been published by other ITU-T Study Groups. Such standards, which have to some extend been jointly developed with other SDO's such as ISO/IEC JTC 1/SC 38/WG 3, focus in detail on, inter alia, requirements and functional architectures of the cloud computing ecosystem, covering inter- and intra-cloud computing and technologies supporting XaaS (X as a Service). This work includes infrastructure and networking aspects of cloud computing models, as well as deployment considerations and requirements for interoperability and data portability. Furthermore, studies orient toward cloud service and infrastructure management as well as the management of composite cloud services and components that use a variety of telecom and IT infrastructure resources.

This flipbook offers a detailed overview on today's ITU-T deliveries related to cloud computing. It aims to give an introduction and guidance for the understanding of cloud computing concepts, eco system and principles.

1 November 2019

Dr Leo Lehmann, Chairman for ITU-T Study Group 13 "Future networks, with focus on IMT-2020, cloud computing and trusted network infrastructures"

Table of Contents

Cloud computing: From paradigm to operation

1.

Framework and requirements for cloud computing

Information technology – Cloud computing – Overview and vocabulary

Rec. ITU-T Y.3500 (2014) | ISO/IEC 17788:2014

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Summary

This Recommendation | International Standard provides an overview of cloud computing, and defines related terms.

The terms and definitions provided in this Recommendation | International Standard:

– cover commonly used terms and definitions in cloud computing standards;

– will not cover all terms and definitions used in cloud computing standards; and

– do not preclude the definition of additional terms for use in cloud computing standards.

Table of Contents

1 Scope

This Recommendation | International Standard provides an overview of cloud computing along with a set of terms and definitions. It is a terminology foundation for cloud computing standards.

This Recommendation | International Standard is applicable to all types of organizations (e.g., commercial enterprises, government agencies, not-for-profit organizations).

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

2.1 Identical Recommendations | International Standards

None.

2.2 Paired Recommendations | International Standards

None.

2.3 Additional references

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation | International Standard uses the following terms defined elsewhere.

The following terms are defined in ISO/IEC 27000:

3.1.1 **availability**: Property of being accessible and usable upon demand by an authorized entity.

3.1.2 **confidentiality**: Property that information is not made available or disclosed to unauthorized individuals, entities, or processes

3.1.3 **information security**: Preservation of **confidentiality** (3.1.2), **integrity** (3.1.4) and **availability** (3.1.1) of information.

NOTE – In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

3.1.4 **integrity**: Property of accuracy and completeness.

The following term is defined in Rec. ITU-T Y.101:

3.1.5 **interoperability**: The ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged.

The following term is defined in ISO/IEC 27729:

3.1.6 **party**: Natural person or legal person, whether or not incorporated, or a group of either.

The following term is defined in ISO/IEC 20000-1:

3.1.7 service level agreement (SLA): Documented agreement between the service provider and customer that identifies services and service targets.

NOTE 1 – A service level agreement can also be established between the service provider and a supplier, an internal group or a customer acting as a supplier.

NOTE 2 – A service level agreement can be included in a contract or another type of documented agreement.

3.2 Terms defined in this Recommendation | International Standard

For the purposes of this Recommendation | International Standard, the following definitions apply:

3.2.1 application capabilities type: **Cloud capabilities type** (3.2.4) in which the **cloud service customer** (3.2.11) can use the **cloud service provider's** (3.2.15) applications.

3.2.2 cloud application portability: Ability to migrate an application from one **cloud service** (3.2.8) to another **cloud service** (3.2.8).

3.2.3 cloud auditor: **Cloud service partner** (3.2.14) with the responsibility to conduct an audit of the provision and use of **cloud services** (3.2.8).

3.2.4 cloud capabilities type: Classification of the functionality provided by a **cloud service** (3.2.8) to the **cloud service customer** (3.2.11), based on resources used.

NOTE – The **cloud capabilities types** are **application capabilities type** (3.2.1), **infrastructure capabilities type** (3.2.25) and **platform capabilities type** (3.2.31).

3.2.5 cloud computing: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

3.2.6 cloud data portability: **Data portability** (3.2.21) from one **cloud service** (3.2.8) to another **cloud service** (3.2.8).

3.2.7 cloud deployment model: Way in which **cloud computing** (3.2.5) can be organized based on the control and sharing of physical or virtual resources.

NOTE – The **cloud deployment models** include **community cloud** (3.2.19), **hybrid cloud** (3.2.23), **private cloud** (3.2.32) and **public cloud** (3.2.33).

3.2.8 cloud service: One or more capabilities offered via **cloud computing** (3.2.5) invoked using a defined interface.

3.2.9 cloud service broker: **Cloud service partner** (3.2.14) that negotiates relationships between **cloud service customers** (3.2.11) and **cloud service providers** (3.2.15).

3.2.10 cloud service category: Group of **cloud services** (3.2.8) that possess some common set of qualities.

NOTE – A **cloud service category** can include capabilities from one or more **cloud capabilities types** (3.2.4).

3.2.11 cloud service customer: **Party** (3.1.6) which is in a business relationship for the purpose of using **cloud services** (3.2.8).

NOTE – A business relationship does not necessarily imply financial agreements.

3.2.12 cloud service customer data: Class of data objects under the control, by legal or other reasons, of the **cloud service customer** (3.2.11) that were input to the **cloud service** (3.2.8), or resulted from exercising the capabilities of the **cloud service** (3.2.8) by or on behalf of the **cloud service customer** (3.2.11) via the published interface of the **cloud service** (3.2.8).

NOTE 1 – An example of legal controls is copyright.

NOTE 2 – It may be that the **cloud service** (3.2.8) contains or operates on data that is not **cloud service customer data**; this might be data made available by the **cloud service providers** (3.2.15), or obtained from another source, or it might be publicly available data. However, any output data produced by the actions of the **cloud service customer** (3.2.11) using the capabilities of the **cloud service** (3.2.8) on this data is likely to be **cloud service customer data** (3.2.12), following the general principles of copyright, unless there are specific provisions in the **cloud service** (3.2.8) agreement to the contrary.

3.2.13 cloud service derived data: Class of data objects under **cloud service provider** (3.2.15) control that are derived as a result of interaction with the **cloud service** (3.2.8) by the **cloud service customer** (3.2.11).

NOTE – **Cloud service derived data** includes log data containing records of who used the service, at what times, which functions, types of data involved and so on. It can also include information about the numbers of authorized users and their identities. It can also include any configuration or customization data, where the **cloud service** (3.2.8) has such configuration and customization capabilities.

3.2.14 cloud service partner: **Party** (3.1.6) which is engaged in support of, or auxiliary to, activities of either the **cloud service provider** (3.2.15) or the **cloud service customer** (3.2.11), or both.

3.2.15 cloud service provider: **Party** (3.1.6) which makes **cloud services** (3.2.8) available.

3.2.16 cloud service provider data: Class of data objects, specific to the operation of the **cloud service** (3.2.8), under the control of the **cloud service provider** (3.2.15).

NOTE – **Cloud service provider data** includes but is not limited to resource configuration and utilization information, **cloud service** (3.2.8) specific virtual machine, storage and network resource allocations, overall data centre configuration and utilization, physical and virtual resource failure rates, operational costs and so on.

3.2.17 cloud service user: Natural person, or entity acting on their behalf, associated with a **cloud service customer** (3.2.11) that uses **cloud services** (3.2.8).

NOTE – Examples of such entities include devices and applications.

3.2.18 Communications as a Service (CaaS): **Cloud service category** (3.2.10) in which the capability provided to the **cloud service customer** (3.2.11) is real time interaction and collaboration.

NOTE – **CaaS** can provide both **application capabilities type** (3.2.1) and **platform capabilities type** (3.2.31).

3.2.19 community cloud: **Cloud deployment model** (3.2.7) where **cloud services** (3.2.8) exclusively support and are shared by a specific collection of **cloud service customers** (3.2.11) who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection.

3.2.20 Compute as a Service (CompaaS): **Cloud service category** (3.2.10) in which the capabilities provided to the **cloud service customer** (3.2.11) are the provision and use of processing resources needed to deploy and run software.

NOTE – To run some software, capabilities other than processing resources may be needed.

3.2.21 data portability: Ability to easily transfer data from one system to another without being required to re-enter data.

NOTE – It is the ease of moving the data that is the essence here. This might be achieved by the source system supplying the data in exactly the format that is accepted by the target system. But even if the formats do not match, the transformation between them may be simple and straightforward to achieve with commonly available tools. On the other hand, a process of printing out the data and rekeying it for the target system could not be described as "easy".

3.2.22 Data Storage as a Service (DSaaS): **Cloud service category** (3.2.10) in which the capability provided to the **cloud service customer** (3.2.11) is the provision and use of data storage and related capabilities.

NOTE – **DSaaS** can provide any of the three **cloud capabilities types** (3.2.4).

3.2.23 hybrid cloud: **Cloud deployment model** (3.2.7) using at least two different **cloud deployment models** (3.2.7).

3.2.24 Infrastructure as a Service (IaaS): **Cloud service category** (3.2.10) in which the **cloud capabilities type** (3.2.4) provided to the **cloud service customer** (3.2.11) is an **infrastructure capabilities type** (3.2.25).

NOTE – The **cloud service customer** (3.2.11) does not manage or control the underlying physical and virtual resources, but does have control over operating systems, storage, and deployed applications that use the physical and virtual resources. The **cloud service customer** (3.2.11) may also have limited ability to control certain networking components (e.g., host firewalls).

3.2.25 infrastructure capabilities type: **Cloud capabilities type** (3.2.4) in which the **cloud service customer** (3.2.11) can provision and use processing, storage or networking resources.

3.2.26 measured service: Metered delivery of **cloud services** (3.2.8) such that usage can be monitored, controlled, reported and billed.

3.2.27 multi-tenancy: Allocation of physical or virtual resources such that multiple **tenants** (3.2.37) and their computations and data are isolated from and inaccessible to one another.

3.2.28 Network as a Service (NaaS): **Cloud service category** (3.2.10) in which the capability provided to the **cloud service customer** (3.2.11) is transport connectivity and related network capabilities.

NOTE – **NaaS** can provide any of the three **cloud capabilities types** (3.2.4).

3.2.29 on-demand self-service: Feature where a **cloud service customer** (3.2.11) can provision computing capabilities, as needed, automatically or with minimal interaction with the **cloud service provider** (3.2.15).

3.2.30 Platform as a Service (PaaS): **Cloud service category** (3.2.10) in which the **cloud capabilities type** (3.2.4) provided to the **cloud service customer** (3.2.11) is a **platform capabilities type** (3.2.31).

3.2.31 platform capabilities type: **Cloud capabilities type** (3.2.4) in which the **cloud service customer** (3.2.11) can deploy, manage and run customer-created or customer-acquired applications using one or more programming languages and one or more execution environments supported by the **cloud service provider** (3.2.15).

3.2.32 private cloud: **Cloud deployment model** (3.2.7) where **cloud services** (3.2.8) are used exclusively by a single **cloud service customer** (3.2.11) and resources are controlled by that **cloud service customer** (3.2.11).

3.2.33 public cloud: **Cloud deployment model** (3.2.7) where **cloud services** (3.2.8) are potentially available to any **cloud service customer** (3.2.11) and resources are controlled by the **cloud service provider** (3.2.15).

3.2.34 resource pooling: Aggregation of a **cloud service provider's** (3.2.15) physical or virtual resources to serve one or more **cloud service customers** (3.2.11).

3.2.35 reversibility: Process for **cloud service customers** (3.2.11) to retrieve their **cloud service customer data** (3.2.12) and application artefacts and for the **cloud service provider** (3.2.15) to delete all **cloud service customer data** (3.2.12) as well as contractually specified **cloud service derived data** (3.2.13) after an agreed period.

3.2.36 Software as a Service (SaaS): **Cloud service category** (3.2.10) in which the **cloud capabilities type** (3.2.4) provided to the **cloud service customer** (3.2.11) is an **application capabilities type** (3.2.1).

3.2.37 tenant: One or more **cloud service users** (3.2.17) sharing access to a set of physical and virtual resources.

4 Abbreviations

For the purposes of this Recommendation | International Standard, the following abbreviations apply:

CaaS	Communications as a Service
CompaaS	Compute as a Service
DSaaS	Data Storage as a Service
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
NaaS	Network as a Service
PaaS	Platform as a Service
PII	Personally Identifiable Information
SaaS	Software as a Service
SLA	Service Level Agreement

5 Conventions

References to terms defined in clause 3 are shown in bold.

6 Cloud computing overview

6.1 General

Cloud computing is a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand. The **cloud computing** paradigm is composed of key characteristics, **cloud computing** roles and activities, **cloud capabilities types** and **cloud service categories**, **cloud deployment models** and **cloud computing** cross cutting aspects that are briefly described in this clause 6.

6.2 Key characteristics

Cloud computing is an evolving paradigm. This clause 6.2 identifies and describes key characteristics of **cloud computing** and is not intended to prescribe or constrain any particular method of deployment, service delivery, or business operation.

Key characteristics of **cloud computing** are:

– ***Broad network access***: A feature where the physical and virtual resources are available over a network and accessed through standard mechanisms that promote use by heterogeneous client platforms. The focus of this key characteristic is that **cloud computing** offers an increased level of convenience in that users can access physical and virtual resources from wherever they need to work, as long as it is network accessible, using a wide variety of clients including devices such as mobile phones, tablets, laptops, and workstations;

– ***Measured service***: A feature where the metered delivery of **cloud services** is such that usage can be monitored, controlled, reported, and billed. This is an important feature needed to optimize and validate the delivered **cloud service**. The focus of this key characteristic is that the customer may only pay for the resources that they use. From the customers' perspective, **cloud computing** offers the users value by enabling a switch from a low efficiency and asset utilization business model to a high efficiency one;

– ***Multi-tenancy***: A feature where physical or virtual resources are allocated in such a way that multiple **tenants** and their computations and data are isolated from and inaccessible to one another. Typically, and within the context of **multi-tenancy**, the group of **cloud service users** that form a **tenant** will all belong to the same **cloud service customer** organization. There might be cases where the group of **cloud service users** involves users from multiple different **cloud service customers**, particularly in the case of **public cloud** and **community cloud** deployments. However, a given **cloud service customer** organization might have many different tenancies with a single **cloud service provider** representing different groups within the organization;

– ***On-demand self-service***: A feature where a **cloud service customer** can provision computing capabilities, as needed, automatically or with minimal interaction with the **cloud service provider**. The focus of this key characteristic is that **cloud computing** offers users a relative reduction in costs, time, and effort needed to take an action, since it grants the user the ability to do what they need, when they need it, without requiring additional human user interactions or overhead;

– ***Rapid elasticity and scalability***: A feature where physical or virtual resources can be rapidly and elastically adjusted, in some cases automatically, to quickly increase or decrease resources. For the **cloud service customer**, the physical or virtual resources available for provisioning often appear to be unlimited and can be purchased in any quantity at any time automatically, subject to constraints of service agreements. Therefore, the focus of this key characteristic is that **cloud computing** means that the customers no longer need to worry about limited resources and might not need to worry about capacity planning;

– ***Resource pooling***: A feature where a **cloud service provider's** physical or virtual resources can be aggregated in order to serve one or more **cloud service customers**. The focus of this key characteristic is that **cloud service providers** can support **multi-tenancy** while at the same time using abstraction to mask the complexity of the process from the customer. From the customer's perspective, all they know is that the service works, while they generally have no control or

knowledge over how the resources are being provided or where the resources are located. This offloads some of the customer's original workload, such as maintenance requirements, to the provider. Even with this level of abstraction, it should be pointed out that users might still be able to specify location at a higher level of abstraction (e.g., country, state, or data centre).

6.3 Cloud computing roles and activities

Within the context of **cloud computing**, it is often necessary to differentiate requirements and issues for certain **parties**. These **parties** are entities that play roles (and sub-roles). Roles, in turn, are sets of activities and activities themselves are implemented by components. All **cloud computing** related activities can be categorized into three main groups: activities that use services, activities that provide services and activities that support services. It is important to note that a **party** may play more than one role at any given point in time and may only engage in a specific subset of activities of that role.

The major roles of **cloud computing** are:

– ***Cloud service customer***: A **party** which is in a business relationship for the purpose of using **cloud services**. The business relationship is with a **cloud service provider** or a **cloud service partner**. Key activities for a **cloud service customer** include, but are not limited to, using **cloud services**, performing business administration, and administering use of **cloud services**;

– ***Cloud service partner***: A **party** which is engaged in support of, or auxiliary to, activities of either the **cloud service provider** or the **cloud service customer**, or both. A **cloud service partner's** activities vary depending on the type of partner and their relationship with the **cloud service provider** and the **cloud service customer**. Examples of **cloud service partners** include **cloud auditor** and **cloud service broker**;

– ***Cloud service provider***: A **party** which makes **cloud services** available. The **cloud service provider** focuses on activities necessary to provide a **cloud service** and activities necessary to ensure its delivery to the **cloud service customer** as well as **cloud service** maintenance. The **cloud service provider** includes an extensive set of activities (e.g., provide service, deploy and monitor service, manage business plan, provide audit data, etc.) as well as numerous sub-roles (e.g., business manager, service manager, network provider, security and risk manager, etc.).

6.4 Cloud capabilities types and cloud service categories

A **cloud capabilities type** is a classification of the functionality provided by a **cloud service** to the **cloud service customer**, based on the resources used. There are three different **cloud capabilities types**: **application capabilities type**, **infrastructure capabilities type**, and **platform capabilities type**, which are different because they follow the principle of separation of concerns, i.e. they have minimal functionality overlap between each other.

The **cloud capabilities types** are:

– ***Application capabilities type***: A **cloud capabilities type** in which the **cloud service customer** can use the **cloud service provider's** applications;

– ***Infrastructure capabilities type***: A **cloud capabilities type** in which the **cloud service customer** can provision and use processing, storage or networking resources;

– ***Platform capabilities type***: A **cloud capabilities type** in which the **cloud service customer** can deploy, manage and run customer-created or customer-acquired applications using one or more programming languages and one or more execution environments supported by the **cloud service provider**.

There are only three **cloud capabilities types** defined in this Recommendation | International Standard. These **cloud capabilities types** should not be confused with other categorizations of **cloud services**.

A **cloud service category** is a group of **cloud services** that possess some common set of qualities. A **cloud service category** can include capabilities from one or more **cloud capabilities types**.

Representative **cloud service categories** are:

– ***Communications as a Service (CaaS)***: A **cloud service category** in which the capability provided to the **cloud service customer** is real time interaction and collaboration;

– ***Compute as a Service (CompaaS)***: A **cloud service category** in which the capabilities provided to the **cloud service customer** are the provision and use of processing resources needed to deploy and run software;

– ***Data Storage as a Service (DSaaS)***: A **cloud service category** in which the capability provided to the **cloud service customer** is the provision and use of data storage and related capabilities;

– ***Infrastructure as a Service (IaaS)***: A **cloud service category** in which the **cloud capabilities type** provided to the **cloud service customer** is an **infrastructure capabilities type**;

– ***Network as a Service (NaaS)***: A **cloud service category** in which the capability provided to the **cloud service customer** is transport connectivity and related network capabilities;

– ***Platform as a Service (PaaS)***: A **cloud service category** in which the **cloud capabilities type** provided to the **cloud service customer** is a **platform capabilities type**;

– ***Software as a Service (SaaS)***: A **cloud service category** in which the **cloud capabilities type** provided to the **cloud service customer** is an **application capabilities type**.

It is expected that there will be additional **cloud service categories** (see Annex A). This Recommendation | International Standard does not imply that any **cloud service category** is more important than any other.

6.5 Cloud deployment models

Cloud deployment models represent how **cloud computing** can be organized based on the control and sharing of physical or virtual resources.

The **cloud deployment models** include:

– ***Public cloud***: **Cloud deployment model** where **cloud services** are potentially available to any **cloud service customer** and resources are controlled by the **cloud service provider**. A **public cloud** may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the **cloud service provider**. Actual availability for specific **cloud service customers** may be subject to jurisdictional regulations. **Public clouds** have very broad boundaries, where **cloud service customer** access to **public cloud** services has few, if any, restrictions;

– ***Private cloud***: **Cloud deployment model** where **cloud services** are used exclusively by a single **cloud service customer** and resources are controlled by that **cloud service customer**. A **private cloud** may be owned, managed, and operated by the organization itself or a third party and may exist on premises or off premises. The **cloud service customer** may also authorize access to other **parties** for its benefit. **Private clouds** seek to set a narrowly controlled boundary around the **private cloud** based on limiting the customers to a single organization;

– ***Community cloud***: **Cloud deployment model** where **cloud services** exclusively support and are shared by a specific collection of **cloud service customers** who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection. A **community cloud** may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises. **Community clouds** limit participation to a group of **cloud service customers** who have a shared set of concerns, in contrast to the openness of **public clouds**, while **community clouds** have broader participation than **private clouds**. These shared concerns include, but are not limited to, mission, **information security** requirements, policy, and compliance considerations;

– ***Hybrid cloud***: **Cloud deployment model** using at least two different **cloud deployment models**. The deployments involved remain unique entities but are bound together by appropriate technology that enables **interoperability**, **data portability** and application portability. A **hybrid cloud** may be owned, managed, and operated by the organization itself or a third party and may exist on premises or off premises. **Hybrid clouds** represent situations where interactions between two different deployments may be needed but remained linked via appropriate technologies. As such the boundaries set by a **hybrid cloud** reflect its two base deployments.

6.6 Cloud computing cross cutting aspects

Cross cutting aspects are behaviours or capabilities which need to be coordinated across roles and implemented consistently in a **cloud computing** system. Such aspects may impact multiple roles, activities, and components, in such a way that it is not possible to clearly assign them to individual roles or components, and thus become shared issues across the roles, activities and components.

Key cross cutting aspects include:

– ***Auditability***: The capability of collecting and making available necessary evidential information related to the operation and use of a **cloud service**, for the purpose of conducting an audit;

– ***Availability***: The property of being accessible and usable upon demand by an authorized entity. The "authorized entity" is typically a **cloud service customer**;

– ***Governance***: The system by which the provision and use of **cloud services** are directed and controlled. Cloud governance is cited as a cross-cutting aspect because of the requirement for transparency and the need to rationalize governance practices with **SLAs** and other contractual elements of the **cloud service customer** to **cloud service provider** relationship. The term internal cloud governance is used for the application of design-time and run-time policies to ensure that **cloud computing** based solutions are designed and implemented, and **cloud computing** based services are delivered, according to specified expectations. The term external cloud governance is used for some form of agreement between the **cloud service customer** and the **cloud service provider** concerning the use of **cloud services** by the **cloud service customer**;

– ***Interoperability***: Ability of a **cloud service customer** to interact with a **cloud service** and exchange information according to a prescribed method and obtain predictable results;

– ***Maintenance and versioning***: Maintenance refers to changes to a **cloud service** or the resources it uses in order to fix faults or in order to upgrade or extend capabilities for business reasons. Versioning implies the appropriate labelling of a service so that it is clear to the **cloud service customer** that a particular version is in use;

– ***Performance***: A set of behaviours relating to the operation of a **cloud service**, and having metrics defined in a **SLA**;

– ***Portability***: Ability of **cloud service customers** to move their data or their applications between multiple **cloud service providers** at low cost and with minimal disruption. The amount of cost and disruption that is acceptable may vary based upon the type of **cloud service** that is being used;

– ***Protection of PII***: Protect the assured, proper, and consistent collection, processing, communication, use and disposal of Personally Identifiable Information (PII) in relation to **cloud services**;

– ***Regulatory***: There are a number of different regulations that may influence the use and delivery of **cloud services**. Statutory, regulatory, and legal requirements vary by market sector and jurisdiction, and they can change the responsibilities of both **cloud service customers** and **cloud service providers**. Compliance with such requirements is often related to governance and risk management activities;

– ***Resiliency***: Ability of a system to provide and maintain an acceptable level of service in the face of faults (unintentional, intentional, or naturally caused) affecting normal operation;

– ***Reversibility***: A process for the **cloud service customer** to retrieve their **cloud service customer data** and application artefacts and for the **cloud service provider** to delete all **cloud service customer data** as well as contractually specified **cloud service derived data** after an agreed period;

– ***Security***: Ranges from physical security to application security, and includes requirements such as authentication, authorization, **availability**, **confidentiality**, identity management, **integrity**, non-repudiation, audit, security monitoring, incident response, and security policy management;

– ***Service levels and service level agreement***: The **cloud computing service level agreement** (cloud **SLA**) is a **service level agreement** between a **cloud service provider** and a **cloud service customer** based on a taxonomy of **cloud computing** specific terms to set the quality of the **cloud services** delivered. It characterizes quality of the cloud services delivered in terms of: 1) a set of measurable properties specific to **cloud computing** (business and technical) and 2) a given set of **cloud computing roles** (**cloud service customer** and **cloud service provider** and related **sub-roles**).

Many of these cross cutting aspects, when combined with the key characteristics of **cloud computing**, represent good reasons for using **cloud computing**. However, cross cutting aspects like security, protection of PII, and governance have been identified as major concerns and in some cases an impediment to the adoption of **cloud computing**.

Annex A

Cloud service categories

(This annex does not form an integral part of this Recommendation | International Standard.)

Annex A describes the possibility of there being additional **cloud service categories** not yet found in this Recommendation | International Standard.

Table A.1 – Cloud service categories and cloud capabilities types

Cloud service categories	Cloud capabilities types		
	Infrastructure	Platform	Application
Compute as a Service	X		
Communications as a Service		X	X
Data Storage as a Service	X	X	X
Infrastructure as a Service	X		
Network as a Service	X	X	X
Platform as a Service		X	
Software as a Service			X

Table A.1 shows the relationship of the seven **cloud service categories** and three **cloud capabilities types** described in clause 6. An "X" at the intersection of a row and column depicts that the **cloud service category**, shown as a row in Table A.1, is of the indicated **cloud capabilities type**, shown as a column in Table A.1.

A **cloud service category** that offers processing, storage or networking resources has an "X" in the Infrastructure column. A **cloud service category** may offer the capability of deploying, managing and running customer-created or customer-acquired applications using one or more programming languages and one or more execution environments supported by the **cloud service provider**, in which case it has an "X" in the Platform column. Similarly, a **cloud service category** may offer the use of an application offered by the **cloud service provider**, in which case it will have an "X" in the Application column. Note that a **cloud service category** could offer any combination of the three **cloud capability types**.

The commercial **cloud computing** market is very dynamic and new **cloud services** continue to materialize into new informal **cloud service categories**. Some examples of such emerging **cloud service categories** are included in Table A.2. Many more **cloud service categories** will continue to emerge as **cloud computing** continues to grow.

Table A.2 – Emerging cloud service categories

Emerging cloud service categories	Description
Database as a Service	The capability provided to the **cloud service customer** is database functionalities on demand where the installation and maintenance of the databases are performed by the **cloud service provider**.
Desktop as a Service	The capabilities provided to the **cloud service customer** are the ability to build, configure, manage, store, execute, and deliver users' desktop functions remotely.
Email as a Service	The capabilities provided to the **cloud service customer** are a complete email service including related support services such as storage, receipt, transmission, backup, and recovery of email.
Identity as a Service	The capabilities provided to the **cloud service customer** are Identity and Access Management (IAM) that can be extended and centralized into existing operating environments. This includes provisioning, directory management, and the operation of a single sign-on service.
Management as a Service	The capabilities provided to the **cloud service customer** including application management, asset and change management, capacity management, problem management (service desk), project portfolio management, service catalog, and service level management.
Security as a Service	The capabilities provided to the **cloud service customer** are the integration of a suite of security services with the existing operating environment by the **cloud service provider**. This may include authentication, anti-virus, anti-malware/spyware, intrusion detection, and security event management, among others.

Bibliography

– ISO/IEC 20000-1:2011, *Information technology – Service management – Part 1: Specification*.

– ISO/IEC 27000:2014, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

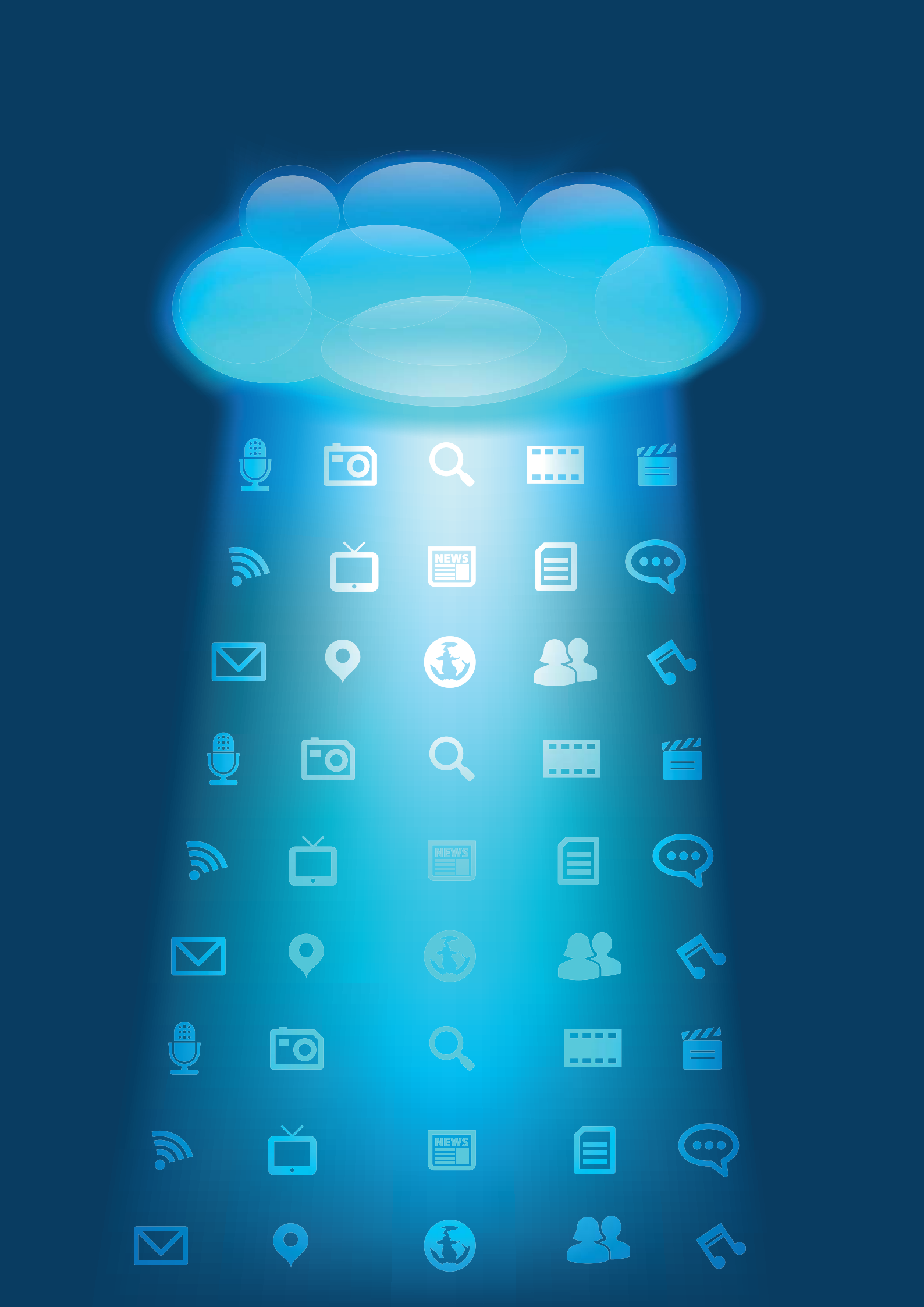
– ISO 27729:2012, *Information and documentation – International standard name identifier (ISNI)*.

– Recommendation ITU-T Y.101 (2000), *Global Information Infrastructure terminology: Terms and definitions*.

– National Institute of Standards and Technology Special Publication 800-145, *The NIST Definition of Cloud Computing*.

– National Institute of Standards and Technology Special Publication 800-146, *Cloud Computing Synopsis and Recommendations*.

– National Institute of Standards and Technology Special Publication 500-292, *NIST Cloud Computing Reference Architecture*.


NEWS
NEWS
NEWS
NEWS

Cloud computing – Framework and high-level requirements

Recommendation ITU-T Y.3501

(06/2016)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Summary

Recommendation ITU-T Y.3501 provides a cloud computing framework by identifying high-level requirements for cloud computing. It specifies the requirements which are derived from an analysis of several use cases.

Keywords

Cloud computing, cloud service, framework, requirement, use case.

Table of Contents

1 Scope

This Recommendation provides a cloud computing framework by identifying high-level requirements for cloud computing. The Recommendation addresses the general requirements and use cases for:

– Cloud computing;

– Infrastructure as a service (IaaS), network as a service (NaaS), desktop as a service (DaaS), platform as a service (PaaS), communication as a service (CaaS) and big data as a service (BDaaS);

– Inter-cloud computing, end-to-end cloud computing management, trusted cloud service, and cloud infrastructure.

This Recommendation addresses a set of use cases and related requirements which are included in Appendix I. Appendix II provides information on the methodology and edition plan of this Recommendation.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing.*

[ITU-T X.1631] Recommendation ITU-T X.1631 (2015), *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services.*

[ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014), *Information technology – Cloud computing – Overview and vocabulary.*

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), *Information technology – Cloud computing – Reference architecture.*

[ITU-T Y.3503] Recommendation ITU-T Y.3503 (2013), *Requirements for desktop as a service.*

[ITU-T Y.3510] Recommendation ITU-T Y.3510 (2016), *Cloud computing infrastructure requirements.*

[ITU-T Y.3511] Recommendation ITU-T Y.3511 (2014), *Framework of inter-cloud computing.*

[ITU-T Y.3512] Recommendation ITU-T Y.3512 (2014), *Cloud computing – Functional requirements of Network as a Service.*

[ITU-T Y.3513] Recommendation ITU-T Y.3513 (2014), *Cloud computing – Functional requirements of Infrastructure as a Service.*

[ITU-T Y.3520] Recommendation ITU-T Y.3520 (2015), *Cloud computing framework for end to end resource management.*

[ITU-T Y.3521] Recommendation ITU-T Y.3521/M.3070 (2016), *Overview of end-to-end cloud computing management.*

[ITU-T Y.3600] Recommendation ITU-T Y.3600 (2015), *Big data – cloud computing based requirements and capabilities.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 big data [ITU-T Y.3600]: A paradigm for enabling the collection, storage, management, analysis and visualization, potentially under real-time constraints, of extensive datasets with heterogeneous characteristics.

NOTE – Examples of datasets characteristics include high-volume, high-velocity, high-variety, etc.

3.1.2 big data as a service (BDaaS) [ITU-T Y.3600]: A cloud service category in which the capabilities provided to the cloud service customer are the ability to collect, store, analyse, visualize and manage data using big data.

3.1.3 cloud computing [ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

3.1.4 cloud service [ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.5 cloud service category [ITU-T Y.3500]: Group of cloud services that possess some common set of qualities.

3.1.6 cloud service customer [ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

NOTE – A business relationship does not necessarily imply financial agreements.

3.1.7 cloud service partner [ITU-T Y.3500]: Party which is engaged in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer, or both.

3.1.8 cloud service provider [ITU-T Y.3500]: Party which makes cloud services available.

3.1.9 cloud service user [ITU-T Y.3500]: Natural person, or entity acting on their behalf, associated with a cloud service customer that uses cloud services.

NOTE – Examples of such entities include devices and applications.

3.1.10 communications as a service (CaaS) [ITU-T Y.3500]: Cloud service category in which the capability provided to the cloud service customer is real time interaction and collaboration.

NOTE – CaaS can provide both application capabilities type and platform capabilities type.

3.1.11 desktop as a service (DaaS) [ITU-T Y.3503]: A cloud service category in which the capabilities provided to the cloud service customer are the ability to build, configure, manage, store, execute and deliver users' desktop functions remotely.

3.1.12 hypervisor [ITU-T Y.3510]: A type of system software that allows multiple operating systems to share a single hardware host.

NOTE – Each operating system appears to have the host's processor, memory and other resources, all to itself.

3.1.13 infrastructure as a service (IaaS) [ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer is an infrastructure capabilities type.

NOTE – The cloud service customer does not manage or control the underlying physical and virtual resources, but does have control over operating systems, storage, and deployed applications that use the physical and virtual resources. The cloud service customer may also have limited ability to control certain networking components (e.g., host firewalls).

3.1.14 infrastructure capabilities type [ITU-T Y.3500]: Cloud capabilities type in which the cloud service customer can provision and use processing, storage or networking resources.

3.1.15 inter-cloud computing [ITU-T Y.3511]: The paradigm for enabling the interworking between two or more cloud service providers.

NOTE – Inter-cloud computing is also referred as inter-cloud.

3.1.16 network as a service (NaaS) [ITU-T Y.3500]: Cloud service category in which the capability provided to the cloud service customer is transport connectivity and related network capabilities.

3.1.17 party [ITU-T Y.3500]: Natural person or legal person, whether or not incorporated, or a group of either.

3.1.18 platform as a service (PaaS) [ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer is a platform capabilities type.

3.1.19 resource management [ITU-T Y.3520]: The most efficient and effective way to access, control, manage, deploy, schedule and bind resources when they are provided by service providers and requested by customers.

3.1.20 role [ITU-T Y.3502]: A set of activities that serves a common purpose.

3.1.21 service level agreement (SLA) [ITU-T Y.3500]: Documented agreement between the service provider and customer that identifies services and service targets.

NOTE 1 – A service level agreement can also be established between the service provider and a supplier, an internal group or a customer acting as a supplier.

NOTE 2 – A service level agreement can be included in a contract or another type of documented agreement.

3.1.22 virtual desktop [ITU-T Y.3503]: An environment for accessing end user's desktop functions remotely.

NOTE – Examples of end user's desktop functions can include desktop interface functions for applications, data access functions for multimedia data, and control functions for input/output (I/O) devices.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 trusted cloud service: A cloud service that satisfies a set of requirements such as transparency for governance, management and security so that a cloud service customer (CSC) can be confident in using the cloud service.

NOTE 1 – The set of requirements will vary depending on the involved cloud service customer, the nature of the cloud service and the governing jurisdiction.

NOTE 2 – The set of requirements could also be related to additional cross-cutting aspects [ITU-T Y.3502] such as performance, resiliency, reversibility, SLAs, etc.

NOTE 3 – Transparency means that the cloud service provider (CSP) should commit to the CSC that they have appropriate and clear control and reporting mechanisms for governance, management and security, such as SLA commitments, online announcements, data handling policies, etc.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
BDaaS	Big Data as a Service
CaaS	Communication as a Service
CPU	Central Processing Unit
CSC	Cloud Service Customer
CSN	Cloud Service Partner
CSP	Cloud Service Provider
DaaS	Desktop as a Service

HD	High Definition
IaaS	Infrastructure as a Service
NaaS	Network as a Service
PaaS	Platform as a Service
PII	Personally Identifiable Information
QoE	Quality of Experience
QoS	Quality of Service
SaaS	Software as a Service
SDK	Software Development Kit
SLA	Service Level Agreement
VLAN	Virtual Local Area Network
VM	Virtual Machine

5 Conventions

In this Recommendation:

The keywords "**is required**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

In the body of this document and its appendixes, the words shall, shall not, should and may sometimes appear, in which case they are to be interpreted, respectively, as is required to, is prohibited from, is recommended and can optionally. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative are to be interpreted as having no normative intent.

For readability, the short titles are attached to the requirements for referring to use cases in Appendix I.

6 General requirements for cloud computing

The general requirements for cloud computing derived from the use cases in clause I.1 are as follows:

– **Service life-cycle management**: It is required that the cloud service provider (CSP) supports automated service provisioning, modification and termination during the service life-cycle;

– **Regulatory**: It is required that all applicable laws and regulations be respected, including those related to the protection of personally identifiable information (PII);

– **Security**: It is required that the cloud computing systems provided by the CSP be appropriately secured to protect the interests of all involved parties (e.g., persons and organizations);

– **Accounting and charging**: It is recommended that cloud service provided by the CSP supports various accounting and charging models and policies;

– **Efficient service deployment**: It is recommended that cloud service provided by the CSP enables efficient use of resources for service deployment;

– **Interoperability**: It is recommended that cloud service provided by the CSP complies with appropriate specifications and/or standards for allowing these systems to work together;
– **Portability**: It is recommended that cloud service provided by the CSP supports the portability of software assets and the data of cloud service customers (CSCs) with minimum disruption;
– **Service access**: The CSP is recommended to provide CSCs with access to cloud services from a variety of user devices. It is recommended that CSCs be provided with a consistent experience when accessing cloud services from different devices;
– **Service availability, service reliability and quality assurance**: It is recommended that the CSP provides end-to-end quality of service assurance, high levels of reliability and continued availability of cloud services according to the service level agreement (SLA) with the CSC.

7 General requirements for IaaS

The general requirements for infrastructure as a service (IaaS) derived from the use cases in clause I.2 are as follows:

– **Configuration, deployment and maintenance of resources**: The IaaS CSP is recommended to configure, deploy and maintain processing, storage and/or networking resources with specific SLAs and charging models to CSCs;
– **Use and monitoring of resources**: The IaaS CSP is recommended to provide the capability for CSCs to use and monitor processing, storage and/or networking resources so that they are able to deploy and run arbitrary software.

NOTE – Functional requirements for IaaS are provided in [ITU-T Y.3513].

8 General requirements for NaaS

The general requirements for network as a service (NaaS) derived from the use cases in clause I.3 are as follows:

– **On-demand network configuration**: It is required that the NaaS CSP provides the network capability, which can be configured on demand by the CSC;
– **Secure connectivity**: It is required that the NaaS CSP provides secure connectivity;
– **QoS-guaranteed connectivity**: The NaaS CSP is recommended to provide QoS-guaranteed connectivity according to the negotiated SLA;
– **Heterogeneous networks compatibility**: It is recommended that the NaaS CSP supports network connectivity through heterogeneous networks.

NOTE – Functional requirements for NaaS are provided in [ITU-T Y.3512].

9 General requirements for DaaS

The general requirements for desktop as a service (DaaS) derived from the use cases in clause I.4 are as follows:

– **Configurability of the virtual environment**: It is recommended that a user is capable of configuring the virtual desktops' virtual environment, such as the central processing unit (CPU), memory, storage, network, etc.;
– **Fast boot-up time**: DaaS CSP is recommended to provide CSCs with appropriate boot-up time of their virtual desktops;
– **QoE**: DaaS CSP is recommended to provide an acceptable user experience, including the running speed of application programs and the capability to select and run various applications, when application programs run in their CSC devices;
– **Single sign-on access control**: It is recommended that a CSC is capable to get all DaaS functionality with appropriate security requirements through a single sign-on mechanism.

The following DaaS general requirements are described in [ITU-T Y.3503] as follows:

– **Support for high-definition (HD) and three-dimensional (3D) applications**: DaaS can optionally support execution of HD applications on virtual desktops for CSCs;

– **Extensible storage**: It is recommended that a CSP support the storage extension requested by a CSC;

– **Response time**: It is recommended that DaaS provide CSCs with acceptable QoE;

– **High availability**: It is recommended that high availability in terms of delivery and operation of DaaS be assured by a CSP;

– **Resiliency to disaster**: In the case of a disaster, DaaS is recommended to provide and maintain an acceptable level of service;

– **Service continuity**: It is recommended that in the case of temporarily unavailable resource access, a CSP provides the capability to preserve the state of the user session;

– **System scalability**: It is recommended that DaaS supports elastic scalability of:

  • Storage for DaaS user account information, virtual desktop environment settings and active and inactive virtual desktop environments;

  • Processing and network capacity for the number of concurrent DaaS user connections and total DaaS users;

  • Underlying DaaS resources.

– **DaaS developer environments**: It is recommended to provide a developer environment for the service and contents regarding DaaS;

– **Diversity of DaaS clients**: It is recommended that the CSP support a wide selection of DaaS clients.

NOTE – Functional requirements for DaaS are provided in clause 8 of [ITU-T Y.3503].

10 General requirements for PaaS

The general requirements for platform as a service (PaaS) derived from the use cases in clause I.5 are as follows:

– **Application hosting**: It is required that the PaaS CSP provides an application hosting environment, where the application can be rapidly deployed, reliably executed, flexibly expanded and isolated from other applications;

– **Services delivery platform**: It is recommended that the PaaS CSP provides the capabilities of service presence, orchestration, billing, mash-up and tools for associated development and testing by CSCs through a unified application programming interface (API);

– **Integrated development environment**: The PaaS CSP can optionally provide comprehensive capabilities to CSCs for software development such as coding, debugging, compiling and distribution;

– **Development tools**: PaaS CSP can optionally provide development tools as a service to CSCs, who can use it on-demand.

11 General requirements for CaaS

The general requirements for communication as a service (CaaS) derived from the use cases in clause I.6 are as follows:

– **Communication capabilities openness**: It is recommended that the CSP provides APIs for accessing communication capabilities of CSNs to enhance their own services by using communication enablers;

– **Communication software development support**: It is recommended that the CSP provides support for communication software development, which is a group of communication building blocks, to CSNs in order to develop communication applications;

NOTE – Examples of communication building blocks are protocol stacks, codecs, authentication, etc.

– **Unified communication**: It is recommended that the CSP provides to CSCs a consistent unified user interface and user experience of communications applications, such as voice, messaging, audio, video conferencing, etc., across multiple devices and media-types.

12 General requirements for BDaaS

The general requirements for big data as a service (BDaaS) derived from the use cases in clause I.7 are as follows:

– **Resource clustering**: It is recommended for the CSP to cluster resources for processing of extensive data;

NOTE 1 – Resources includes processing, storage and networks, etc.

– **Data collection**: It is recommended for the BDaaS CSP to collect data from CSCs, CSNs and CSPs;

NOTE 2 – Data includes various types, different formats, real time streaming/static data and CSC data including users' behaviour data.

– **Data storing**: It is recommended for the BDaaS CSP to store data with sufficient storage and fulfil performance demands;

– **Data analysing**: It is recommended for the BDaaS CSP to analyse data with various kinds of analysis algorithms;

NOTE 3 – Data analysis algorithms include classification, clustering, regression, association, ranking, etc.

– **Data visualizing**: It is recommended for the BDaaS CSP to provide reporting tools with multiple styles of data visualization;

NOTE 4 – Visualization styles include statistical graphics, forms, diagrams, charts, etc.

– **Data managing**: It is recommended for the BDaaS CSP to support management of data lifecycle and resources monitoring.

NOTE 5 – Functional requirements for BDaaS are provided in clause 8 of [ITU-T Y.3600].

13 General requirements for inter-cloud computing

The general requirements for inter-cloud computing derived from the use cases in clause I.8 are as follows:

– **On-demand assignment of cloud computing resources among CSPs**: For assigning cloud computing resources among CSPs on demand, it is required that a CSP defines (a) a trusted relationship between cooperating CSPs; (b) an appropriate agreement and means of exchanging data on cost, performance and other information for each resource; and (c) an agreed methodology for requesting, using and returning the resources of other CSPs;

– **Resource and load distribution**: A CSP in an inter-cloud federation is required to utilize appropriate resources distributed in other CSPs for wide-area load distribution according to the required promptness, flexibility and cost;

– **User environment adaptation**: A CSP is required to detect changes in the cloud service user environment, discover alternative resources in other CSPs for these changes and migrate the service environment smoothly with minimum impact based on the CSC's approval;

NOTE 1 – These actions are to be performed for all cloud service users.

– **Inter-cloud service intermediation**: Inter-cloud service intermediation enables the CSP to select the most suitable cloud services and to create new cloud services by integrating cloud services offered by other CSPs. It is recommended that the CSP engages in support of intermediation for multiple cloud services of various cloud service categories such as IaaS, NaaS, PaaS and SaaS;

– **Large-scale migration**: A CSP in an inter-cloud federation is recommended to be able to guarantee continuity of all the cloud services in the CSP by large-scale service migration to other federated CSPs with minimum impact during a desired period. It is recommended to consider the priority of cloud services when migrating.

NOTE 2 – For more information on functional requirements for inter-cloud computing, see clause 9 of [ITU-T Y.3511].

14 General requirements for end-to-end cloud resource management

The general requirements for end-to-end cloud resource management derived from the use cases in clause I.9 are as follows:

– **Manageability for a single cloud service**: It is required that the CSP be able to collect management, telemetry and diagnostics and/or status information from the cloud computing systems used for providing cloud services and report the information to the CSC;

– **Manageability for multiple cloud services**: It is recommended that multiple CSPs work together to offer comprehensive status awareness and management information to expand across multiple cloud data centres as composite cloud services are built from multiple services implemented by multiple cloud service providers, requiring the need for multi-cloud, end-to-end management data.

NOTE – For more information on end-to-end cloud computing management, refer to [ITU-T Y.3520] and [ITU-T Y.3521].

15 General requirements for cloud infrastructure

The general requirements for cloud infrastructure derived from the use cases in clause I.10 are as follows:

– **Resource abstraction and control**: It is required for cloud infrastructure to provide resource abstraction and control capability to cloud services;

– **Resource provisioning**: It is required for cloud infrastructure to provide collaboratively processing, storage and network resources to cloud services and supporting functions.

NOTE – Functional requirements for cloud computing infrastructure are provided in [ITU-T Y.3510].

16 General requirements for trusted cloud services

The general requirements for trusted cloud services are derived from the use case in clause I.11. The following requirements are important for CSCs in order to be able to select a trusted cloud service. These requirements do not specify the levels and abilities of the cloud services, but require that the cloud services which are treated as trusted cloud services should satisfy the following:

– **Governance for trusted cloud service**: It is recommended for trusted cloud services to comply with appropriate or local standards and best practices of corporate governance and include appropriate mechanisms by which policies affecting the provision and use of cloud services are directed and controlled;

NOTE 1 – Part of this requirement refers to [ITU-T Y.3502].

– **Management for trusted cloud service**: It is recommended for trusted cloud services to include appropriate mechanisms for administration, reporting, location of stored data, privacy, de-identification of data, etc.

– **Resiliency for trusted cloud service**: It is recommended for trusted cloud services to include appropriate mechanisms by which an acceptable level of service can be maintained in the face of faults (unintentional, intentional or naturally caused) affecting normal operation;

NOTE 2 – Part of this requirement refers to [ITU-T Y.3502].

– **Security for trusted cloud service**: It is recommended for trusted cloud services to include appropriate mechanisms for cryptography, attack resistance, intrusion detection, security incident handling and reporting, etc.

NOTE 3 – Part of this requirement refers to [ITU-T X.1601].

– **Availability for trusted cloud service**: It is recommended for trusted cloud services to include appropriate mechanisms for ensuring the appropriate level of access to the service and usability by the CSC;

– **Auditability for trusted cloud service**: It is recommended for trusted cloud services to include appropriate mechanisms for collecting and making available necessary evidential information related to the operation and use of a cloud service, for the purpose of conducting an audit;

NOTE 4 – Part of this requirement refers to [ITU-T Y.3502].

– **Service agreement for trusted cloud service**: It is recommended for trusted cloud services to have appropriate service agreements or contracts for commitments to CSC on terms of their requirements and considerations.

17 Security considerations

The security framework from cloud computing [ITU-T X.1601], analyses security threats and challenges in the cloud computing environment, describes security capabilities that could mitigate these threats and addresses security challenges.

[ITU-T X.1631] provides guidelines supporting the implementation of information security controls for CSCs and CSPs. Many of the guidelines guide the CSPs to assist the CSCs in implementing the controls and guide the CSCs to implement such controls. Selection of appropriate information security controls and the application of the implementation guidance provided, will depend on a risk assessment as well as any legal, contractual, regulatory or other cloud-sector specific information security requirements.

Regarding the protection of PII, ISO/IEC 27018 is designed for organizations to use as a reference for selecting PII protection controls within the process of implementing a cloud computing information security management system based on ISO/IEC 27001, or as a guidance document for organizations for implementing commonly accepted PII protection controls.

Appendix I

Use cases of cloud computing

(This appendix does not form an integral part of this Recommendation.)

This appendix identifies use cases of cloud computing. Table I.1 shows the template used for the description of the use cases.

Table I.1 – Template for the description of a use case

Use case	
Name	Title of the use case
Abstract	Overview and features of the use case
Roles	Roles relating to/appearing in the use case
Figure	Figure to present the use case. (A UML-like diagram is suggested for clarifying relations between roles)
Pre-conditions (optional)	Pre-conditions represent the necessary conditions or use cases that should be achieved before starting the described use case. NOTE – As dependency may exist among different use cases, pre-conditions and post-conditions are introduced to help understand the relationships among use cases.
Post-conditions (optional)	As for pre-conditions, the post-condition describes conditions or use cases that will be carried out after the termination of a currently described use case.
Requirements	The title of requirements derived from the use case. For example: – Large-scale migration

Table I.2 lists the use cases described in this appendix.

Table I.2 – List of use cases

Domains	Use cases
Generic use case	– General CSC-CSP-CSN use case – Use case publish service – Use case consult service – Use case use service
IaaS	– IaaS general use case
NaaS	– NaaS general use case
DaaS	– DaaS general use case
PaaS	– PaaS general use case
CaaS	– CaaS general use case
BDaaS	– BDaaS general use case
Inter-cloud computing	– Inter-cloud computing use case for federation – Inter-cloud computing use case for intermediation
Cloud resource management	– End-to-end cloud resource management use case
Cloud infrastructure	– Cloud infrastructure use case
Trusted cloud service	– Trusted cloud service use case

I.1 Generic use case

Use case	
Name	General CSC-CSP-CSN use case
Abstract	This general use case, which describes the general activities of the CSC, CSP and CSN, consists of a set of use cases. It introduces a basic scenario where a CSP publishes a cloud service. A CSC or CSN consults this cloud service and uses this cloud service. These use cases clarify the relationships between these three main cloud roles.
Roles	CSC, CSP, CSN
Figure	
Included use cases	– UC-US (Use case use service) – UC-CS (Use case consult service) – UC-PS (Use case publish service)

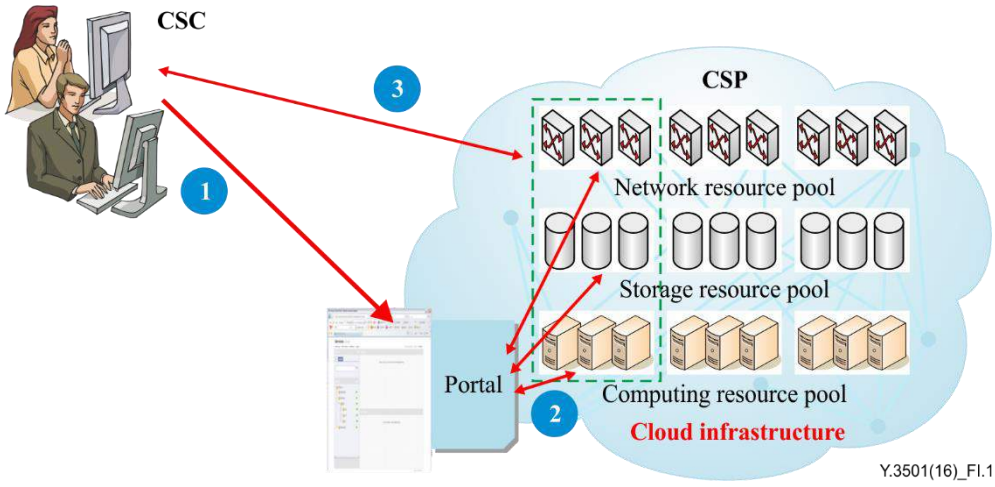
Use case	
Name	Use case publish service
Abstract	A CSP publishes cloud service information to the public so that any users including a CSP, CSC or CSN can use the published cloud service. In terms of service publishing, the CSP adds the service to a service catalogue which will be accessible to others. The CSP also maintains the catalogue.
Roles	CSP
Pre-conditions (optional)	
Post-conditions (optional)	– The CSP should maintain the public service.
Requirements	– Service life-cycle management – Security – Efficient service deployment – Portability – Regulatory aspects – Service availability, service reliability and quality assurance – Service access – Accounting and charging

Use case	
Name	Use case consult service
Abstract	A CSC, CSP or CSN consults a published service. For all the published services in the cloud service catalogue, any users including the CSC, CSP and CSN can access them. The consult scenario refers to consulting published-service details and associated SLAs.
Roles	CSC, CSP, CSN
Pre-conditions (optional)	– The service to be used has already been published by a CSP (UC-PS). – The CSC, CSP or CSN has been authenticated.
Post-conditions (optional)	– A given service should be accessible.

Use case	
Requirements	– Security – Service availability, service reliability and quality assurance – Service access – Interoperability – Regulatory aspects – Accounting and charging

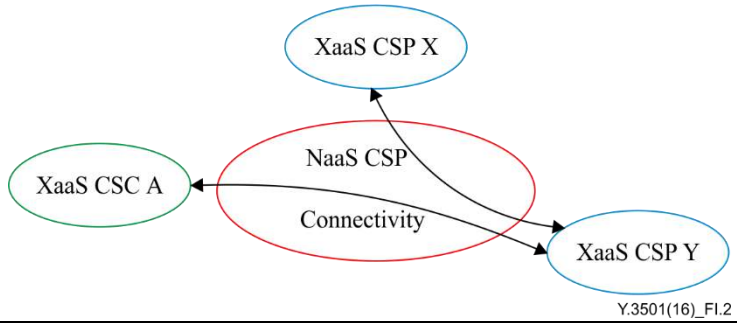
Use case	
Name	Use case use service
Abstract	A CSC or a CSN uses a published service. According to the agreement of the SLA, the user invokes the cloud service.
Actors	CSC, CSN
Pre-conditions (optional)	– The service to be used has already been published by a CSP (UC-PS). – The CSC or the CSN has been authenticated.
Post-conditions (optional)	– The used service should be kept available during the whole invocation. – The SLA should be met for service use.
Requirements	– Service life-cycle management – Security – Portability – Interoperability – Regulatory aspects – Service availability, service reliability and quality assurance – Service access – Accounting and charging

I.2 IaaS general use case

Use case	
Name	IaaS general use case
Abstract	CSC uses IaaS services including computing, storage and network capabilities to deploy and run arbitrary applications.
Roles	CSC, CSP
Figure	

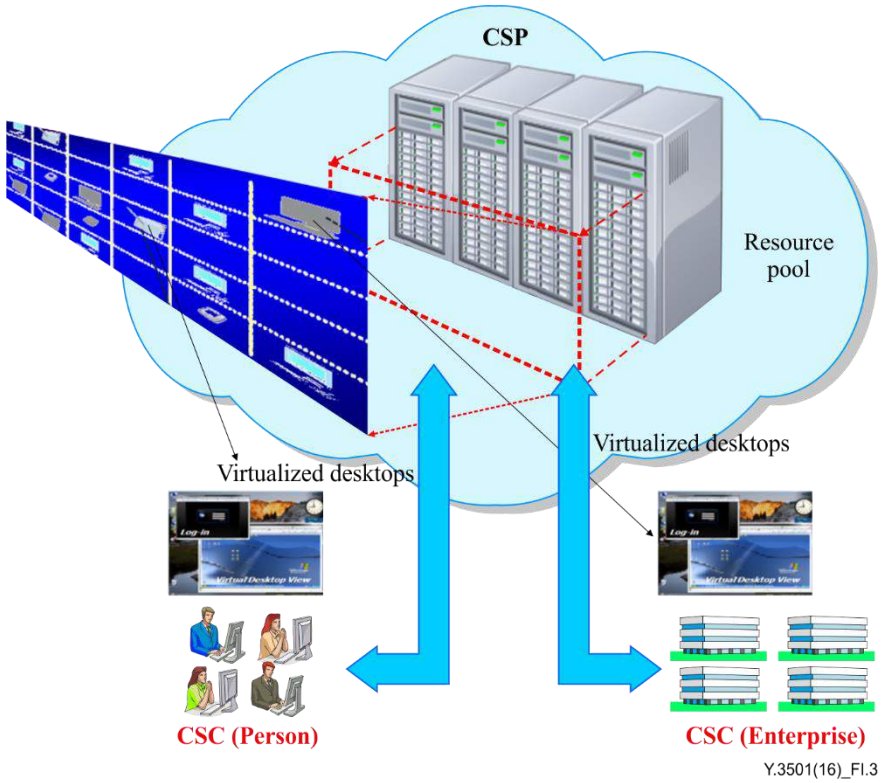
Use case	
Pre-conditions (optional)	– ① The CSC has accessed the IaaS service through the CSP portal with an appropriate security mechanism. – ② The CSC has selected the template or configured a specific VM and/or physical host. – ② The CSC has selected the storage resources, such as block, file and object storage, then attached them via their computing capabilities or used them directly. – ② The CSC has selected the network connectivity services, such as the IP address, VLAN, firewall and load balance and then applied them to the related computing and/or storage capabilities. – ② The CSC confirmed the SLAs and charge model with selected computing, storage and network connectivity services provided by the CSP.
Post-conditions (optional)	– ③ The CSC manages and monitors computing, storage and network capabilities with arbitrary applications. – ③ The CSP configures, deploys and maintains hypervisors and storage resources. – ③ The CSP establishes, configures, delivers and maintains network connectivity to the CSC. – ③ The CSP provides security infrastructure to the CSC.
Requirements	– Configuration, deployment and maintenance of resources – Use and monitoring of resources

I.3 NaaS general use case

Use case	
Name	NaaS general use case
Abstract	A NaaS CSP sets up, maintains and releases the network connectivity between CSCs and between the CSP and CSC as a cloud service. This can include on-demand and semi-permanent connectivity.
Roles	CSC, CSP
Figure	
Pre-conditions (optional)	– There is no connectivity between XaaS CSC A and XaaS CSP Y. – There is no connectivity between XaaS CSP X and XaaS CSP Y. – Either XaaS CSC A or XaaS CSP Y requests the connectivity between them with their end-point identifiers and associated characteristics (referring to QoS and security aspects) for the connectivity. – Either XaaS CSP X or XaaS CSP Y requests the connectivity between them with their end-point identifiers and associated characteristics (referring to QoS and security aspects) for the connectivity.
Post-conditions (optional)	– XaaS CSC A and XaaS CSP Y can communicate with each other. – XaaS CSC X and XaaS CSP Y can communicate with each other.

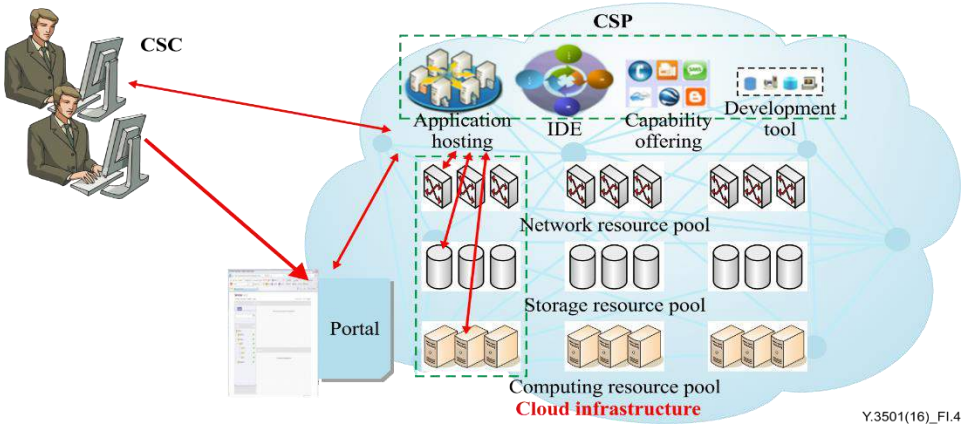
Use case	
Requirements	– On-demand network configuration – Heterogeneous networks compatibility – QoS-guaranteed connectivity – Secured connectivity

I.4 DaaS general use case

Use case	
Name	DaaS general use case
Abstract	– Between a consumer and a CSP: In this scenario, a consumer accesses and uses data or applications in a CSP which offers a virtual desktop service. A consumer can enjoy the environment with all programs and applications which are identical with those of traditional PCs. The consumer can choose the virtual hardware specification of its virtual desktops. If necessary, the environment (i.e., operating system) can be changed to another one immediately. Since all data is totally stored with password protection and managed in the CSP, all the consumer has to do is keep up with a password. – Between an enterprise and a CSP: An enterprise using a virtual desktop service from a CSP for its internal processes is included in this use case. In this scenario, the enterprise can select applications or OS in the DaaS service for certain enterprise functions. Unlike the use case between a consumer and a CSP, the enterprise normally uses storage for backups. Also, the enterprise can overcome peak loads and save energy by requesting the CSP online to increase or decrease the number of virtual desktops, respectively. – Between an enterprise, a consumer and a CSP: In this scenario, the enterprise makes the consumer work with its internal processes outside of the enterprise by transferring virtual desktops and related data through the CSP. Contrary to the above two scenarios, the consumer cannot select applications freely and more limitations to access data in the enterprise may exist than within the enterprise. Whenever the consumer connects with the CSP, the CSP sends data to the consumer by accessing the enterprise to handle or bypass corresponding data.
Roles	CSP, CSC
Figure	

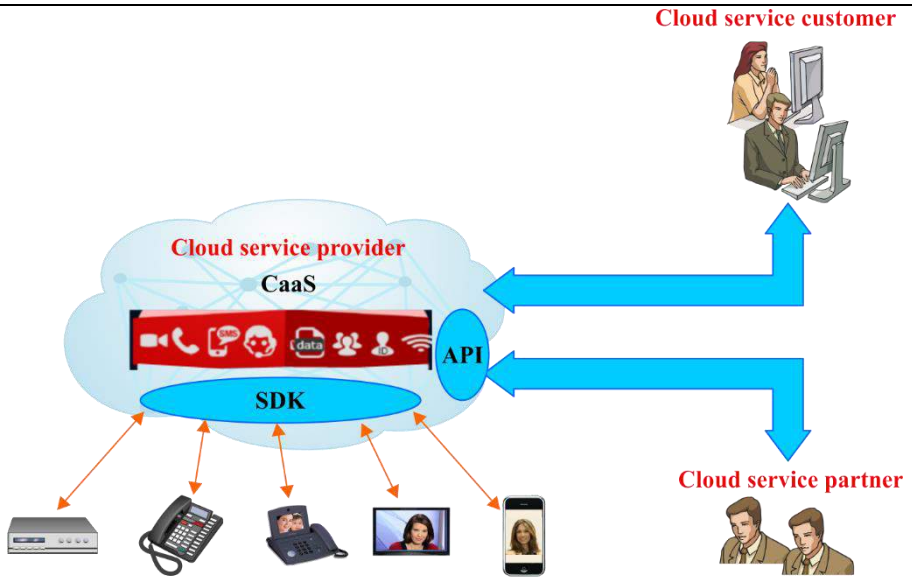
Use case	
Pre-conditions (optional)	– A CSP offers the configuration menu of the virtual desktop to CSCs. – A CSC specifies parameter-settings shown in the configuration menu.
Post-conditions (optional)	– A CSC uses DaaS service.
Requirements	– QoE – Fast boot-up time – Configurability of the virtual environment – Single sign-on access control – Support for high-definition (HD) and three dimensional (3D) applications – Extensible storage – Response time – High availability – Resiliency to disaster – Service continuity – System scalability – DaaS developer environments – Diversity of DaaS client

I.5 PaaS general use case

Use case	
Name	PaaS general use case
Abstract	A PaaS CSP provides application hosting, capabilities offering, integrated development environment and development tools to CSC.
Roles	CSC, CSP
Figure	
Pre-conditions (optional)	– CSC requests PaaS service from CSP1 to develop an application. – CSP1 provides a cloud-based integrated development environment to CSC as well as some development tools. – CSC requests PaaS service from CSP2 to use a service delivery platform provided by CSP. – CSP2 provides service presence, orchestration, billing, mash-up and associated development and testing tools. – CSC requests PaaS service from CSP3 to an application hosting environment provided by CSP. – CSP3 provides application hosting service to CSC to deploy and execute the application.

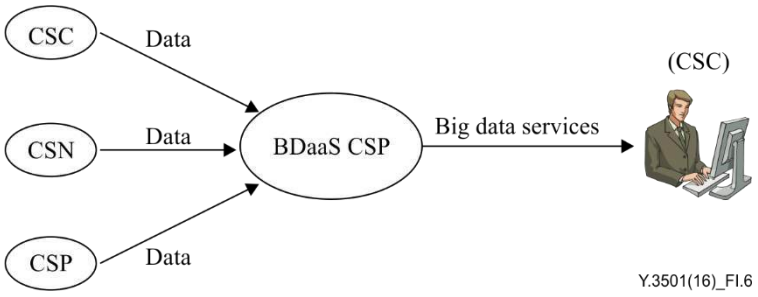
Use case	
Post-conditions (optional)	– CSC develops an application using an integrated development environment to be more productive by reducing the configuration necessary to piece together multiple development utilities and setup time. – CSC uses development tools without deploy and maintain. – CSC uses capabilities sets, such as location and SMS to develop an application. – CSC deploys and runs an application on the application hosting environment without concerning the underlying resources.
Requirements	– Application hosting – Services delivery platform – Integrated development environment – Development tools

I.6 CaaS general use case

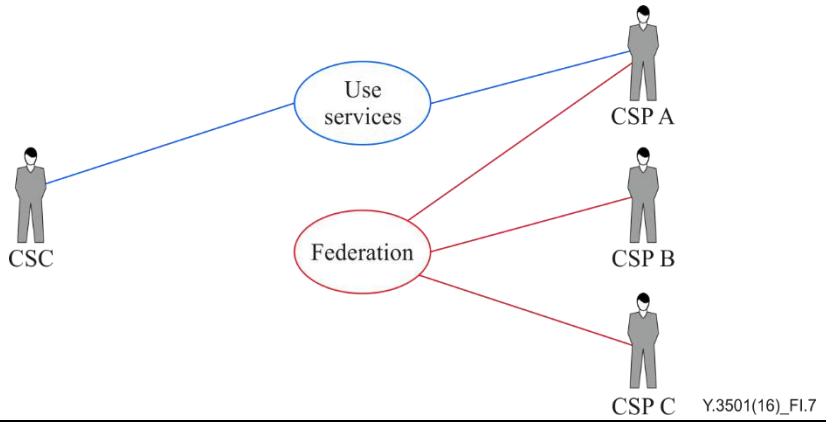
Use case	
Name	CaaS general use case
Abstract	A CaaS CSP provides API and/or software development support such as a software development kit (SDK) to enable building of a communication platform and services by a CSN, or in addition to build communication services offered to CSC directly by CaaS CSP. This involves both platform capabilities type and application capabilities type.
Roles	CSC, CSP,CSN
Figure	
Pre-conditions (optional)	With platform capabilities type: – CSN wants to develop some product or service, using communication features such as video call capability. For example, a non-cloud video game developer could include CaaS-based voice and video calling between players of their game. – CSP provides carrier-grade video call capabilities to a CSN through CaaS API. – CSN wants to enhance a device (such as an IP-connected camera) with a remote control feature, while the original device only has connectivity capabilities but no communication capabilities. – CSP provides the SDK to a CSN, in this case, the CSN can add communication capabilities to the device. With application capabilities type: – CSC wants to use communication applications on different kinds of devices, such as wire-line telephone, mobile phone, IMS device, tablet and PC.

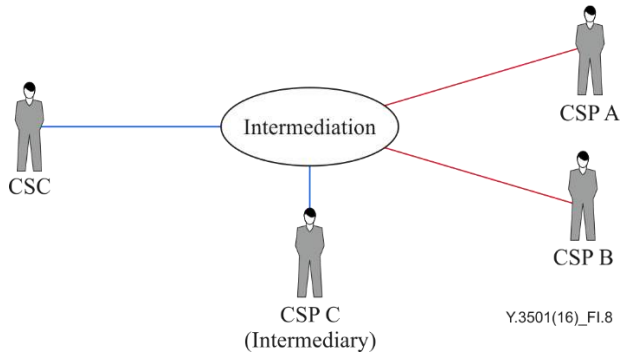
Use case	
Post-conditions (optional)	With platform capabilities type: – CSN develops a product or service with carrier-grade video call capabilities provided by the CaaS CSP. – CSC can call the device and control it remotely by using SDK provided by the CSP. With application capabilities type: – CSC can access all kinds of communications applications with consistent unified user-interface and user-experience over multiple devices, such as wire-line telephone, mobile phone, IMS device, tablet and PC.
Requirements	– Communication capabilities openness – Communication software development support – Unified communication

I.7 BDaaS general use case

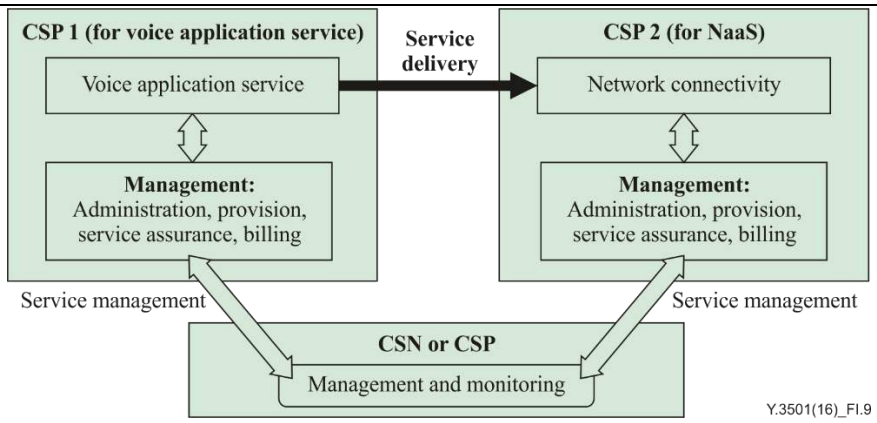
Use case	
Name	BDaaS general use case
Abstract	A BDaaS CSP provides big data services through cloud computing. The BDaaS CSP uses the cloud computing capabilities to implement various big data capabilities such as collecting data, managing data storage, managing data privacy, managing data pre-processing, providing data integration, managing data provenance, analyzing data and visualizing data.
Roles	CSC, CSP, CSN
Figure	
Pre-conditions (optional)	– The CSN provides appropriate access methods of data to the BDaaS CSP.
Post-conditions (optional)	
Requirements	– Resource clustering – Data collection – Data storing – Data analysing – Data visualizing – Data managing

I.8 Inter-cloud computing use case

Use case	
Name	Inter-cloud computing use case for federation
Abstract	CSPs federate to provide a service to the CSC
Roles	CSC, CSP
Figure	
Pre-conditions (optional)	– CSPs federate with each other by establishing a trust relationship and policy settlement. – A CSC uses a service provided by one of the federated CSPs. – Case-A: The CSP that offers the service to the CSC is going to spend all resources due to overload, or has lost the resources due to disaster. – Case-B: The CSC changes its environment (e.g., location) and reaches the CSP from a place which is further away than before.
Post-conditions (optional)	– Case-A: The CSP ensures that its services continue to be offered by the support of other federated CSPs, even when performance or availability of the service may be degraded due to CSP's resource problems (e.g., overload or disaster). – Case-B: Another CSP in the federation, on behalf of the CSP which has offered the service to the CSC, provides a new appropriate service environment to the CSC to compensate for possible degradation, even when performance or availability of the service may be degraded due to a CSC's environmental change (e.g., location changes).
Requirements	– On-demand assignment of cloud resource among CSPs – Resource and load distribution – Large-scale migration – User environment adaptation

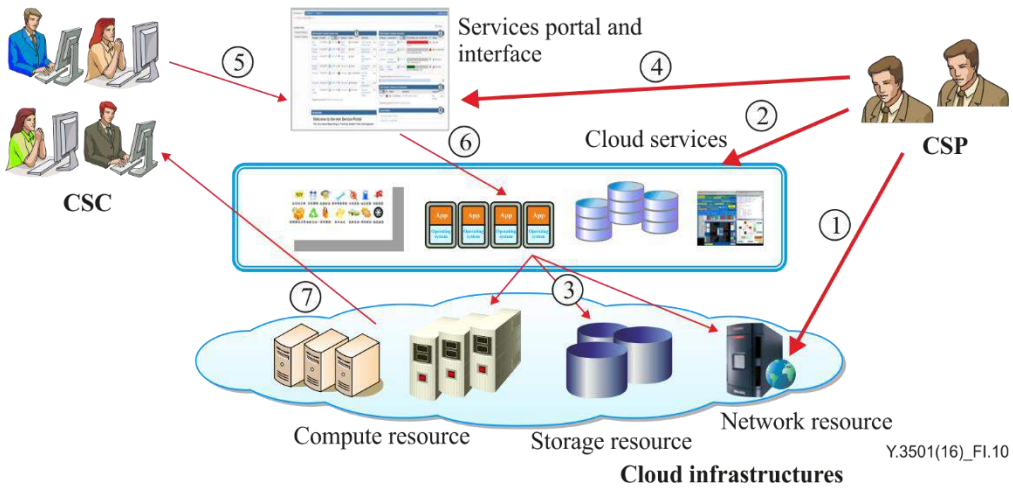
Use case	
Name	Inter-cloud computing use case for intermediation
Abstract	A CSP intermediates services from other CSPs to provide a service to the CSC.
Actors	CSP, CSC
Figure	
Pre-conditions (optional)	
Post-conditions	– A CSP selects a service from other CSPs' services and intermediates them to a CSC. – A CSP creates a new service by integrating several services in other CSPs and intermediates them to a CSC.
Requirements	– On-demand assignment of cloud resource – Inter-cloud computing service intermediation

I.9 End-to-end cloud resource management use case

Use case	
Name	End-to-end cloud resource management use case
Abstract	A CSC uses a service offered by multiple CSPs and/or CSNs, one of which supports customer services. In order to deliver customer services properly, the CSN manages end-to-end health and QoS of the service offered by a CSP which can integrate several base services offered by multiple CSPs.
Actors	CSC, CSP, CSN
Figure	 As shown in the above figure, this problem requires visibility into CSP2's management systems delivering the voice application service, as well as similar CSP's management systems. When the voice application customer calls into CSP2 support, then the CSP2 support person should have visibility into the health and welfare of the CSP1's voice application service, its underlying cloud infrastructure, as well as the local service provider's network management systems relevant to the voice application service.

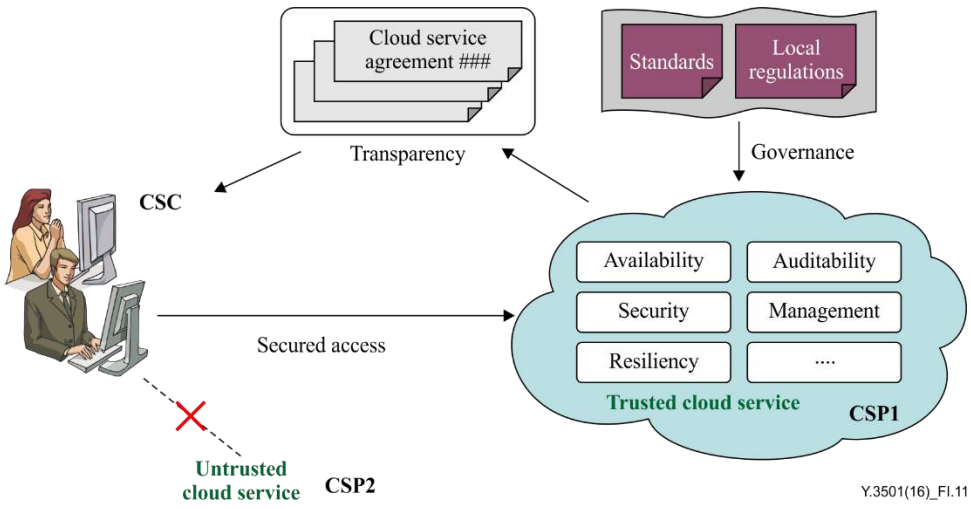
Use case	
Pre-conditions	In this service syndication example involving multiple clouds, voice application is being provided as SaaS to a CSP that is bundling it with other services and reselling a package to a CSC. Although a voice application service provider may run a global data network, it does not own the carrier's network and enterprise infrastructures that actually connect the cloud and network services to end-user devices. A local service provider might provide an IP network service to provide an optimized voice application experience for an enterprise customer's employees using the voice application service. In this use case, there are the two types of connection paths, namely a service delivery path and a service management path. When the CSC is experiencing a problem with the voice application service, the responsibility for the diagnostics, management and resolution of the problem involves more than one service provider. End-to-end resource management cannot require a major system integration effort with each new service deployment. In order for the composite cloud computing services to work effectively, all the prerequisite services of both the CSP1 and CSP2 must function properly.
Post-conditions	Voice application service is restored rapidly and easily. End-to-end resource management of components that deliver the voice application customer service support and the administrative, provisioning, service assurance and billing that make up a complete voice application service is necessary.
Requirements	– Manageability for a single cloud service – Manageability for multiple cloud services

I.10 Cloud infrastructure use case

Use case	
Name	Cloud infrastructure use case
Abstract	The CSP uses cloud infrastructure which consists of compute, storage and network resources to deploy and deliver any kinds of cloud services. The CSC accesses and uses cloud services deployed in and delivered by cloud infrastructure.
Roles	CSC, CSP
Figure	

Use case	
Pre-conditions (optional)	– ① A CSP builds a cloud infrastructure with cloud resources including compute, storage and network resources. – ②,③ The CSP allocates and configures related compute, storage and network resources in the cloud infrastructure needed for deploying any kind of cloud services through resource orchestration functions. – ④ The CSP publishes the deployed cloud services in the catalogue of the cloud service portal. – ⑤ A CSC accesses the cloud services published by the CSP through service portals or service interfaces which are protected by appropriate security mechanisms. – ⑥ Related cloud resources and capabilities have been invoked to respond to the CSC's access and interaction.
Post-conditions	– ⑦ The CSP manages and monitors pooled compute, storage and network resources in the cloud infrastructure.
Requirements	– Resource provisioning – Resource abstraction and control

I.11 Trusted cloud service use case

Use case	
Name	Trusted cloud service use case
Abstract	The CSP provides trusted cloud service which satisfies a set of requirements and transparency for governance, management and security to provide CSC confidence in using the cloud service.
Roles	CSC, CSP
Figure	
Pre-conditions (optional)	– The CSC requests a trusted cloud service: • The CSP1 offers the same cloud services as CSP2, but CSP2 does not meet trusted cloud service requirements. • The CSC gets effective cloud service information from CSP1. • The CSC does not have effective cloud service information from CSP2. – The CSP1 negotiates a cloud service agreement with the CSC before providing a cloud service, while CSP2 does not.

Use case	
Post-conditions (optional)	– The CSP 1 provides a trusted cloud service which meets the needs of the CSC. – The CSP 1 ensures PII protection of the CSC. – The CSP 1 ensures that the CSC can control and manage their application and data. – The CSP 1 provides a secure access to the CSC. – The CSC uses the trusted cloud service from CSP 1. – The CSC no longer uses the cloud service from CSP 2.
Requirements	– Governance for trusted cloud service – Management for trusted cloud service – Resiliency for trusted cloud service – Availability for trusted cloud service – Auditability for trusted cloud service – Security – Service agreement for trusted cloud service.

Appendix II

Methodology and edition plan of this Recommendation

(This appendix does not form an integral part of this Recommendation.)

This Recommendation adopts a use-case-driven approach. Use cases are selected and elaborated first. Based on these use cases, relevant requirements are derived. As an example shown in Figure II.1, one use case may derive multiple requirements.

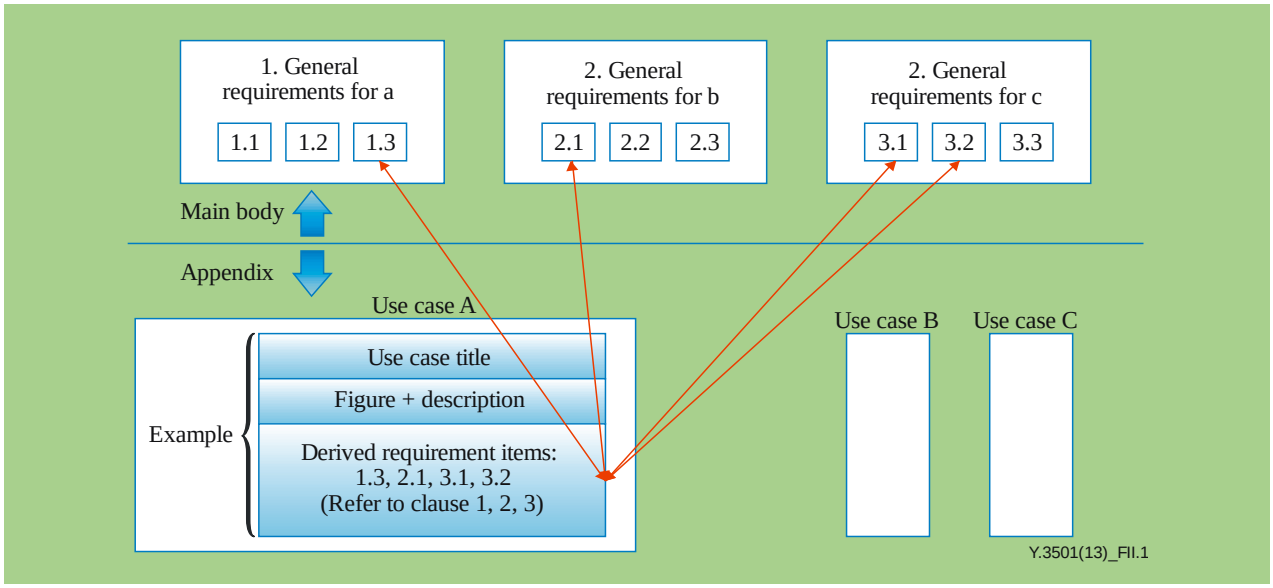


Figure II.1 – Methodology including mapping of use cases and requirements

The use-case-driven approach may also ease the preparation of future editions of this Recommendation. As explained in Figure II.2, a new edition will include new use cases with derived new requirements.

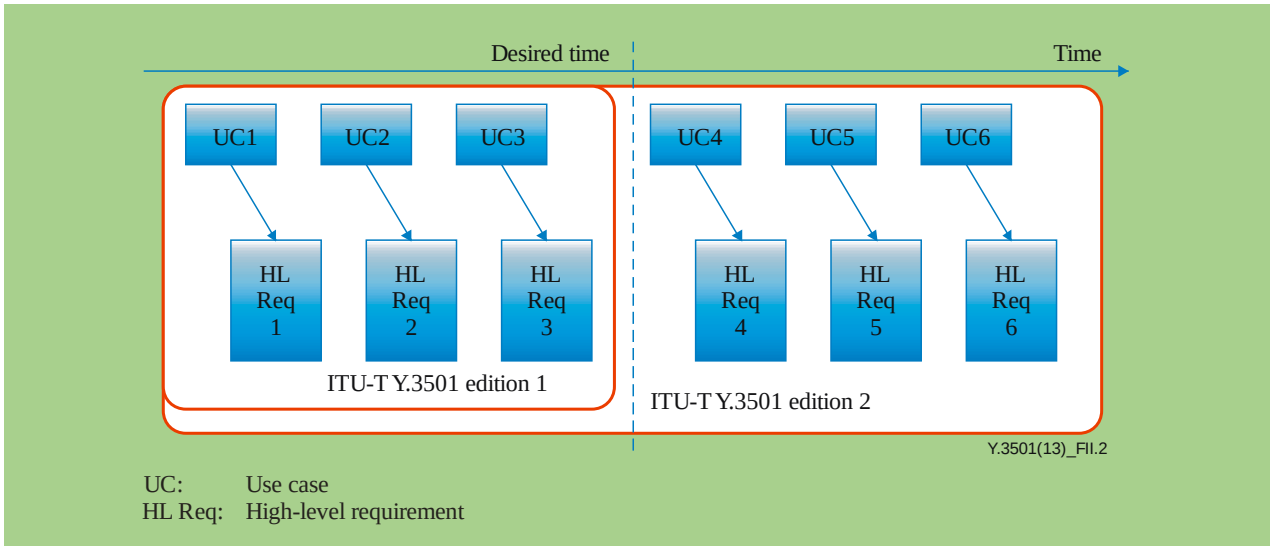


Figure II.2 – Editions of this Recommendation

NOTE – For the sake of readability, this Recommendation describes the requirements with short titles. Exact description of short titles is provided in relevant clauses of this Recommendation.

Table II.1 presents the edition plan of this Recommendation based on the progress of the corresponding content.

Table II.1 – Edition plan of this Recommendation

Scope		Edition 1	Edition2	Edition3
General requirements for cloud computing		O	Extended	Extended
General requirements for IaaS		O	Extended	Extended
General requirements for NaaS		O	Extended	Extended
General requirements for DaaS		O	Extended	Extended
General requirements for PaaS			O	Extended
General requirements for CaaS			O	Extended
General requirements for BDaaS			O	Extended
General requirements for SaaS				O
General requirements for Inter-cloud		O	Extended	Extended
General requirements for end-to-end cloud resource management		O	Extended	Extended
General requirements for cloud infrastructure		O	Extended	Extended
General requirements for Trusted cloud service			O	Extended
Others general requirements				O
Security consideration		O	Extended	Extended
Use case	Generic use cases	O	Extended	Extended
	IaaS general use case	O	Extended	Extended
	NaaS general use case	O	Extended	Extended
	DaaS general use case	O	Extended	Extended
	PaaS general use case		O	Extended
	CaaS general use case		O	Extended
	BDaaS use case		O	Extended
	SaaS general use case			O
	Inter-cloud general use case	O	Extended	Extended
	End-to-end cloud resource management use case	O	Extended	Extended
	Cloud infrastructure use case	O	Extended	Extended
	Trusted cloud service use case		O	Extended
	Other use cases			O
NOTE – The mark "O" indicates initial requirements and use cases are prepared, "extended" indicates additional requirements and use cases will be provided.				


24
@
24

Information technology – Cloud computing – Reference architecture

Rec. ITU-T Y.3502 (2014) | ISO/IEC 17789:2014

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Summary

Rec. ITU-T Y.3502 | ISO/IEC 17789 provides the reference architecture for cloud computing, which includes the cloud computing roles, cloud computing activities, and the cloud computing functional components and their relationships.

Table of Contents

1 Scope

This Recommendation | International Standard specifies the cloud computing reference architecture (CCRA). The reference architecture includes the **cloud computing roles**, **cloud computing activities**, and the **cloud computing functional components** and their relationships.

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

2.1 Identical Recommendations | International Standards

– Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary*.

2.2 Additional references

– ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy framework*.

3 Definitions

For the purposes of this Recommendation | International Standard, the terms and definitions in Rec. ITU-T Y.3500 | ISO/IEC 17788 and the following definitions apply.

3.1 Terms defined elsewhere

The following term is defined in ISO/IEC/IEEE 42010:

3.1.1 architecture: Fundamental concepts or properties of a system in its environment embodied in its elements, relationships and in the principles of its design and evolution.

The following term is defined in ISO/IEC 29100:

3.1.2 personally identifiable information (PII): Any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal.

NOTE – To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other **party**, to identify that natural person.

3.2 Terms defined in this Recommendation | International Standard

This Recommendation | International Standard defines the following terms:

3.2.1 activity: A specified pursuit or set of tasks.

3.2.2 cloud service product: A cloud service, allied to the set of business terms under which the cloud service is offered.

NOTE – Business terms can include pricing, rating and service levels.

3.2.3 functional component: A functional building block needed to engage in an **activity** (clause 3.2.1), backed by an implementation.

3.2.4 peer cloud service: A **cloud service** of one **cloud service provider** which is used as part of a **cloud service** of one or more other **cloud service providers**.

3.2.5 **peer cloud service provider**: A **cloud service provider** who provides one or more **cloud services** for use by one or more other **cloud service providers** as part of their **cloud services**.

3.2.6 **product catalogue**: A listing of all the **cloud service products** (clause 3.2.2) which **cloud service providers** make available to **cloud service customers**.

3.2.7 **role**: A set of **activities** (clause 3.2.1) that serves a common purpose.

3.2.8 **service catalogue**: A listing of all the cloud services of a particular **cloud service provider**.

3.2.9 **sub-role**: A subset of the **activities** (clause 3.2.1) of a given **role** (clause 3.2.7).

4 Abbreviations

For the purposes of this Recommendation | International Standard, the following abbreviations apply:

API	Application Programming Interface
CaaS	Communications as a Service
CCRA	Cloud Computing Reference Architecture
CPU	Central Processing Unit
CS	Cloud Service
CSC	Cloud Service Customer
CSN	Cloud Service partner
CSP	Cloud Service Provider
IaaS	Infrastructure as a Service
ICT	Information and Communication Technology
KPI	Key Performance Indicator
MSA	Master Service Agreement
NaaS	Network as a Service
PaaS	Platform as a Service
PII	**Personally Identifiable Information**
QoS	Quality of Service
RAM	Random Access Memory
SaaS	Software as a Service
SLA	Service Level Agreement
ToS	Terms of Service
T&C	Terms and Conditions
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VM	Virtual Machine

5 Conventions

The following conventions apply:

1) Diagrams are used throughout this Recommendation | International Standard to help illustrate the CCRA. Figure 5-1 provides the conventions used regarding the content of the diagrams.

NOTE – In Figure 5-1, "Aspect" is to be understood as referring to "Cross-cutting aspect".

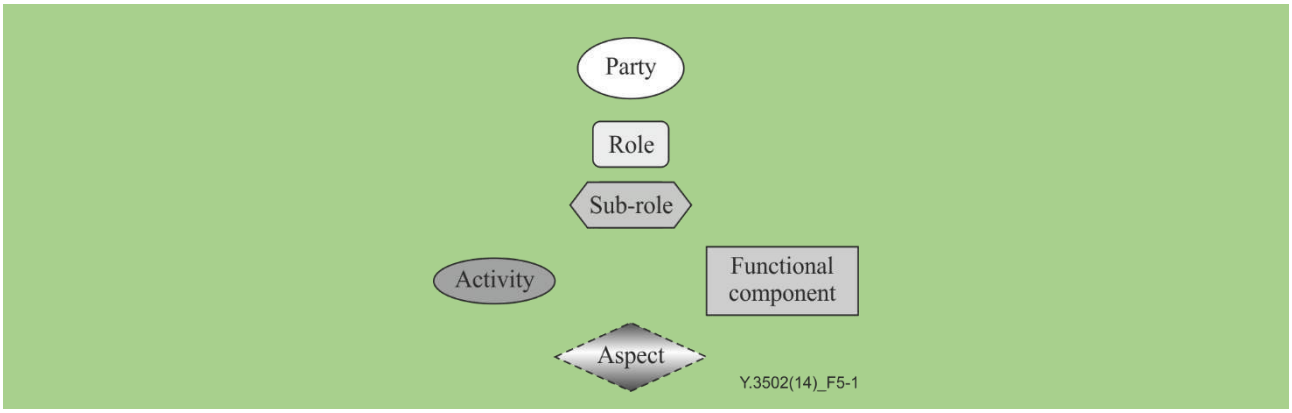


Figure 5-1 – Legend to the diagrams used throughout this Recommendation | International Standard

2) This CCRA uses the term "ICT" and "ICT systems", where the abbreviation ICT stands for "information and communication technology", as defined in clause 3.1332 of ISO/IEC/IEEE 24765. This term is used to make it clear that the CCRA covers not only the compute and storage technologies associated with computer systems, but also the communication networks that link systems together.

3) References to terms defined in clause 3 and in Rec. ITU-T Y.3500 | ISO/IEC 17788 are shown in bold.

6 Cloud computing reference architecture goals and objectives

Cloud computing is a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on demand. See Rec. ITU-T Y.3500 | ISO/IEC 17788.

The CCRA presented in this Recommendation | International Standard provides an architectural framework that is effective for describing the **cloud computing roles**, **sub-roles**, **cloud computing activities**, cross-cutting aspects, as well as the functional architecture and **functional components** of **cloud computing**.

The CCRA serves the following goals:

- to describe the community of stakeholders for **cloud computing**;
- to describe the fundamental characteristics of **cloud computing** systems;
- to specify basic **cloud computing activities** and **functional components**, and describe their relationships to each other and to the environment;
- to identify principles guiding the design and evolution of the **CCRA**.

The CCRA supports the following important standardization objectives:

- to enable the production of a coherent set of international standards for **cloud computing;**
- to provide a technology-neutral reference point for defining standards for **cloud computing**;
- to encourage openness and transparency in the identification of **cloud computing** benefits and risks.

The CCRA focuses on the requirements of "what" **cloud services** provide and not on "how to" design cloud-based solutions and implementations. The CCRA does not represent the system architecture of a specific **cloud computing** system, although it could put constraints on a specific system. The CCRA is not tied to any specific vendor products, services or reference implementation; nor does it define prescriptive solutions that inhibit innovation.

The CCRA is also intended to:

- facilitate the understanding of the operational intricacies of **cloud computing**;
- illustrate and provide understanding of various **cloud services** and their provisioning and use;
- provide a technical reference to enable the international community to understand, discuss, categorize and compare **cloud services**;
- be a tool for describing, discussing, and for developing a system-specific architecture using a common framework of reference;
- facilitate the analysis of candidate standards in areas including security, **interoperability**, portability, **reversibility**, reliability and service management, and support analysis of reference implementations.

7 Reference architecture concepts

This Recommendation | International standard defines a CCRA that can serve as a fundamental reference point for **cloud computing** standardization and which provides an overall framework for the basic concepts and principles of a **cloud computing** system.

This clause provides an overview of the architectural approaches that are used in this Recommendation | International standard.

7.1 CCRA architectural views

Cloud computing systems can be described using a viewpoint approach.

Four distinct viewpoints are used in the CCRA (see Figure 7-1):

- user view;
- functional view;
- implementation view; and
- deployment view.

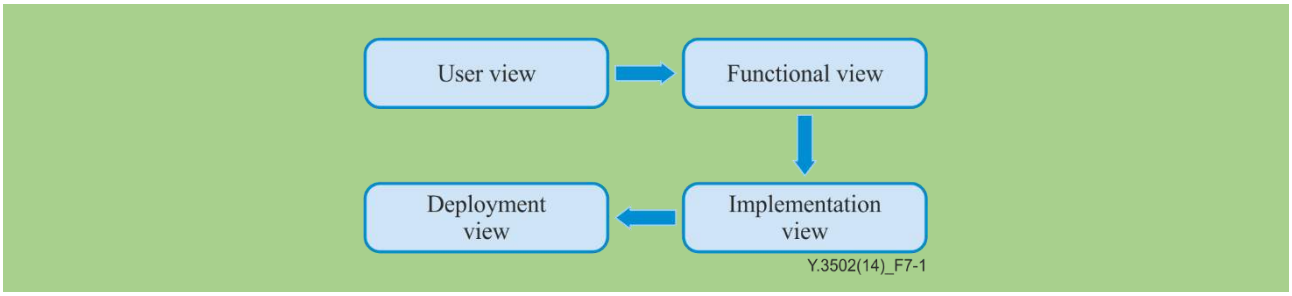


Figure 7-1 – Transformations between architectural views

Table 7-1 provides a description of each of these views.

Table 7-1 – CCRA views

CCRA view	Description of the CCRA view	Scope
User view	The system context, the **parties**, the **roles**, the **sub-roles** and the **cloud computing activities**	Within scope
Functional view	The functions necessary for the support of **cloud computing activities**	Within scope
Implementation view	The functions necessary for the implementation of a **cloud service** within service parts and/or infrastructure parts	Out of scope

Table 7-1 – CCRA views

CCRA view	Description of the CCRA view	Scope
Deployment view	How the functions of a **cloud service** are technically implemented within already existing infrastructure elements or within new elements to be introduced in this infrastructure	Out of scope
NOTE – While details of the user view and functional view are addressed within this Recommendation | International Standard, the implementation and deployment views are related to technology and vendor-specific **cloud computing** implementations and actual deployments, and are therefore out of the scope of this Recommendation | International Standard.		

Figure 7-2 shows the transition from the user view to the functional view. Details are presented in clause 7.4.

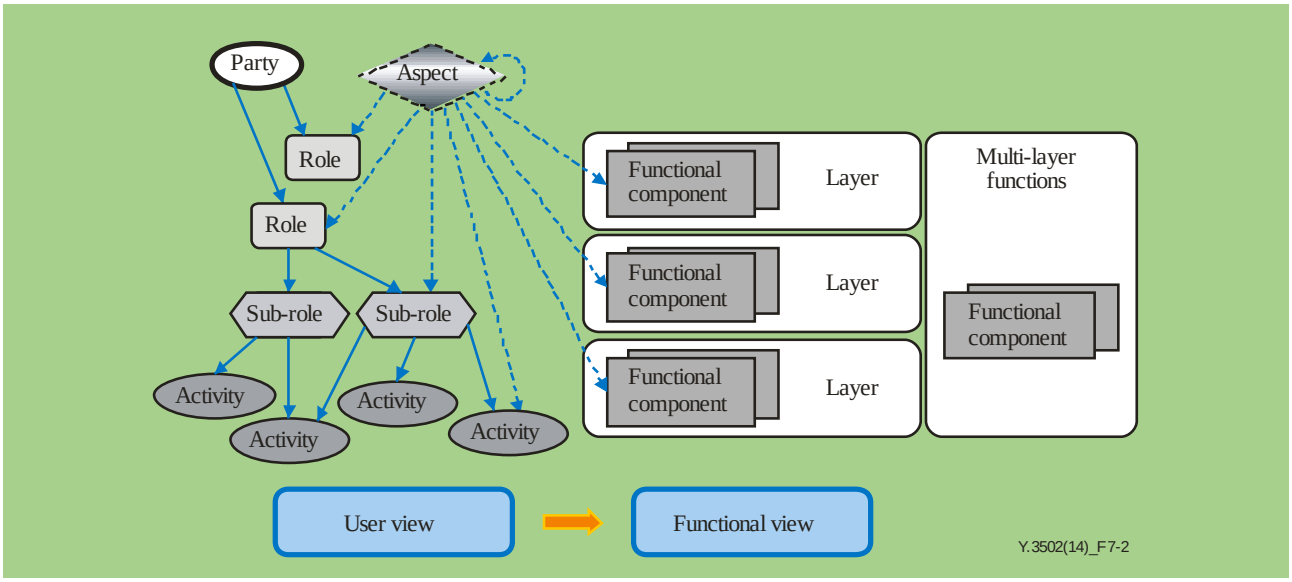


Figure 7-2 – Transition from user view to functional view

7.2 User view of cloud computing

The user view addresses the following **cloud computing** concepts:

- **cloud computing activities**;
- **roles** and **sub-roles**;
- **parties**;
- **cloud services**;
- **cloud deployment models**;
- cross-cutting aspects.

Figure 7-3 illustrates the entities that are defined for the user view.

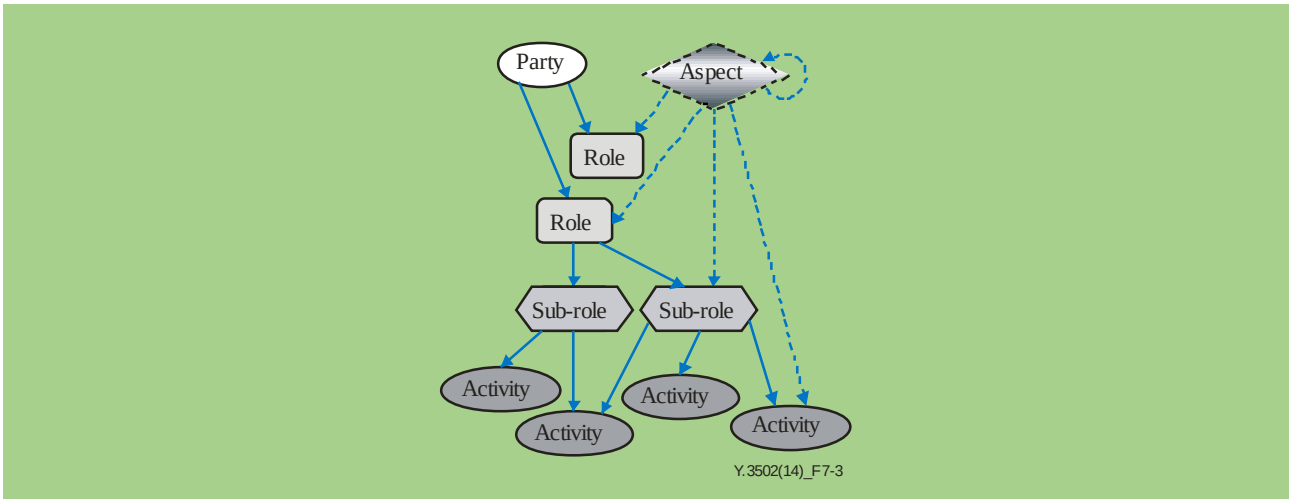


Figure 7-3 – User view entities

7.2.1 Cloud computing activities

A **cloud computing activity** is defined as a specified pursuit or set of tasks.

Cloud computing activities need to have a purpose and deliver one or more outcomes.

Activities in a **cloud computing** system are conducted using **functional components** (see clause 7.3.1).

Cloud computing activities are identified and described in more detail in clause 8.

7.2.2 Roles and sub-roles

A **role** is a set of **cloud computing activities** that serve a common purpose.

In the CCRA, three **roles** have been defined:

- **cloud service customer (CSC)**: A **party** which is in a business relationship for the purpose of using **cloud services**.
- **cloud service provider (CSP)**: A **party** which makes **cloud services** available.
- **cloud service partner (CSN)**: A **party** which is engaged in support of, or auxiliary to, **activities** of either the **cloud service provider** or the **cloud service customer**, or both.

A **sub-role** is a subset of the **cloud computing activities** for a given **role**.

Different **sub-roles** can share the **cloud computing activities** associated with a given **role**.

Descriptions of the **cloud computing roles** and **sub-roles** are provided in clause 8.

7.2.3 Parties

A **party** is a natural person or legal person, whether or not incorporated, or a group of either. **Parties** in a **cloud computing** system are its stakeholders.

A **party** can assume more than one **role** at any given point in time and can engage in a specific subset of **activities** of that **role**. Examples of parties include, but are not limited to, large corporations, small and medium sized enterprises, government departments, academic institutions and private citizens.

7.2.4 Cloud services

Cloud services are the essential elements of **cloud computing. Cloud services** are covered in Rec. ITU-T Y.3500 | ISO/IEC 17788. This clause provides a summary.

Cloud services can be described in terms of the **cloud capabilities types** which they offer, based on the resources provided by the **cloud service**. There are three **cloud capabilities types**:

- **application capabilities type**;
- **platform capabilities type**;
- **infrastructure capabilities type**.

Cloud capabilities types and **cloud service categories** are covered in Rec. ITU-T Y.3500 | ISO/IEC 17788.

Cloud services are also grouped into categories, where each category is a group of **cloud services** that possess a common set of qualities. The services in these categories can include capabilities from one or more of the **cloud capabilities types** above.

Representative **cloud service categories** include:

- **Infrastructure as a service (IaaS)**;
- **Platform as a service (PaaS)**;
- **Software as a service (SaaS)**;
- **Network as a service (NaaS)**.

Other **cloud service categories** are described in Rec. ITU-T Y.3500 | ISO/IEC 17788.

7.2.5 Cloud deployment models

Cloud deployment models are covered in Rec. ITU-T Y.3500 | ISO/IEC 17788. This clause provides a summary.

Cloud deployment models are a way in which **cloud computing** can be organized based on the control and sharing of physical or virtual resources.

The **cloud deployment models** include:

- **public cloud**;
- **private cloud**;
- **community cloud**;
- **hybrid cloud**.

7.2.6 Cross-cutting aspects

Cross-cutting aspects are behaviours or capabilities which need to be coordinated across **roles** and implemented consistently in a **cloud computing** system.

Cross-cutting aspects can be shared and can impact multiple **roles**, **cloud computing activities** and **functional components**.

Cross-cutting aspects apply to multiple individual **roles** or **functional components**.

An example of a cross-cutting aspect is security.

A description of the cross-cutting aspects is provided in clause 8.5.

7.3 Functional view of cloud computing

The functional view is a technology-neutral view of the functions necessary to form a **cloud computing** system. The functional view describes the distribution of functions necessary for the support of **cloud computing activities**.

The functional architecture also defines the dependencies between functions.
The functional view addresses the following **cloud computing** concepts:

- **functional components**;
- functional layers; and
- multi-layer functions.

Figure 7-4 illustrates the concepts of functions, layers and **functional components**.

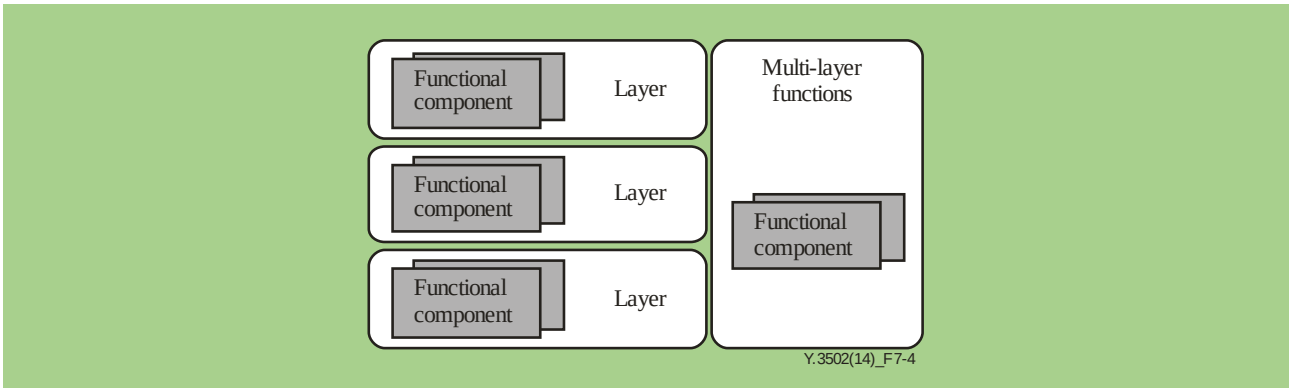


Figure 7-4 – Functional layering

The **cloud computing** functional architecture is described in clause 9.1.

7.3.1 Functional components

A **functional component** is a functional building block needed to engage in an **activity**, backed by an implementation.

The capabilities of a **cloud computing** system are fully defined by the set of implemented **functional components**.

Functional components are further described in clause 9.2.

7.3.2 Functional layers

A layer is a set of **functional components** that provide similar capabilities or serve a common purpose.

The functional architecture is partially layered (i.e., has layers and a set of multi-layer functions).

There are four distinct layers defined in the CCRA:

- user layer, which includes **functional components** that support the **cloud computing activities** of **cloud service customers** and **cloud service partners**;
- access layer, which includes **functional components** that facilitate function distribution and interconnection;
- service layer, which includes **functional components** that provide the **cloud services** themselves plus related administration and business capabilities, and the orchestration capabilities necessary to realize them;
- resource layer, which includes the **functional components** that represent the resources needed to implement the **cloud computing** system.

Note that not all layers or **functional components** are necessarily instantiated in a specific **cloud computing** system.

7.3.3 Multi-layer functions

The multi-layer functions include **functional components** that provide capabilities that are used across multiple functional layers.

Multi-layer functions are grouped into subsets.

The following subsets of multi-layer functions are defined:

- development support;
- integration;
- security systems;
- operational support systems;
- business support systems.

Functional components of the multi-layer functions are described in clause 9.2.5.

7.4 Relationship between the user view and the functional view

Figure 7-5 illustrates how the user view provides the set of **cloud computing activities** that are represented within the functional view (and realized using the technologies of the implementation view).

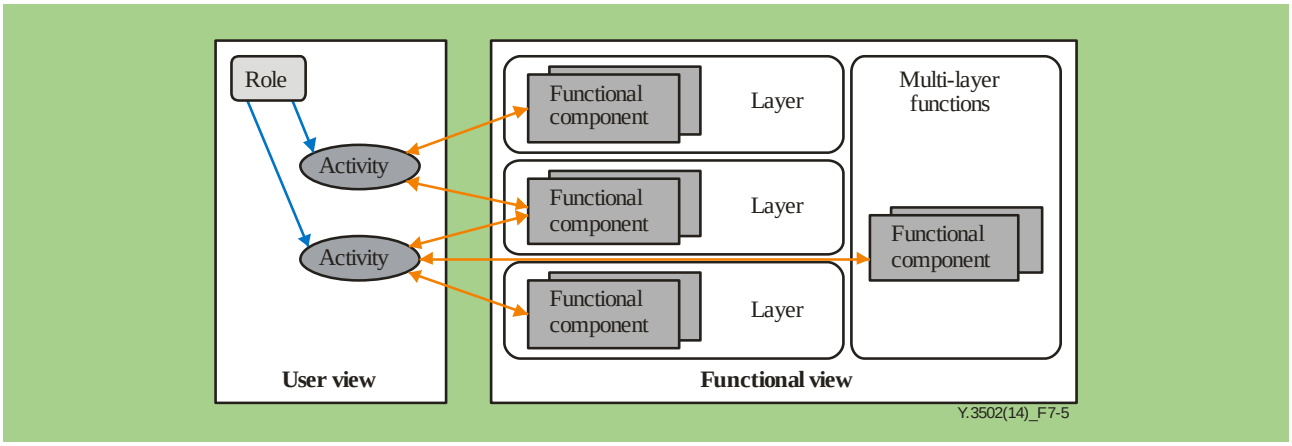


Figure 7-5 – From user view to functional view

Further details on the relationship between the user view and functional view can be found in clause 10.

7.5 Relationship of the user view and functional view to cross-cutting aspects

Cross-cutting aspects, as their name implies, apply across both the user view and across the functional view of **cloud computing**.

Cross-cutting aspects apply to **roles** and **sub-roles** in the user view and they directly or indirectly affect the **activities** which those **roles** perform.

Cross-cutting aspects also apply to the **functional components** within the functional view, which are used when performing the **activities** described in the user view.

Cross-cutting aspects of **cloud computing** described in clause 8.5 include:

- auditability;
- **availability**;
- governance;
- **interoperability**;
- maintenance and versioning;
- performance;
- portability;
- protection of **personally identifiable information**;
- regulatory;
- resiliency;
- **reversibility**;
- security;
- service levels and **service level agreement**.

7.6 Implementation view of cloud computing

While details of the user view and functional view are addressed within this Recommendation | International Standard, the implementation view is out of the scope of this Recommendation | International Standard.

7.7 Deployment view of cloud computing

While details of the user view and functional view are addressed within this Recommendation | International Standard, the deployment view is out of the scope of this Recommendation | International Standard.

8 User view

8.1 Introduction to roles, sub-roles and cloud computing activities

Given that distributed services and their delivery are at the core of **cloud computing**, all **cloud computing** related **activities** can be categorized into three main groups: **activities** that use services, **activities** that provide services and **activities** that support services.

This clause contains descriptions of some of the common **roles** and **sub-roles** associated with **cloud computing**.

It is important to note that a **party** can play more than one **role** at any given point in time. When playing a **role**, the **party** can restrict itself to playing one or more **sub-roles**. **Sub-roles** are a subset of the **cloud computing activities** of a given **role**.

As shown in Figure 8-1, the **roles** of **cloud computing** are:

- **cloud service customer** (clause 8.2);
- **cloud service provider** (clause 8.3);
- **cloud service partner** (clause 8.4).

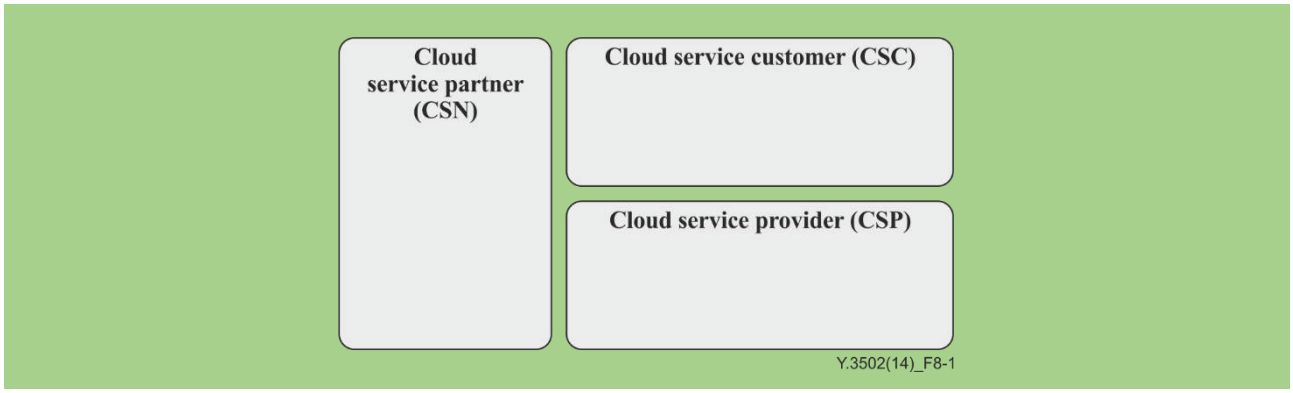


Figure 8-1 – Cloud computing roles

Figure 8-2 shows the **roles** of **cloud computing**, with their associated **sub-roles**. Each of the **sub-roles** shown in the figure is described in more detail in the following clauses.

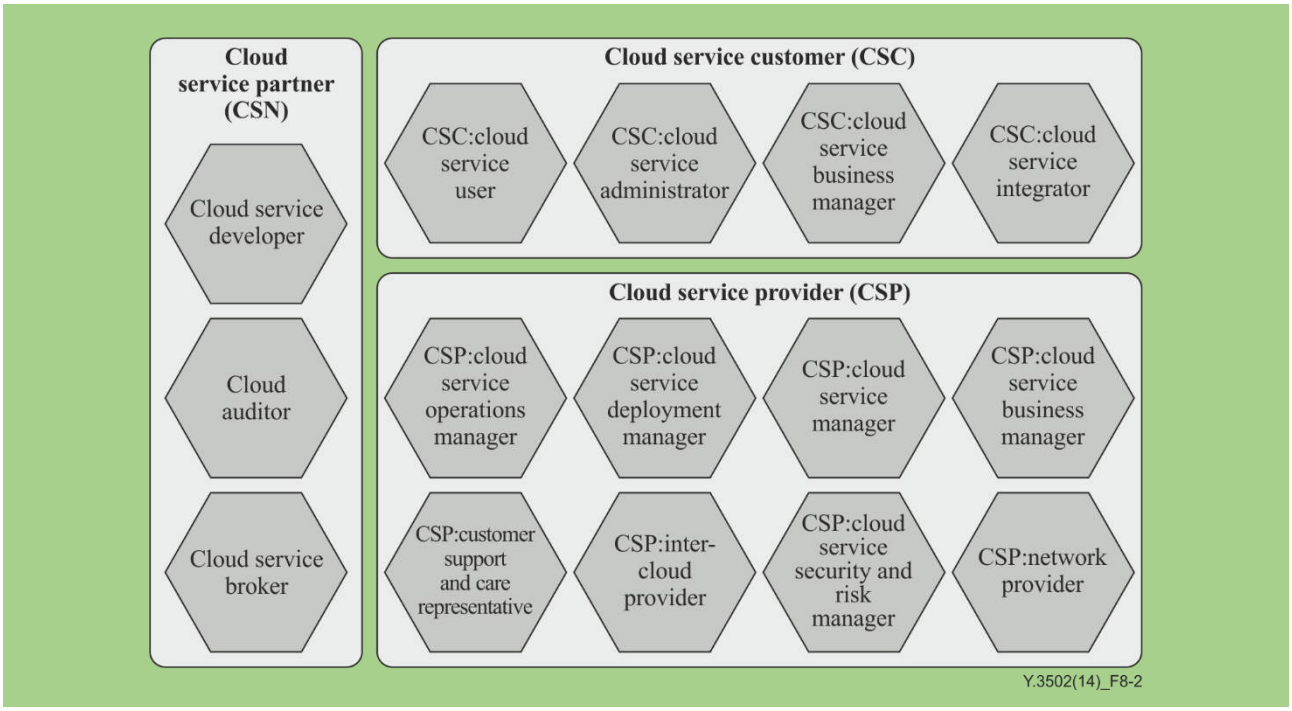


Figure 8-2 – Roles and sub-roles

8.2 Cloud service customer

8.2.1 Role

A **cloud service customer** (CSC) has a business relationship with a **cloud service provider** for the purpose of using **cloud services**. A **cloud service customer** can also have a business relationship with a **cloud service partner** for a variety of purposes.

A **cloud service customer's activities** are included beneath the **sub-roles** described in clauses 8.2.1.1 to 8.2.1.4.

8.2.1.1 CSC:cloud service user

The CSC:cloud service user is a sub-role of **cloud service customer** corresponding to a natural person or an entity acting on their behalf, associated with a **cloud service customer** that uses **cloud services**.

The CSC:cloud service user's **cloud computing activities** include:

- use **cloud service** (clause 8.2.2.1).

8.2.1.2 CSC:cloud service administrator

The CSC:cloud service administrator is a **sub-role** of **cloud service customer,** whose main goal is to ensure the smooth operation of the customer's use of **cloud services,** and that those **cloud services** are running well with the customer's existing ICT systems and applications. The CSC:cloud service administrator oversees all the operational processes relating to the use of **cloud services** and acts as the focal point for technical communications between the **cloud service customer** and the **cloud service provider**.

The CSC:cloud service administrator's **cloud computing activities** include:

- perform service trial (clause 8.2.2.2);
- monitor service (clause 8.2.2.3);
- administer service security (clause 8.2.2.4);
- provide billing and usage reports (clause 8.2.2.5);
- handle problem reports (clause 8.2.2.6);
- administer tenancies (clause 8.2.2.7).

8.2.1.3 CSC:cloud service business manager

The CSC:cloud service business manager is a **sub-role** of **cloud service customer** which aims to meet the business goals of the **cloud service customer** through the acquisition and use of **cloud services** in a cost efficient way. The main responsibilities of the CSC:cloud service business manager concern financial and legal aspects of the use of **cloud services**, including approval, on-going ownership and accountability.

The CSC:cloud service business manager's **cloud computing activities** include:

- perform business administration (clause 8.2.2.8);
- select and purchase service (clause 8.2.2.9);
- request audit report (clause 8.2.2.10).

8.2.1.4 CSC:cloud service integrator

The CSC:cloud service integrator is a **sub-role** of **cloud service customer** which is responsible for the integration of **cloud services** with a **cloud service customer**'s existing ICT systems, including application function and data.

The CSC:cloud service integrator's **cloud computing activities** include:

- connect ICT systems to **cloud services** (clause 8.2.2.11).

8.2.2 Cloud computing activities

The **cloud computing activities** which relate to the **sub-roles** of **cloud service customer** are shown in Figure 8-3.

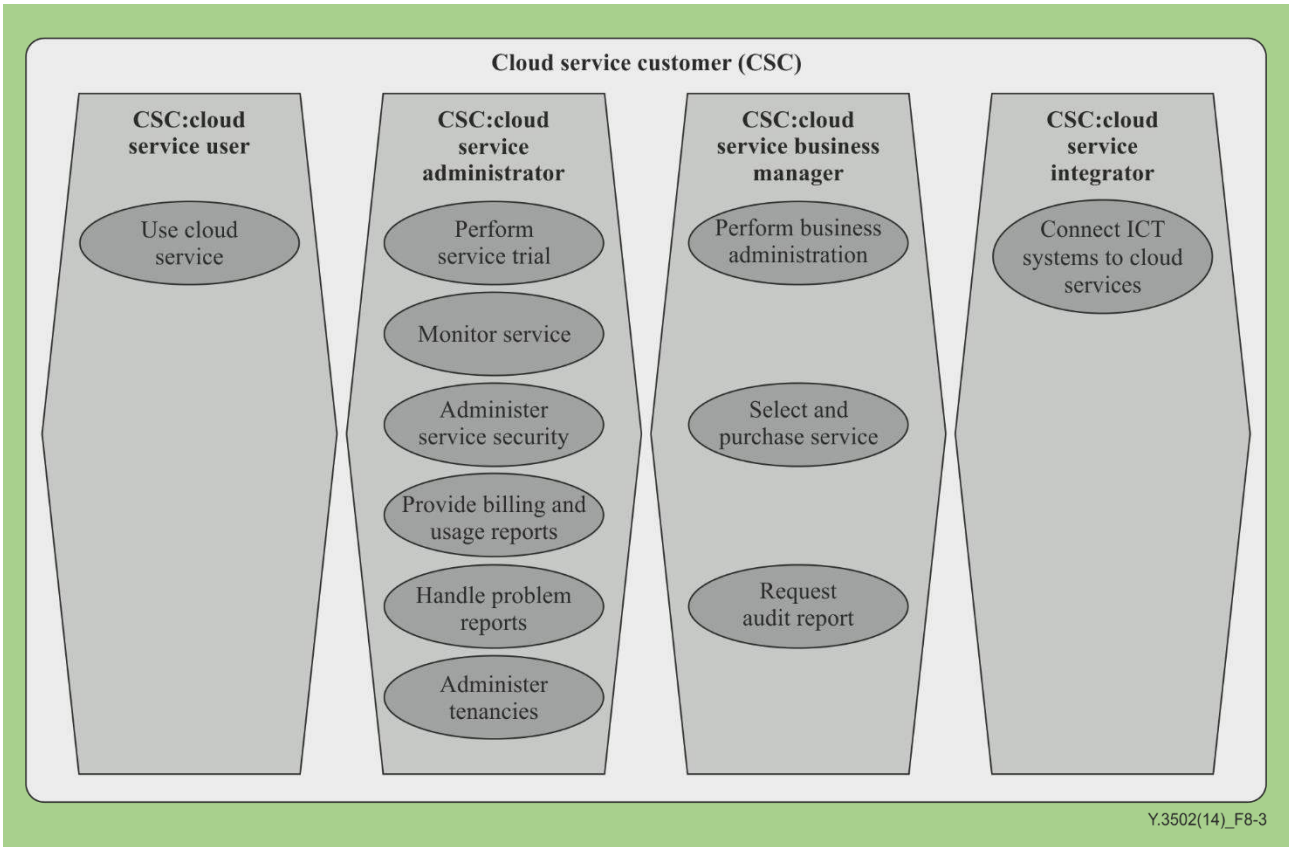


Figure 8-3 – Cloud computing activities relating to cloud service customer sub-roles

8.2.2.1 Use cloud service

The use **cloud service activity** involves using the services of a **cloud service provider** in order to accomplish some tasks.

The use **cloud service activity** typically involves:

1) the provision of user credentials to enable the **cloud service provider** to authenticate the user and grant access to the **cloud service**;
2) the invocation of the **cloud service**, which then operates and delivers its specified outcomes.

8.2.2.2 Perform service trial

The perform service trial **activity** involves using the services of a **cloud service provider** in order to ensure that the **cloud service** is fit for the **cloud service customer**'s business needs. The **cloud services** are used on a trial basis, with mutual agreement and understanding between the **cloud service provider** and **cloud service customer**.

The perform service trial **activity** involves:

1) The provision of the user credentials to enable the **cloud service provider** to authenticate the user and grant access to the "trial" **cloud service**;
2) The invocation of the "trial" **cloud service**, which can be tested by the **cloud service customer** for business purposes.

8.2.2.3 Monitor service

The monitor service **activity** monitors the delivered service quality with respect to service levels as defined in the **service level agreement** (**SLA)** between **cloud service customer** and **cloud service provider**. This **activity** utilizes intrinsic monitoring functions of the cloud system. This **activity** involves:

- keeping track of how much use is being made of each **cloud service**, and by which users. This includes assurance that the use is appropriate;
- monitoring the integration of the **cloud services** with customer's existing ICT systems to ensure that business goals are being met;
- defining measurement points and performance indicators related to the service in question (e.g., service **availability**, service outage frequency, mean time to repair, responsiveness of the provider's help desk, etc.);
- monitoring, analysing and archiving of these indicator data;
- comparing the actual service quality that is delivered with the agreed service quality.

8.2.2.4 Administer service security

The administer service security **activity** involves:

- ensuring appropriate security for **cloud service customer data** that is placed into a **cloud computing** environment
- putting in place plans for data backup and recovery, and potentially for data duplication and failover;
- administering security policies;
- defining encryption and **integrity** technologies to apply to the **cloud service customer data** both at rest and also in motion;
- defining the handling of any **personally identifiable information (PII)** in the **cloud service customer data**.

8.2.2.5 Provide billing and usage reports

The provide billing and usage reports **activity** involves preparing reports of the usage of **cloud services** by the customer organization and associated reports of the billing/invoice data which relate to that usage. These reports are provided to the CSC:business manager.

8.2.2.6 Handle problem reports

The handle problem reports **activity** involves the customer-side handling of any reported problems associated with the usage of **cloud services.** This includes:

- assessing the impact of each problem;

- troubleshooting to determine the cause(s) of the problem;
- opening a problem report(s) with the **cloud service provider** and tracking to resolution;
- developing workarounds to address the problem;
- escalating problems that are not fixed within agreed timescales or which have serious business impacts.

8.2.2.7 Administer tenancies

The administer tenancies **activity** involves administering the tenancies of the **cloud service customer** with the **cloud service provider**. This **activity** involves:

- configuring and controlling security aspects including user accounts, security **roles**, identities and permissions;
- identifying and controlling data that is shared between users within the tenancy;
- creating and removing **tenants**;
- managing users and allocated resources of **tenants**;
- defining enforcement policies for each **tenant**.

8.2.2.8 Perform business administration

The perform business administration **activity** involves the management of the business aspects of the use of **cloud services** including accounting and financial management. This **activity** includes:

- adjusting business plan to accommodate the use of **cloud services**;
- tracking the use of the services and dealing with accounting and financial management;
- handling billing/invoices received from the **cloud service provider** for the use made of **cloud services**;
- ensuring that billing matches the actual usage of **cloud services** made by the **cloud service customer**;
- making payments to the **cloud service provider**;
- keeping accounts in relation to the use of **cloud services**.

8.2.2.9 Select and purchase service

The select and purchase service **activity** involves:

- examining the **cloud service** offerings of (one or more) **cloud service providers** to determine if the service offered meets the business and technical requirements of the **cloud service customer**. This typically involves the reading of a **product catalogue** and the documentation for each service, which can include technical information about the service and its **SLAs**, plus business information including pricing;
- negotiating the terms for the **cloud service** (if the **cloud service provider** permits variable terms for the service);
- accepting the contract for the **cloud service** and performing registration with the **cloud service provider**.

8.2.2.10 Request audit report

The request audit report **activity** involves the **cloud service customer** requesting the report of an audit of the **cloud service**, typically conforming to a particular audit standard or scheme. The **cloud service customer** can request the report from a **cloud auditor**, or possibly from the **cloud service provider**, although it is expected that the audit report is prepared by an entity independent of the **cloud service provider** both before a purchase is completed and also periodically once the service is in use.

8.2.2.11 Connect ICT systems to cloud services

The connect ICT systems to **cloud services activity** includes the integration between existing ICT systems and **cloud services** and involves the connection of existing ICT component(s) and applications with the target **cloud service**(s) and also the connection of the customer monitoring and management systems with the **cloud service provider 's** monitoring and control of **cloud services**.

The connection of existing ICT components and applications with the target **cloud service**(s) involves:

- assessing the impact of **cloud service**(s) on existing processes, systems and services;
- mapping business data between **cloud service customer's** existing ICT systems and **cloud services**;
- invoking **cloud service** operations from existing ICT components and applications, with the supply of input data and the handling of output data;
- provisioning of access rights for CSC:cloud service users;
- defining and implementing security related requirements, including the **confidentiality** and **integrity** of data flows;
- integrating customer facilities for the administration of user accounts, security **roles**, identities and permissions with the equivalent facilities for the **cloud services**;
- creating and monitoring specific user accounts and identities for the use of management interfaces for **cloud services**;
- integrating logging and security incident management between **cloud services** and **cloud service customer** monitoring and management infrastructure.

8.3 Cloud service provider

8.3.1 Role

A **cloud service provider** (CSP) makes **cloud services** available to **cloud service customers**. This **role** (and all of its **sub-roles**) focuses on the **cloud computing activities** necessary to provide a **cloud service** and the **cloud computing activities** necessary to ensure its delivery to the **cloud service customer**, as well as **cloud service** maintenance.

The **cloud service provider** is responsible for dealing with the business relationship with **cloud service customers**.

A **cloud service provider's activities** are included beneath the **sub-roles** described in clauses 8.3.1.1 to 8.3.1.8.

8.3.1.1 CSP:cloud service operations manager

The CSP:cloud service operations manager is a **sub-role** of **cloud service provider** which is responsible for performing all operational processes and procedures of the **cloud service provider**, ensuring that all services and associated infrastructure meet operational targets.

The CSP:cloud operations manager's **cloud computing activities** include:

- prepare systems (clause 8.3.2.1);
- monitor and administer services (clause 8.3.2.2);
- manage assets and inventory (clause 8.3.2.3);
- provide audit data (clause 8.3.2.4).

8.3.1.2 CSP:cloud service deployment manager

The CSP:cloud service deployment manager is a **sub-role** of **cloud service provider** which has responsibility for the planning of the deployment of a service into production. This includes defining the operational environment for the service, the initial steps for deployment of the service and its dependencies, and the enablement of operations processes which are used during the running of the service.

The CSP:cloud service deployment manager's **cloud computing activities** include:

- define environment and processes (clause 8.3.2.5);
- define and gather metrics (clause 8.3.2.6);
- define deployment steps (clause 8.3.2.7).

8.3.1.3 CSP:cloud service manager

The CSP:cloud service manager is a sub-role of **cloud service provider** which has responsibility for ensuring that the **cloud service provider**'s services are available for use by **cloud service customers**, and that they function correctly and comply with targets specified in the **service level agreement**. The CSP:cloud service manager is also responsible for ensuring the smooth operation of the **cloud service provider**'s business support system and operational support system, as well as the operation of the other functionalities offered to the **cloud service customers** and **cloud service partners** for management, administration and other **cloud computing activities**.

The CSP:cloud service manager's **cloud computing activities** include:

- provide services (clause 8.3.2.8);
- deploy and provision services (clause 8.3.2.9);
- perform service level management (clause 8.3.2.10).

8.3.1.4 CSP:cloud service business manager

The CSP:cloud service business manager is a **sub-role** of **cloud service provider** which has overall responsibility for the business aspects of offering **cloud services** to **cloud service customers**. The CSP:cloud service business manager creates and tracks the business plan, defines the service offering strategy and manages the business relationship with **cloud service customers**.

The CSP:cloud service business manager's **cloud computing activities** include:

- manage business plan to provide **cloud services** (clause 8.3.2.11);
- manage customer relationships (clause 8.3.2.12);
- manage financial processing (clause 8.3.2.13).

8.3.1.5 CSP:customer support and care representative

The CSP:customer support and care representative is a **sub-role** of **cloud service provider** that is the main interface for the **cloud service customer** with the **cloud service provider** and is responsible for reacting to customer issues and queries in a timely and cost efficient way, with the goal of maintaining customer satisfaction with the **cloud service provider** and the **cloud services** offered.

The CSP:customer support and care representative's **cloud computing activities** include:

- handle customer requests (clause 8.3.2.14).

8.3.1.6 CSP:inter-cloud provider

The CSP:inter-cloud provider is a **sub-role** of **cloud service provider** that relies on one or more **peer cloud service providers** to provide part or all of the **cloud services** offered to **cloud service customers** by that CSP:inter-cloud provider. The CSP:inter-cloud provider's main activities are the intermediation, aggregation, arbitrage, peering or federation of **peer cloud service providers' cloud services** and their business and administration capabilities from the **cloud service customer** viewpoint so that the **cloud service customer** only uses the service, business and administration interfaces of the inter-cloud service provider.

The CSP:inter-cloud provider's **cloud computing activities** include:

- manage **peer cloud services** (clause 8.3.2.15);
- perform peering, federation, intermediation, aggregation and arbitrage (clause 8.3.2.16).

8.3.1.7 CSP:cloud service security and risk manager

The CSP:cloud service security and risk manager is a **sub-role** of **cloud service provider** which has the responsibility of ensuring that the **cloud service provider** appropriately manages the risks associated with the development, delivery, use and support of **cloud services**. This includes ensuring that the **information security** policies of the **cloud service customer** and the **cloud service provider** are aligned and meet the security requirements stated in the **SLA**.

The CSP:cloud service security and risk manager's **cloud computing activities** include:

- manage security and risks (clause 8.3.2.17);
- design and implement service continuity (clause 8.3.2.18);
- ensure compliance (clause 8.3.2.19).

8.3.1.8 CSP:network provider

The CSP:network provider is a **sub-role** of **cloud service provider** which is to provide network connectivity and network services for the **cloud service customer**, **cloud service partner** and **cloud service provider**. The CSP:network provider may provide network connectivity between systems within the **cloud service provider**'s data centre, or provide network connectivity between the **cloud service provider**'s systems and systems outside the provider's data centre, for example, **cloud service customer** systems or systems belonging to other **cloud service providers**.

The CSP:network provider's **cloud computing activities** include:

- provide network connectivity (clause 8.3.2.20);
- deliver network services (clause 8.3.2.21);
- provide network management services (clause 8.3.2.22).

The CSP:network provider can also choose to offer dynamic control of network connectivity as an **NaaS**.

8.3.2 Cloud computing activities

The **cloud computing activities** which relate to the **sub-roles** of **cloud service provider** are shown in Figure 8-4.

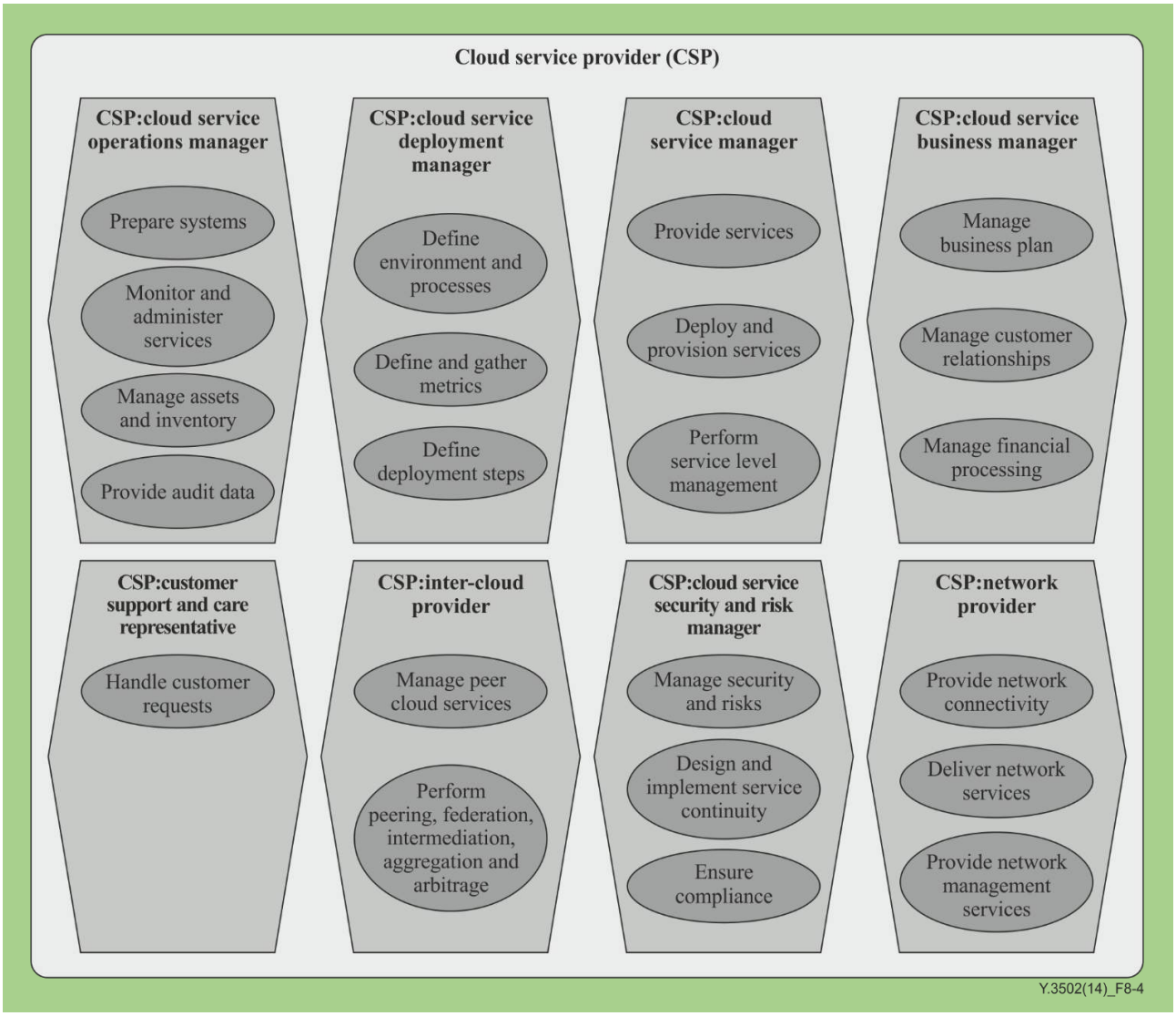


Figure 8-4 – Cloud computing activities relating to cloud service provider sub-roles

8.3.2.1 Prepare systems

The prepare systems **activity** is focused on preparing the systems of the provider's environment for new **cloud service** deployments. This **activity** involves:

- assessing the impact of new service deployments or the increase in use of existing services;
- modifying or expanding the resources in the data centre to meet the needs of new deployments.

8.3.2.2 Monitor and administer services

The monitor and administer services **activity** focuses on monitoring and administering services and their associated infrastructure which includes user and system privileges. This **activity** involves:

- monitoring the services and infrastructure of the **cloud service provider**;
- capturing events and data that are significant to the business of the provider and presenting this data in a form that is significant to the CSP:cloud service business manager. Such information includes items such as the usage of the **cloud services** by **cloud service customers** and the cost of provision of those services;
- administering network infrastructure including routers, domain name servers, IP addresses, virtual private networks (VPNs), firewalls and content filtering;
- allocating and administering storage;
- administering user and system privileges;

- configuring and maintaining operating systems and hypervisors;
- administering a virtualization environment;
- monitoring the behaviour of the ICT environment of the **cloud service provider** to ensure that it is running correctly and that provided **cloud services** are meeting the terms of the **SLA**;
- recording problems, reporting problems appropriately (which can involve a message being sent to one or more customers), and following problem resolution processes until the problem is fixed.

8.3.2.3 Manage assets and inventory

The manage assets and inventory **activity** involves:

- keeping track of all compute, storage, network and software assets and the relationship between them. This includes tracking aspects such as versions and patch levels, plus configuration information, where relevant;
- 'on-boarding' of new assets and disposal of old assets. This can include ensuring that new assets are fit for purpose and have been properly checked from a security and manageability standpoint and can include the disposal of assets that are no longer required. This can include appropriate secure disposal of any assets that might hold data.

8.3.2.4 Provide audit data

The provide audit data **activity** is the collection and provision of data relevant to an audit request, such as that relating to security controls or to service performance. The data requested will depend on the auditing scheme or standard that is being used. This **activity** involves:

- creating and sending appropriate audit information from logs, etc.;
- redacting information from any log records or other data that might contain sensitive information or **PII**.

8.3.2.5 Define environment and processes

The define environment and process **activity** focuses on defining the required technical environment and operational processes used when a service is running. This **activity** involves:

- defining the required technical environment in terms of compute, storage and network resources, the software dependencies including configuration;
- defining policies and processes for scaling up and scaling down the use of resources in response to changing usage demand;
- assuring that the **cloud service** adheres to appropriate standards relating to security and business compliance;
- defining the processes to follow when the service is running, including plans for fixes, upgrades and migration.

8.3.2.6 Define and gather metrics

The define and gather metrics **activity** focuses on defining service level metrics and management. This **activity** involves:

- defining the metrics that are used in relation to the operation of **cloud services**, which are typically reflected in the **SLA** relating to those services;
- designing how the metrics are captured for each **cloud service**;
- defining how the metrics are reported and managed, in particular to ensure that **SLA** targets are met.

8.3.2.7 Define deployment steps

The define deployment steps **activity** focuses on defining the steps for the deployment of services. This **activity** involves describing each of the steps that need to be taken by the operations and support teams in order to get the service implementation deployed and ready for use by **cloud service customers**.

8.3.2.8 Provide services

The provide services **activity** involves all steps required to deliver a **cloud service** to its **cloud service customers**. The provide services **activity** includes accepting and processing service invocations from the user with associated authentication and authorization of the user identity. The processing of a service invocation is done by means of an instance of the service implementation, which can in turn involve the composition and calling of other services as determined by the design and configuration of the service implementation.

The provide services **activity** also involves the following:

- managing the service fault handling process;
- managing the business support system and the operational support system;
- maintaining the service and underlying infrastructure;
- automating system processes;
- managing long term capacity and performance trends;
- installing, configuring and performing maintenance updates on required hardware for compute, storage and network capabilities for the **cloud service provider**'s data centre;
- installing and configuring the software required to run the cloud provider's data centre and support **cloud service** implementations. This includes applying fixes, updates and upgrades to that software, as required.

8.3.2.9 Deploy and provision services

The deploy and provision services **activity** involves getting a service implementation running and making it available at a network end point accessible to the CSC:cloud service users and making it able to handle service requests from users. This activity includes:

- following the deployment processes defined for the service.

NOTE – This activity also covers the processes required to un-deploy and de-provision a cloud service.

8.3.2.10 Perform service level management

The perform service level management **activity** focuses on managing compliance with **SLA** targets. This **activity** involves:

- monitoring the metrics for each service and comparing them with the service targets required by the **SLA** for the service;
- taking action when the metrics do not meet the values required by the **SLA**, to bring the service back into compliance with the **SLA,** for example, by following procedures laid down by the CSP:cloud service deployment manager;
- reporting a problem if compliance cannot be maintained.

8.3.2.11 Manage business plan

The manage business plan **activity** involves:

- defining a service offering, describing the technical aspects of the offering (functional interfaces, **SLAs**,…) and the business aspects of the offering;

  NOTE – When establishing the service offering, the **cloud service provider** can take into account aspects related to the interaction with **peer cloud service providers**.

- creating a business plan which covers the offering of one or more **cloud services** to customers, handling both financial and technical aspects of the services, the target customer set, contracts and **SLAs**, channels to market, sales targets;

- tracking the sales and service usage against the plan to ensure that financial targets are achieved for the **cloud service provider;**
- preparing a business plan and adjusting the business plan to provide **cloud services**.

8.3.2.12 Manage customer relationships

The manage customer relationships activity involves the management of the business relationship of the **cloud service provider** with the **cloud service customer** including:

- creating and maintaining content of a **product catalogue**;
- acquiring customers;
- providing the point of contact for the customer for all business matters;
- discussing and resolving concerns or problems raised by the customer;
- processing change requests (e.g., entitlement changes).

8.3.2.13 Manage financial processing

The manage financial processing **activity** involves:

- handling billing updates or challenges;
- generating billing information and/or an invoice for charges relating to the use of **cloud services** and transmitting the billing information or invoice to the **cloud service customer**;
- handling the receipt of payments from the **cloud service customer** and their accounting.

8.3.2.14 Handle customer requests

The handle customer requests **activity** involves:

- handling support requests, reports and incidents from **cloud service customers**, however received. Customers can be provided with a variety of means to communicate, from forums through email, customer support desk systems or web portals to real-time communication with provider support personnel;

NOTE – Some requests or reports can only require the provision of information or the clarification of details. Other requests and reports can require problem analysis, or they can involve the creation of a change request.

8.3.2.15 Manage peer cloud services

The manage peer **cloud services activity** focuses on managing the usage of **cloud services** of a **peer cloud service provider**. This **activity** involves:

- selecting and using one or more services of a **peer cloud service provider**;
- monitoring and managing the **peer cloud service provider's cloud services** to ensure that they meet agreed **SLA** targets including the reporting and resolution of problems with those services;
- managing the business aspects of the **cloud services** of a **peer cloud service provider**, including the business plan and financial processing;
- keeping track of how much use is being made of each **cloud service** of a **peer cloud service provider**, and by which users, and including assurance that the use is appropriate and within the business plan;
- monitoring the integration of the **cloud services** of a **peer cloud service provider** with service implementations to ensure that business goals are being met;
- coordinating identity and security credentials between the **cloud service customer** and all the **peer cloud service providers**.

8.3.2.16 Perform peering, federation, intermediation, aggregation and arbitrage

The perform peering, federation, intermediation, aggregation and arbitrage **activity** involves the use of **peer cloud service provider's cloud services** in particular ways:

- peering is the use of **cloud services** of a **peer cloud service provider**;

- federation involves using the **cloud services** of a group of **peer cloud service providers** who mutually combine their service capabilities in order to provide the set of **cloud services** required by customers;
- intermediation involves a **cloud service provider** offering a **cloud service** which is based on conditioning or enhancing the **cloud service** of a **peer cloud service provider**. Examples of enhancements include managing access to **cloud services**, providing a **cloud service** application programming interface (API) façade, identity management, performance reporting, enhanced security, and so on;
- aggregation involves a **cloud service provider** offering a **cloud service** which is based on the composition of a set of services provided by **peer cloud service providers**;
- arbitrage involves a **cloud service provider** offering a **cloud service** which is based on selecting one service offering from a group offered by **peer cloud service providers**.

8.3.2.17 Manage security and risks

The manage security and risks **activity** focuses on the management of security and risks associated with the development, delivery, use and support of **cloud services**. This **activity** involves:

- defining **information security** policy – taking into consideration the service requirements, statutory and regulatory requirements and contractual and **SLA** obligations;
- defining **information security** risks relating to the **cloud service** and the approach to those risks that meets the business goals of the **cloud service provider.** A significant point here is that managing **information security** risks has an associated cost and that the provider can take a business position of not handling some risks, instead passing over responsibility for those risks to the **cloud service customer** via the service agreement, in order to address the cost requirements of some part of the marketplace.
- selecting design point and associated **information security** controls required to address risks associated with the service and design point chosen. The controls typically cover a set of categories, such as:
  - identity and access management;
  - discover, categorize, protect data and information assets;
  - information systems acquisition, development and maintenance;
  - secure infrastructure against threats and vulnerabilities;
  - problem and **information security** incident management;
  - security governance and compliance;
  - physical and personnel security;
  - security of networks and communications;
  - isolation (between **tenants** in a multi-tenant situation).
- ensuring that the identified controls are in place for the deployed service and the underlying infrastructure;
- designing, implementing and evaluating system and application security;
- managing, designing, implementing and evaluating the security of **cloud services** of **peer cloud service providers**;
- evaluating the effectiveness of the implemented controls and make changes based on experience;
- assuring that operating and business support systems provide data access to **cloud service provider** staff based on the particular **cloud service customers tenants** they provide a service to.

8.3.2.18 Design and implement service continuity

The design and implement service continuity **activity** involves:

- considering potential modes of failure of a **cloud service** and the supporting infrastructure and putting in place recovery processes that will enable the **cloud service** to be available within the terms of the **SLA**, through techniques such as failover and redundancy.

8.3.2.19 Ensure compliance

The ensure compliance **activity** focuses on implementing regulatory and standards compliance. This **activity** involves:

- ensuring that the implementation of the **cloud service** and its supporting infrastructure meets the requirements of any standards that need to be supported, for example, the standards can be required by the target customer set, or can be required by the certification scheme that the provider has chosen to assure the service;
- ensuring that the implementation of the **cloud service** and its supporting infrastructure (including data handling) meets any regulatory requirements that can exist for the service or for the data that is stored or processed by the service.

8.3.2.20 Provide network connectivity

The provide network connectivity **activity** involves the setting up of requested network connections and related capabilities, including (amongst others) connections between the **cloud service customer** and the **cloud service provider's** system and between one **cloud service provider's** system and another **cloud service provider's** system. This can include the establishment of facilities such as a VPN or of dedicated bandwidth connections.

Network capabilities include the ability to provide appropriate bounded delay, jitter, bandwidth, quality of service and reliability for all **cloud service categories** and for both cloud and non-cloud purposes in the case of **NaaS**.

8.3.2.21 Deliver network services

The deliver network services **activity** involves the provision of network related services such as firewalls or load balancing.

8.3.2.22 Provide network management services

The provide network management services **activity** focuses on managing the network infrastructure used to carry **cloud services**. This **activity** provides methods, tools and procedures allowing the operation, administration, maintenance and provisioning of the cloud network infrastructure. It includes tasks for:

- keeping the network up and running smoothly;
- keeping track of resources in the network and how they are allocated;
- performing repairs and upgrades, for example, when equipment must be replaced or upgraded with new functions;
- configuring resources in the network to support a **cloud service**.

8.4 Cloud service partner

8.4.1 Role

A **cloud service partner (CSN)** is a **party** which is engaged in support of, or auxiliary to, **activities** of either the **cloud service provider** or the **cloud service customer**, or both.

A cloud service partner's cloud computing activities vary depending on the type of partner and their relationship with the **cloud service provider** and the **cloud service customer**.

8.4.1.1 Cloud service developer

The cloud service developer is a **sub-role** of **cloud service partner** which is responsible for designing, developing, testing and maintaining the implementation of a **cloud service**. This can involve composing the service implementation from existing service implementations.

The cloud service developer's **cloud computing activities** include:

- design, create and maintain service components (clause 8.4.2.1);
- compose services (clause 8.4.2.2);
- test services (clause 8.4.2.3).

NOTE 1 – Cloud service integrator and cloud service component developer describe **sub-roles** of cloud service developer, where the cloud service integrator deals with the composition of a service from other services, and where cloud service component developer deals with the design, creation, testing and maintenance of individual service components.

NOTE 2 – This includes service implementations and service components that involve interactions with **peer cloud service providers**.

8.4.1.2 Cloud auditor

The **cloud auditor** is a **sub-role** of **cloud service partner** with the responsibility of conducting an audit of the provision and use of **cloud services**. A cloud audit typically covers operations, performance and security, and examines whether a specified set of audit criteria are met. There are a variety of specifications for the audit criteria, for example, ISO/IEC 27002 addresses security considerations.

The **cloud auditor's cloud computing activities** include:

- perform audit (clause 8.4.2.4);
- report audit results (clause 8.4.2.5).

8.4.1.3 Cloud service broker

The **cloud service broker** is a **sub-role** of **cloud service partner** that negotiates relationships between **cloud service customers** and **cloud service providers**. The **cloud service broker** is not itself a **cloud service provider** and should not be confused with the role of inter-cloud provider (see clause 8.3.1.6). The **cloud service broker** role could be combined with or operate independently of the role of inter-cloud provider.

The **cloud computing activities** of a **cloud service broker** include:

- acquire and assess customers (clause 8.4.2.6);
- assess marketplace (clause 8.4.2.7);
- set up legal agreement (clause 8.4.2.8);

The marketplace assessment can happen prior to customer acquisition, creating pre-agreements with **cloud service providers** and this can enable **cloud service customers** to select **cloud service providers** from a **service catalogue**, possibly negotiating service details (e.g., service level objectives) at selection time.

In either case, the **cloud service broker** only acts during the contracting phase of the service, between the **cloud service customer** and **cloud service provider**. The **cloud service broker** is not involved during the consumption of the service. In such cases, the **activities** involve **cloud service provider's activities**.

8.4.2 Cloud computing activities

The **cloud computing activities** which relate to the **sub-roles** of **cloud service partner** are shown in Figure 8-5.

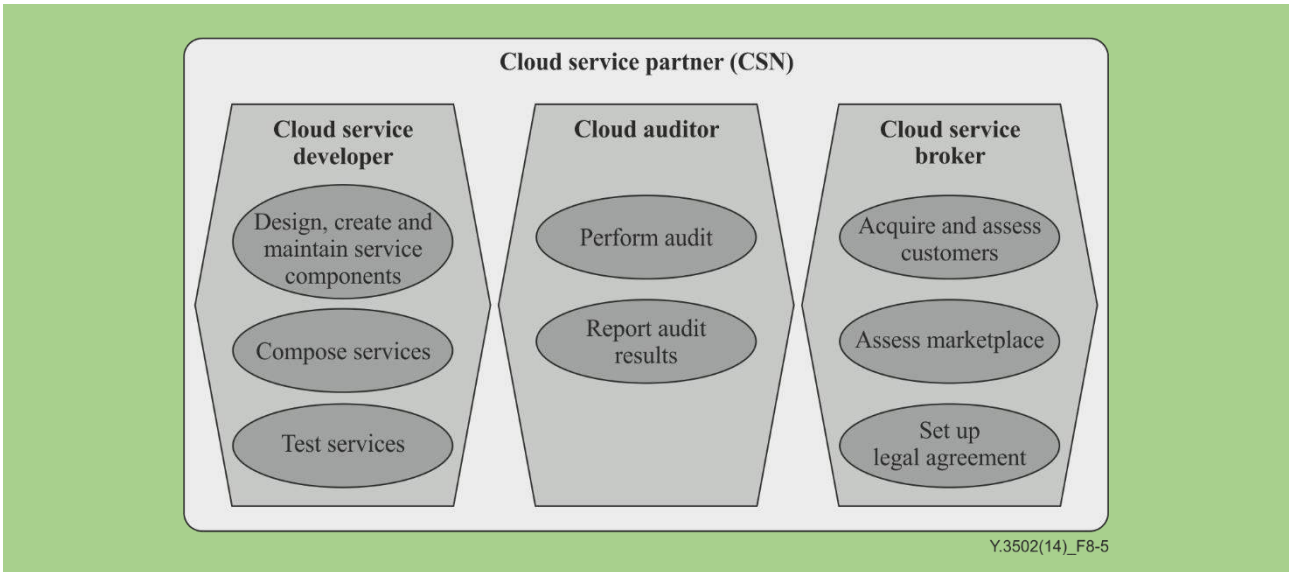


Figure 8-5 – Cloud computing activities related to cloud service partner sub-roles

8.4.2.1 Design, create and maintain service components

The design, create and maintain service components **activity** involves:

- designing and creating software components that are part of the implementation of a service;
- creating the functionality which is offered to users of the service, which also involves connecting the service components to the provider's operational support systems, so that the service implementation can be monitored and controlled;
- processing problem reports relating to the operation of a service implementation;
- providing fixes to service implementations;
- providing enhancements to service implementations.

8.4.2.2 Compose services

The compose services **activity** focuses on composing services using existing services. This **activity** involves:

- creating service functionality by means of composing together one or more existing services provided elsewhere;
- describing the technical aspects of the service (functional interfaces, **SLAs**,…);
- designing an interface to the **cloud service customer** representing the composed services from across multiple **cloud service provider** offerings;
- performing composition which can involve intermediation, aggregation or arbitrage of the existing services.

8.4.2.3 Test services

The test services **activity** focuses on testing the components and services created by the cloud service developer. This **activity** involves:

- performing tests of the components that make up a service implementation to assure that they perform the functionality of the service completely and correctly;
- ensuring **interoperability** with the **cloud services** provided by a **peer cloud service provider**;
- testing which should include checking that the connections to the **cloud service provider's** operational support systems operate correctly – as a result, it is typically necessary to perform some of the testing in a test area of the **cloud service provider's** data centre.

8.4.2.4 Perform audit

The perform audit **activity** involves:

- requesting or obtaining audit evidence;
- conducting any required tests on the system being audited;
- obtaining evidence programmatically, through a set of interfaces provided by the system being audited;
- redacting the evidence, if necessary, in order to protect sensitive information or information subject to regulatory control (e.g., **PII**);
- comparing the obtained audit evidence against the audit criteria as described by the audit scheme or standard that is being used.

The type of audit evidence required and the criteria used to evaluate it are determined by the audit scheme or standard being used. Examples include data relating to security controls and performance data for particular services. In addition to obtaining data, the perform audit **activity** can be asked to evaluate the services provided by a **cloud service provider** which includes security controls, privacy impact, performance, and other **cloud service** related **cloud computing activities** identified by the audit requester. The request can come from the **cloud service provider** itself, where the **cloud service provider** wants proof of the quality of its **cloud services** which can then be presented to potential **cloud service customers**.

8.4.2.5 Report audit results

The report audit results **activity** involves providing a documented report of the results of performing an audit, for example on a given **cloud service** or on a **cloud service provider** or on a **cloud service customer's** use of a **cloud service**. The form of the documented report can be prescribed by the audit scheme that is being used. The results of the audit might be given to the **cloud service provider**, or possibly on request to a **cloud service customer**, depending on the business situation or the legal context.

8.4.2.6 Acquire and assess customers

The acquire and assess customers **activity** includes the tasks required to market and sell **cloud services** up to the point where a **cloud service customer** agrees a contract to use one or more services. This **cloud computing activity** includes:

- providing information to potential customers about available services and associated **SLAs** and contract terms;
- negotiating terms and prices with customers;
- assessing the customer's needs and requirements for **cloud services**.

NOTE – The **cloud service customer** needs assessment activity includes the actions taken to determine and address the **cloud service customer**'s requirements as identified by a gap analysis performed by looking at the customer's current capabilities and their desired future capabilities.

8.4.2.7 Assess marketplace

The assess marketplace **activity** focuses on assessing the current **cloud services** marketplace to find **cloud service** (s) that meet the customers' requirements. This **cloud computing activity** includes:

- surveying the product offerings of **cloud service providers**, obtaining both technical and business information;
- subscribing to and receiving notifications of changes to the content of **cloud service providers' product catalogues**.
- matching the product offerings to the customer's needs and requirements, including technical, business and regulatory aspects.

8.4.2.8 Set up legal agreement

The set up legal agreement **activity** concerns the service agreement between the **cloud service customer** and the chosen **cloud service provider**(s). This involves negotiating the service agreement between the **cloud service customer** and the chosen **cloud service provider**(s), aiming to meet the customer's needs.

8.5 Cross-cutting aspects

8.5.1 General

Cross-cutting aspects include both architectural and operational considerations. Cross-cutting aspects apply to multiple elements within the description of the CCRA or in connection with its operation as an instantiated system. These cross-cutting aspects are shared issues across the **roles**, **activities** and **functional components**. For example, security is a cross-cutting aspect because it applies to infrastructure, services, **cloud service providers**, **cloud service customers** and **cloud service partners** (**cloud auditors**, cloud service developers etc.). All of these need to be secured, but how they are secured is different based on what is being secured. So, securing infrastructure and infrastructure services is very different from securing software services.

Some cross-cutting aspects can apply to other cross-cutting aspects, for example, governance applies to functional elements as well as to the cross-cutting aspects of performance and security.

Cross-cutting aspects often affect the **cloud computing activities** performed by **roles**. **Roles** can coordinate supporting a cross-cutting aspect amongst themselves and their **cloud computing activities**. Supporting cross-cutting aspects also needs **functional components** to provide support for **cloud computing activities**, technical capabilities and implementations.

For each cross-cutting aspect, a set of **cloud computing activities** and **functional components** are defined to support them. Different **roles** and solutions can use different subsets of these.

Cross-cutting aspects include:

- auditability (clause 8.5.2);
- **availability** (clause 8.5.3);
- governance (clause 8.5.4);
- **interoperability** (clause 8.5.5);
- maintenance and versioning (clause 8.5.6);
- performance (clause 8.5.7);
- portability (clause 8.5.8);
- protection of **personally identifiable information** (clause 8.5.9);
- regulatory;
- resiliency (clause 8.5.10);
- **reversibility** (clause 8.5.11);
- security (clause 8.5.12);
- service levels and **service level agreement** (clause 8.5.13).

8.5.2 Auditability

Auditability is the capability of collecting and making available necessary evidential information related to the operation and use of a **cloud service**, for the purpose of conducting an audit. Related to the governance of **cloud services** is the assurance that those services are provided and used in consistency with the associated service agreements between the **cloud service customers, cloud service providers and cloud service partners**. This assurance is most often achieved by means of independent audits of services. An audit typically consists of an audit report or audit certification made available to the parties of the associated service agreements: the **cloud service customers**, the **cloud service providers** and the **cloud service partners**.

The audit itself depends upon data and evidence being available, relating to the usage, environment, **availability** and performance of services and associated resources. Such data and evidence includes records and logs of activities and conditions of the operational environments of all parties of the governing agreements. These records and logs need to be collected and maintained in a secure manner.

8.5.3 Availability

Availability is the property of being accessible and usable upon demand by an authorized entity. The "authorized entity" is typically a **cloud service customer**.

8.5.4 Governance

Governance is the system by which the provision and use of **cloud services** are directed and controlled.

The term internal cloud governance is used for the application of design-time and run-time policies to ensure that **cloud computing** based solutions are designed and implemented, and **cloud computing** based services are delivered according to specified expectations. These expectations can cover any or all of the cross-cutting aspects.

The individual governance practices used by **cloud service customers** and **cloud service providers** exist on a continuum from simple to sophisticated and are encapsulated within their **role**. It is the responsibility of each **role** to implement governance according to their needs. Cloud governance is cited as a cross-cutting aspect because of the requirement for transparency and the need to rationalize governance practices with **SLAs** and other contractual elements of the **cloud service customer** to **cloud service provider** relationship.

The term external cloud governance is used for some form of agreement between the **cloud service customer** and the **cloud service provider** concerning the use of **cloud services** by the **cloud service customer**. The agreement can make reference to a **service level agreement** which provides detailed information about functional and non-functional aspects of the services.

8.5.5 Interoperability

Interoperability in the context of **cloud computing** includes the ability of a **cloud service customer** to interact with a **cloud service** and exchange information according to a prescribed method and obtain predictable results. Typically, **interoperability** implies that the **cloud service** operates according to an agreed specification, one that is possibly standardized. The **cloud service customer** should be able to use widely available ICT facilities in-house when interacting with **cloud services**, avoiding the need to use proprietary or highly specialized software.

Interoperability also includes the ability for one **cloud service** to work with other **cloud services**, either through a CSP:inter-cloud provider relationship, or where a **cloud service customer** uses multiple different **cloud services** in some form of composition to achieve their business goals.

Interoperability stretches beyond the **cloud services** themselves and also includes the interaction of the **cloud service customer** with the **cloud service** management facilities of the **cloud service provider**. Ideally, the **cloud service customer** should have a consistent and interoperable interface to the **cloud service** management functionality and be able to interact with two or more **cloud service providers** without needing to deal with each provider in a specialized way.

Standards are implemented in order to support **interoperability** between components or to support the portability of data or of program components. The implementations should support the evolution of the standards used, both from an earlier version of a standard to a later version, or from one standard to a different one, while minimizing disruptive changes.

8.5.6 Maintenance and versioning

A significant item relating to governance is the maintenance of services and underlying resources. Maintenance can take place for a variety of reasons, including the need to fix faults and also the need to upgrade or extend facilities for business reasons. Maintenance actions can have the effect of changing the behaviour of **cloud services** – in particular changes can affect how a service operates when used by a customer.

It is important to distinguish between maintenance performed by the **cloud service provider** and maintenance performed by the **cloud service customer**. In the case of an **SaaS** service, it is likely that virtually all maintenance actions will be performed by the provider. In the case of **IaaS** and **PaaS** services, the application components belong to the **cloud service customer** and the **cloud service customer** is responsible for the maintenance of those components. The provider is responsible for the environment in which the application components run, which varies depending on the details of the service, but which might include such elements as the hardware resources, operating system or middleware.

On the one hand, it can be in the customer's interests that a service or service platform be upgraded or fixed. On the other hand, any changes to the behaviour of a service can have a negative impact on the customer, possibly requiring changes to application components and to customer ICT systems or calling for retraining of customer service users. As a result, it is important that maintenance of services is subject to governance practices that are transparent to the customer.

Maintenance practices should be documented in the **SLA** for the **cloud services** and should include the capability for the customer to report problems and request fixes and also a mechanism for the **cloud service provider** to notify the customer of pending maintenance changes and their schedule.

Versioning is the appropriate labelling of a service (or of components of a service, such as the operating system level used in an **IaaS** service), so that it is clear to the customer that a particular version is in use. It is important that the service be given a new version label when maintenance of a **cloud service** occurs.

Where significant changes are made to a service between two versions, the older version of the service should be available in parallel with the new versions for an agreed period of time.

8.5.7 Performance

Performance includes a set of non-functional facets relating to the operation of a **cloud service** such as:

- **availability** of the service;
- response time to complete service requests;
- transaction rate at which service requests are executed;
- latency for service requests;
- data throughput rate (input and output);
- number of concurrent service requests (scalability);
- capacity of data storage;
- (for **IaaS** and **PaaS**) the number of concurrent execution threads available to an application;
- (for **IaaS** and **PaaS**) the amount of memory (RAM) available to the running program;
- data centre network IP address pool and/or VLAN range capacity.

Where the service involves running an application (**IaaS**, **PaaS**), the same facets of performance apply to the behaviour of the application running in the **cloud service provider**'s environment.

Depending on the charging model, the ability of the **cloud service** to scale its use of resources in accordance with the terms of the **SLA** can also be an important facet of performance. Performance should have metrics defined in the **SLA** for each performance condition identified and these metrics should be monitored during operation of the **cloud service** to ensure that the service meets the performance terms of the **SLA**.

8.5.8 Portability

Portability is significant in **cloud computing** since prospective **cloud service customers** are interested in avoiding lock-in when they choose to use **cloud services**. **Cloud service customers** need to know that they can move **cloud service customer data** or their applications between multiple **cloud service providers** at low cost and with minimal disruption. The amount of cost and disruption that is acceptable can vary based upon the type of **cloud service** that is being used.

For example if a **cloud service customer** organization is considering moving from one **IaaS cloud service provider** to another, the **cloud service customer** should be able to take its data and the virtual machine (VM)

image and get it up and running on an equivalent **IaaS** service in a relatively straightforward manner. In an **SaaS** environment, when a **cloud service customer** organization wants to move an **SaaS** application to a different **cloud service provider** (i.e., switch **SaaS** service providers), the **cloud service customer** needs to be able to take their data with them, but the rest of the switching cost will include exporting, mapping and importing the data into the new **cloud service provider**'s **SaaS** application, and that cost is a function of how well the data models and formats of the two **SaaS cloud service providers** line up. Ideally, **SaaS cloud service providers** should adopt standard data interchange format(s) relevant to their application domain. Changing between **SaaS** applications can also involve the **cloud service customer** adapting to a new service interface (which relates to the **interoperability** of the service).

However, since different **cloud capabilities types** can have different requirements related to portability, it is more useful to focus on specific types of portability such as **cloud data portability** and **cloud application portability**.

Cloud service customer data is a class of data objects under the control of the **cloud service customer**. **Cloud data portability** allows the **cloud service customers** the ability to copy **cloud service customer data** into or out of a **cloud service** through network access or by physical transfer of storage devices.

Cloud application portability allows the migration of items such as a fully-stopped virtual machine instance or a machine image (**IaaS** service) from one **cloud service provider** to another **cloud service provider**, or the migration of application components (**PaaS** service) from one **cloud service provider** to another. In both cases, there is a related aspect of the support of portability of metadata relating to the application components, providing information about the relationships of program components and about the required infrastructure for the program components (e.g., load balancing configuration, firewall settings).

8.5.9 Protection of personally identifiable information (PII)

Cloud service providers should protect the assured, proper and consistent collection, processing, communication, use and disposition of **personally identifiable information (PII)** in relation to **cloud services**.

According to established guidelines, one of an organization's key business imperatives is to ensure the protection of **personally identifiable information (PII)**. Though **cloud computing** provides a flexible solution for shared resources, software and information, it also poses additional **confidentiality** challenges to **cloud service customers** using **cloud services,** and also for **cloud service providers**.

In many jurisdictions, there are strict rules and regulations applied to the handling of **PII** – any use of **cloud services** to store and process **PII** often has to conform to those rules and regulations.

Statutory, regulatory and legal requirements vary by market sector and jurisdiction, and they can change the responsibilities of both **cloud service customers** and **cloud service providers**. Compliance with such requirements is often related to governance and risk management **activities**.

8.5.10 Resiliency

Resiliency is the ability of a system to provide and maintain an acceptable level of service in the face of faults (unintentional, intentional or naturally caused) affecting normal operation.

Resiliency describes the set of monitoring, preventive and responsive processes that enable a **cloud service** to provide continuous operations, or predictable and verifiable outages, through failure and recovery actions. These can include hardware, communication and/or software failures, and can occur as isolated incidents or in combination, including serial failure. These processes can include both automated and manual actions, usually spanning multiple systems, and thus their description and realization are part of the overall cloud infrastructure, not an independent function.

Inherent in resiliency is the realization of risk management – since resiliency is determined by the least resilient component in the system, and cost/performance or other factors can limit the extent to which resiliency is possible or practical. The association of risk to value is realized in the implementation choices to provide resiliency.

8.5.11 Reversibility

Reversibility is a term which applies to the process for **cloud service customers** to retrieve their **cloud service customer data** and application artefacts and for the **cloud service provider** to delete all **cloud service customer data,** as well as contractually specified **cloud service derived data** after an agreed period. The principle is the "right to be forgotten", in that the **cloud service customer** has a right to expect that once they indicate to the **cloud service provider** that their use of the service(s) will cease, there will be an orderly process for the **cloud service customer** to retrieve **cloud service customer data** and their application artefacts and that the **cloud service provider** will delete all copies and not retain any materials belonging to the **cloud service customer** after an agreed period.

The activity related to **reversibility** will in most cases involve a series of steps, typically requiring the **cloud service customer** to retrieve their data and inform the **cloud service provider** that the **cloud service provider** can delete their copies of the **cloud service customer data** – safeguarding backup copies until that point in case of failures in the exit process. These steps would also necessarily apply to any peer services that are used by the **cloud service provider** to support the **cloud service provider**'s services.

8.5.12 Security

8.5.12.1 General

It is critical to recognize that security is a cross-cutting aspect of the architecture that spans across all views of the reference model, ranging from physical security to application security. Therefore, security in **cloud computing** architecture is not solely a cross-cutting aspect under the control of **cloud service providers**, but also affects **cloud service customers**, **cloud service partners** and their **sub-roles**.

Cloud computing systems can address security requirements such as authentication, authorization, **availability**, **confidentiality**, non-repudiation, identity management, **integrity**, audit, security monitoring, incident response, and security policy management. This clause describes **cloud computing** specific perspectives to help analyse and implement security in a **cloud computing** system.

Security capabilities for **cloud services** include: access control, **confidentiality**, **integrity** and **availability**. Security for **cloud computing** is described in detail in other specifications.

Security capabilities also include the management and administration functions which are used to control **cloud services**, underlying resources and the use of **cloud services**, with particular attention applied to access control for users of these functions. This is in addition to:

- facilities to enable early detection, diagnosis and fixing of **cloud service** and resource related problems;
- secure logging of access records, activity reports, session monitoring and packet inspections on the network;
- provision of firewalling, and malicious attack detection and prevention for the **cloud service providers'** systems. One user should not be able to disrupt other users' use of **cloud services**.

Intranet level security should be provided on the network connecting the **cloud service customer** to the **cloud service provider** (for example, through the use of VPN capabilities).

Security measures in **cloud computing** exist to address a series of threats that relate to the use of **cloud services** by **cloud service customers**, which affect both **cloud service customers** and **cloud service providers**. These threats are more fully described in other specifications, such as ISO/IEC 27018.

8.5.12.2 Distribution of security responsibilities

A **cloud service provider** and a **cloud service customer** have differing degrees of control over the computing resources in a **cloud computing** system. Compared to traditional information technology systems, where one organization has control over the whole stack of computing resources and the entire life cycle of the systems, **cloud service providers** and **cloud service customers** collaboratively design, build, deploy and operate **cloud computing** systems.

The split of control means that both **roles** now share the responsibilities of providing adequate protections to the **cloud computing** systems. Security is a shared responsibility. Security controls, i.e., measures used to provide protections, need to be analysed to determine which **role** is in a better position to implement such controls. This analysis needs to include considerations from a service category perspective, where different **cloud service categories** imply different degrees of control between **cloud service providers** and **cloud service customers**. It is important to provide a clear definition of the responsibilities of both the customer and the provider and to ensure that all aspects of security are covered, to avoid responsibility ambiguity.

For example, account management controls for initial system privileged users for an **IaaS** service are typically performed by the **IaaS cloud service provider;** meanwhile, application user account management for the application deployed to that **IaaS** service is typically the responsibility of the **cloud service customer** who deploys the application using the **IaaS** service. By contrast, for an **SaaS** application service, the account management controls for all types of users are in the hands of the **cloud service provider** (although the **cloud service customer** can provide capabilities such as third-party authentication).

8.5.12.3 Cloud service category perspectives

A **cloud service category** defined in Rec. ITU-T Y.3500 | ISO/IEC 17788 is a group of **cloud services** that possess a common set of qualities. **Cloud service categories** present **cloud service customers** with different types of service management operations and expose different entry points into **cloud computing** systems, which in turn also create different attack surfaces for adversaries. Hence, it is important to consider the impact of **cloud service categories** and their different issues in security design and implementation.

For example, **SaaS** provides users with accessibility of **cloud computing** offerings using a network connection, possibly over the Internet and through a web browser. There has been an emphasis on web browser security in **SaaS cloud computing** system security considerations. CSC:cloud service users of **IaaS** services are typically provided with virtual machines (VMs) that are executed on hypervisors on the hosts; therefore, hypervisor security for achieving VM isolation has been studied extensively for **IaaS cloud service providers** that use virtualization technologies.

8.5.12.4 Implications of cloud deployment models

The different **cloud deployment models** have important security implications. One way to look at the security implications from the deployment model perspective is the differing level of exclusivity of **tenants** in the deployment model. A **private cloud** is dedicated to one **cloud service customer** organization, whereas a **public cloud** could have **tenants** from many different organizations co-existing with each other.

Another way to analyse the security impact of **cloud deployment models** is to use the concept of access boundaries. For example, an on-site **private cloud** system can or cannot need additional boundary controllers at the **cloud service** boundary when the **private cloud** system is hosted on site within the **cloud service customer** organization's network boundary, whereas an outsourced **private cloud** tends to require the establishment of such perimeter protection at the boundary of the **cloud services**.

8.5.12.5 Data protection strategy and responsibility

Protection of data assumes a new dimension in **cloud computing**. An organization can opt to store its data in a **cloud service** but then the data protection responsibility and accountability needs to be agreed upon clearly. The first step that the **cloud service customer** takes is to properly catalogue the data and identify its sensitivity and the risk to the business of its leakage, loss or corruption. (See ISO/IEC 27002 as a reference for how to identify the sensitivity of data).

Ideally, it should be the **cloud service customer's** responsibility to secure the data before it is moved to a **cloud computing** system. However, the provider would be accountable for any data tampering or theft. Encryption is a potential technique to use but then key management has to be given consideration where the **cloud service customer** or any third party manages the keys. If the keys are managed by the **cloud service provider** then they are responsible for the logical and physical control of the keys, as well as the data.

8.5.13 Service levels and service level agreements

Service level agreements are important components of **cloud computing** governance and represent measurable elements needed to assure an agreed upon quality of service between a **cloud service customer** and a **cloud service provider**.

The **cloud computing service level agreement** (cloud **SLA**) is a **service level agreement** between a **cloud service provider** and a **cloud service customer** based on a taxonomy of **cloud computing** specific terms to set the quality of the cloud services delivered. It characterizes the quality of the **cloud services** delivered in terms of:

- a set of measurable properties specific to **cloud computing** (business and technical);
- a given set of **cloud computing roles** (**cloud service customer** and **cloud service provider** and related **sub-roles**).

For instance, **cloud service customers** need a cloud **SLA** to specify the technical performance requirements of one or more **cloud services**. A cloud **SLA** can cover terms regarding the quality of service, security, performance and remedies for failures to meet the terms of the **SLA**. A **cloud service provider** can also list within the cloud **SLA** a set of promises explicitly not made to **cloud service customers**, i.e., limitations and obligations that **cloud service customers** need to accept. A cloud **SLA** should define the classification of data objects (i.e., **cloud service customer data**, **cloud service provider data**, and **cloud service derived data**), who has access and control of data objects in these data classifications and how they will be used.

The **service level agreement** should specify information relating to the **availability** of the services, the **confidentiality** and **integrity** of the services and the access controls which apply to the services. The **service level agreement** should specify how any **personally identifiable information** will be handled in relation to the **cloud service**s.

The service agreement – alternatively known as the master service agreement (MSA), terms of service (ToS), terms and conditions (T&C), or simply "the contract" – is the higher order document in agreements between parties and the **service level agreement** (**SLA**) is subservient. This is an important distinction because the **SLA** acronym is frequently, and incorrectly, used to reference the contractual relationship as a whole – a **role** that an **SLA** alone is incapable of performing. The service agreement addresses the whole of the contractual relationship and therefore contains contractual elements not directly related to **cloud computing**.

9 Functional view

9.1 Functional architecture

The functional architecture for **cloud computing** describes **cloud computing** in terms of a high level set of **functional components**. The **functional components** represent sets of functions that are required to perform the **cloud computing activities** described in clause 8 for the various **roles** and **sub-roles** involved in **cloud computing**.

The functional architecture describes **functional components** in terms of a layering framework where specific types of functions are grouped into each layer and where there are interfaces between the **functional components** in successive layers.

9.1.1 Layering framework

The layering framework used in the CCRA has four layers, plus a set of functions which spans across the layers. The four layers are:

- user layer;
- access layer;
- service layer;
- resource layer.

The functions which span the layers are called the multi-layer functions.

The layering framework is shown diagrammatically in Figure 9-1.

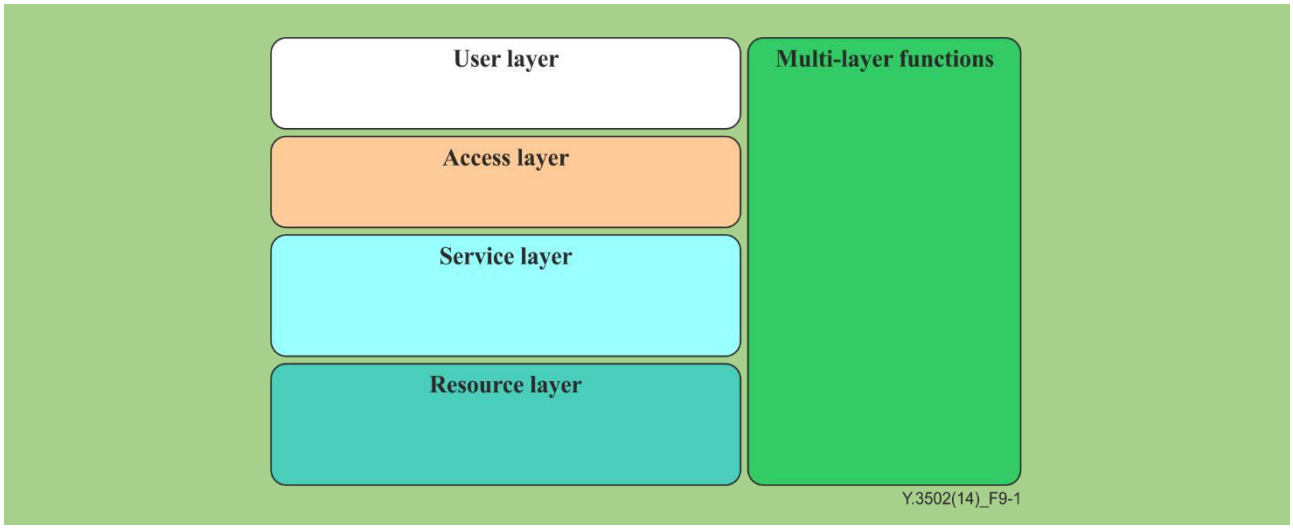


Figure 9-1 – Cloud computing layering framework

Each of the layers in the framework is described in the following subclauses.

9.1.1.1 User layer

The user layer is the user interface through which a **cloud service customer** interacts with **cloud service provider** and with **cloud services**, performs customer related administrative **activities**, and monitors **cloud services.** It can also offer the output of **cloud services** to another resource layer instance.

9.1.1.2 Access layer

The access layer provides a common interface for both manual and automated access to the capabilities available in the services layer. These capabilities include both the capabilities of the services and also the administration and business capabilities.

The access layer is responsible for presenting **cloud service** capabilities over one or more access mechanisms – for example, as a set of web pages accessed via a browser, or as a set of web services which can be accessed programmatically, on secure communication. Another responsibility of the access layer is to apply appropriate security functionality to the access to **cloud service** capabilities. The access layer is responsible for authenticating the request through the use of user credentials and for validating the authorization of the user to use particular capabilities. The access layer is also responsible for handling encryption and checking for request **integrity**, where required.

The access layer can also be responsible for enforcing QoS policies on the traffic coming from the user layer (e.g., service requests to the **cloud service provider**) and the traffic towards the user layer (e.g., output of **cloud services**).

The access layer passes on validated requests to the components in the services layer. The access layer accepts **cloud service customer** or **cloud service provider**'s **cloud service** consumption requests to access **CSP**s' services and resources.

9.1.1.3 Service layer

The service layer contains the implementation of the services provided by a **cloud service provider**. The service layer contains and controls the software components that implement the services (but not the underlying hypervisors, host operating systems, device drivers, etc.), and arranges to offer the **cloud services** to users via the access layer.

The service implementation software in the service layer in turn relies upon the capabilities available in the resource layer to provide the services that are offered and to ensure that the requirements of any **SLA** relating to the services are met, for example, through the use of sufficient resources.

9.1.1.4 Resource layer

The resource layer is where the resources reside. This includes equipment typically used in a data centre such as servers, networking switches and routers, storage devices, and also the corresponding non-cloud-specific software that runs on the servers and other equipment such as host operating systems, hypervisors, device drivers and generic systems management software.

The resource layer also represents and houses the cloud transport network functionality which is required to provide underlying network connectivity between the **cloud service provider** and the users, as well as within the **cloud service provider** and between **peer cloud service providers**.

Note that for a **cloud service provider** to provide services consistent with the **SLA**, it can require dedicated and/or secure connections between users and the **cloud service provider**.

9.1.1.5 Multi-layer functions

The multi-layer functions include a series of **functional components** that interact with **functional components** of the above four other layers to provide supporting capabilities including and not limited to:

- operational support systems capabilities (runtime administration, monitoring, provisioning and maintenance);
- business support systems capabilities (**product catalogue**, billing and financial management);
- security systems capabilities (authentication, authorization, auditing, validation, encryption);
- integration capabilities (linkage of different components to achieve the required functionality);
- development support capabilities (involving the creation, testing and life-cycle management of services and service components).

9.2 Functional components

This clause describes the cloud architecture in terms of the common set of **cloud computing functional components**. A **functional component** is a functional element of the CCRA which is used to perform an **activity** or some part of an **activity** and which has an implementation artefact in a concrete realization of the architecture, e.g., a software component, a subsystem or an application.

Figure 9-2 presents a high level overview of the CCRA **functional components** organized by means of the layering framework.

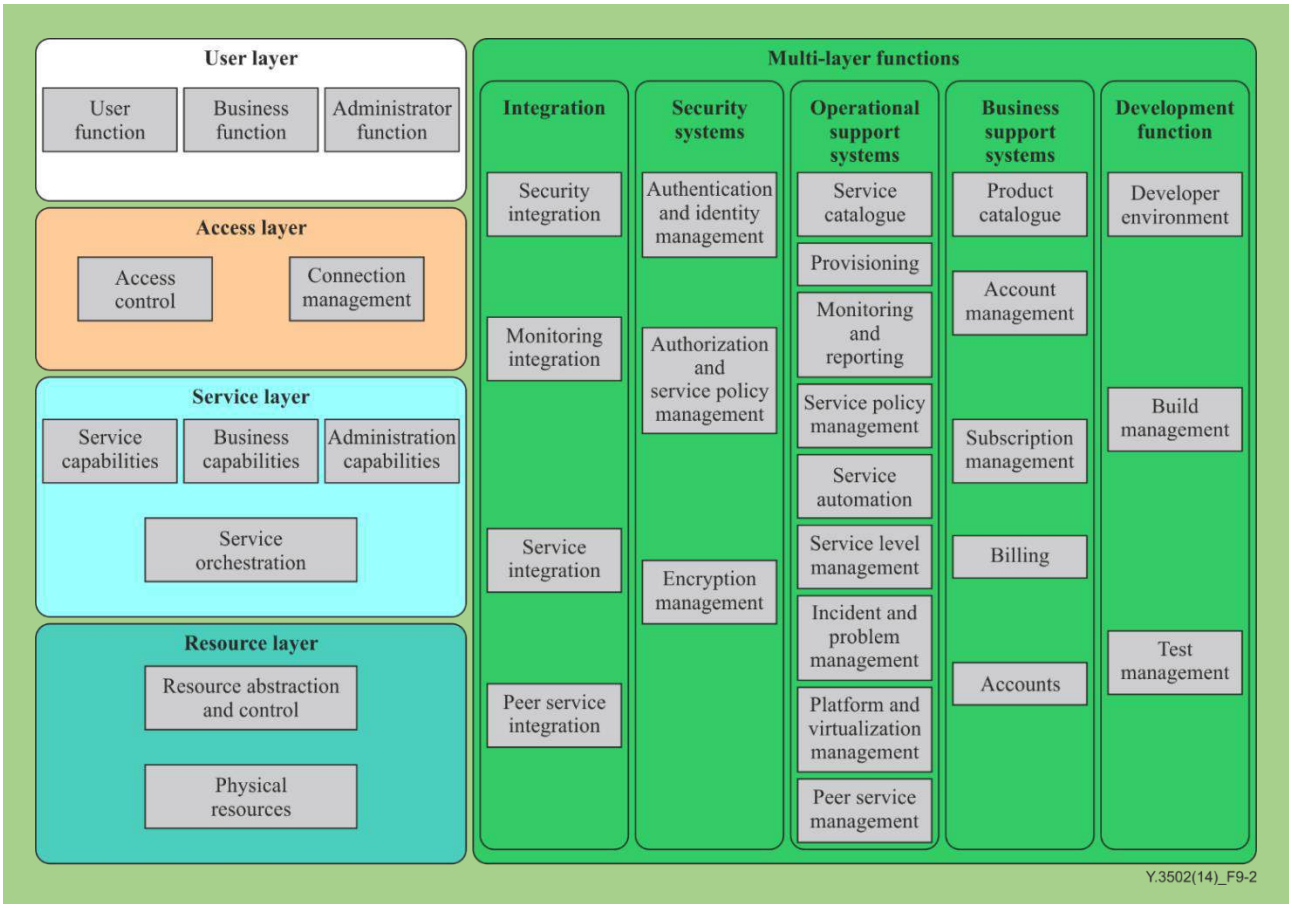


Figure 9-2 – Functional components of the CCRA

9.2.1 User layer functional components

The user layer **functional components** include:

- user function;
- business function;
- administrator function.

The **cloud services** that are presented to CSC:cloud service users can be broken down into two major categories, functional services and self-service management services. The latter can be further divided into business and administration services.

The interface that is presented to the user of the **cloud service** encompasses the primary function of the **cloud service**. This is distinct from the interface that is used to manage the use of the **cloud service**. But all cases are **cloud service**s, tailored for different types of capabilities.

9.2.1.1 User function

The user function **functional component** supports the CSC:cloud service user to access and use **cloud services** (the ***use service* activity**). In some cases, the user function **functional component** could be as simple as a browser running on a user device. However, in other cases, it might involve a sophisticated enterprise system running business processes, applications, middleware and associated infrastructure.

9.2.1.2 Business function

The business function **functional component** supports the **cloud computing activities** of the CSC:business manager including the selection and purchase of **cloud services**; the accounting and financial management relating to the use of **cloud services**. It should be noted that business capabilities are themselves offered via **cloud services**.

9.2.1.3 Administrator function

The administrator function **functional component** supports the **cloud computing activities** of the CSC:cloud service administrator. This includes functions for the administration of user identities and profiles, the monitoring of service activity and usage, event handling and problem reporting. Cloud administration capabilities are only accessed using **cloud services**.

9.2.2 Access layer functional components

Figure 9-3 shows the access layer **functional components** which include:

- access control:
  - service access;
  - business access;
  - administration access;
  - development access.
- connection management.

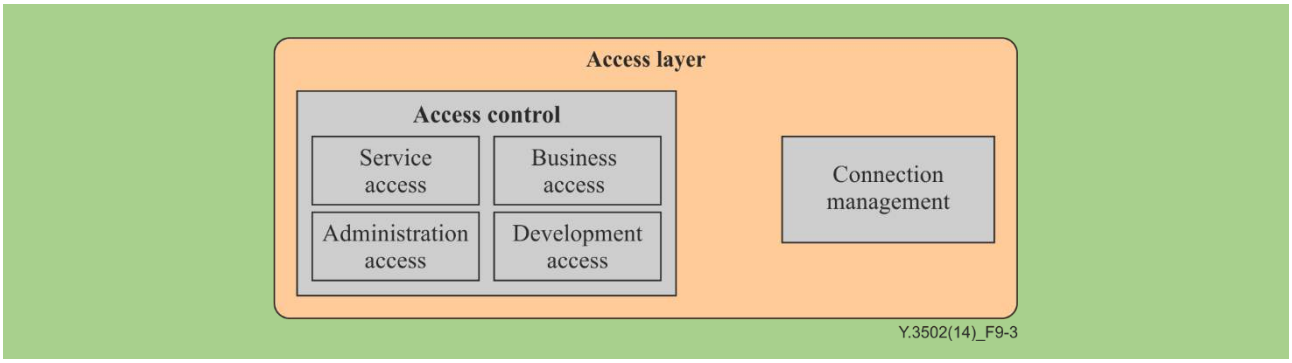


Figure 9-3 – Access layer functional components

9.2.2.1 Access control

Access control limits users to the use of particular services. Principally, access control involves the authentication of a user through the presentation and validation of credentials, followed by the authorization of this authenticated user to use specific services. Associated with this is identity management.

Access control for **cloud services**, the resources they depend on, and the related control functions should be provided.

9.2.2.2 Service access

The service access **functional component** provides access to the **cloud services** offered by the **cloud service provider**.

9.2.2.3 Business access

The business access **functional component** provides access to business capabilities offered by the **cloud service provider**, as implemented by the business support systems.

9.2.2.4 Administration access

The administration access **functional component** provides access to administration capabilities offered by the **cloud service provider**, as implemented by the operational support systems.

9.2.2.5 Development access

The development access **functional component** provides access to a set of capabilities within the provider's system that supports the development, test and maintenance of **cloud service** implementations.

9.2.2.6 Connection management

The connection management functional component provides enforcement of QoS policies regarding the traffic from and/or to the user layer **functional components**. The connection management **functional component** interacts with the multi-layer functions to retrieve policies stored there and enforces them locally in the access layer.

9.2.3 Services layer functional components

The services layer **functional components** include:

- service capabilities;
- business capabilities;
- administration capabilities;
- service orchestration.

9.2.3.1 Service capabilities

The service capabilities **functional component** consists of the necessary software required to implement the service offered to **cloud service customers**. It implements the functionality defined by the service interface, i.e., the interface offered to **cloud service customers**, independent of the service implementation.

9.2.3.2 Business capabilities

The business capabilities **functional component** provides a set of capabilities for accessing the business function related to the provision of **cloud services**. The business function itself is contained within the business support systems **functional components**.

9.2.3.3 Administration capabilities

The administration capabilities **functional component** provides a set of capabilities for accessing the administration function related to the provision of cloud services.

The administration function itself is contained within the operations support systems and business support systems **functional components**.

9.2.3.4 Service orchestration

The service orchestration **functional component** provides coordination, aggregation and composition of multiple service components in order to deliver the **cloud service**.

9.2.4 Resource layer functional components

The resource layer **functional components** include:

- resource abstraction and control;
- physical resources.

9.2.4.1 Resource abstraction and control

The resource abstraction and control **functional component** is used by **cloud service providers** to provide access to the physical computing resources through software abstraction. Resource abstraction needs to ensure efficient, secure and reliable usage of the underlying infrastructure. The control feature of the **functional component** enables the management of the resource abstraction features.

The resource abstraction and control **functional component** enables a **cloud service provider** to offer qualities such as rapid elasticity, **resource pooling** and **on-demand self-service**. The resource abstraction and control **functional component** can include software elements such as hypervisors, virtual machines, virtual data storage, and time-sharing.

The resource abstraction and control **functional component** enables control functionality, enabling monitoring and management capabilities implemented in the operational support systems **functional component** (see clause 9.2.5.3). For example, there can be a centralized algorithm to control, correlate and

connect various processing, storage and networking units in the physical resources so that together they deliver an environment where **NaaS**, **IaaS**, **PaaS** or **SaaS cloud service categories** can be offered. The controller might decide which CPUs and/or racks contain which virtual machines executing which parts of a given **cloud service**'s workload, and how such processing units are connected to each other, and when to dynamically and transparently reassign parts of the workload to new units as conditions change.

The decision as to whether the physical resources are virtualized or not depends on the workload characteristics to be run. For many **cloud services'** workloads (e.g., related to **Compute as a Service** and **Data Storage as a Service**), it is convenient to virtualize the underlying physical resources, especially since virtualization enables some scenarios which basically cannot be realized with a physical infrastructure (e.g., scenarios related to image management or dynamic scaling of CPU capacity as needed). For other workloads (e.g., analytics and/or search) it is required to have maximum compute capacity and use hundreds or thousands of nodes to run a single specialized workload. In such cases non-virtualized physical resources can be more appropriate.

9.2.4.2 Physical resources

The physical resources **functional component** represents the elements needed by the **cloud service provider** to run and manage the **cloud services** that they offer.

Physical resources include hardware resources, such as computers (CPU and memory), networks (routers, firewalls, switches, network links and network connectors, storage components (hard disks) and other physical computing infrastructure elements. These resources can include those that reside inside cloud data centres (e.g., computing servers, storage servers, and intra-data centre networks), and those that reside outside of data centres, typically networking resources, such as inter-data centre networks and core transport networks.

All the elements of the physical resources are managed from the operational support systems **functional component**, with the capability to place instances of each **cloud service** onto the resources as required to satisfy customer requirements. Note that typically, the operational support systems **functional component** itself runs on some part of the physical resources.

9.2.5 Multi-layer functions

9.2.5.1 Integration functional components

The integration **functional components** are responsible for connecting **functional components** in the architecture to create a unified architecture. The integration **functional components** provide message routing and message exchange mechanisms within the cloud architecture and its **functional components** as well as with external **functional components**. Message routing can be based on various criteria, e.g., context, policies.

The integration **functional components** include:

- security integration;
- monitoring integration;
- service integration;
- peer service integration.

9.2.5.1.1 Security integration

The security integration **functional component** provides integration to security capabilities including authentication, authorization, encryption and **integrity** verification and to policy mechanisms that relate to security capabilities.

9.2.5.1.2 Monitoring integration

The monitoring integration **functional component** provides connection from **functional components** in the access layer, services layer and resource layer to the monitoring and reporting capabilities of the operational support systems.

9.2.5.1.3 Service integration

The service integration **functional component** provides connections to services running within the provider's environment. The service integration **functional component** is an essential aspect of virtualizing the services so that, for example, their location and implementation details are hidden from the components that depend on those services.

9.2.5.1.4 Peer service integration

The peer service integration **functional component** is used to connect to services of **peer cloud service providers** in a controlled fashion, with appropriate security and with appropriate accounting for the usage, linking back to the identity of the **cloud service customer**. The peer service integration **functional component** also virtualizes the links to the target services, so that the details of those services can change dynamically without impact on the **functional components** that reference the services.

9.2.5.2 Security systems functional components

The security systems **functional components** are responsible for applying security related controls to mitigate the security threats in **cloud computing** environments. The security systems **functional components** encompass all the security facilities required to support **cloud services**.

The security systems **functional components** include:

- authentication and identity management;
- authorization and security policy management;
- encryption management.

9.2.5.2.1 Authentication and identity management

The authentication and identity management **functional component** provides capabilities relating to user identities and the credentials required to authenticate users when they access **cloud services** and their related administration and business capabilities.
Identity management can involve federated identity management to permit users to employ the same identity and credentials to access multiple **cloud services**, providing capabilities such as "single sign-on".

9.2.5.2.2 Authorization and security policy management

The authorization and security policy management **functional component** provides capabilities for the control and application of authorization for users to access specific capabilities or data. Service policy management provides for the definition and application of security policies which relate to **cloud services**.

9.2.5.2.3 Encryption management

The encryption management **functional component** provides capabilities relating to the encryption of data, whether data at rest or data in motion. Encryption key management and encryption scheme selection are some of the capabilities provided.

9.2.5.3 Operational support systems functional components

The operational support systems **functional components** encompass the set of operational related management capabilities that are required in order to manage and control the **cloud services** offered to customers.

The operational support systems **functional components** include:

- **service catalogue**;
- provisioning;
- monitoring and reporting;
- service policy management;
- service automation;

- service level management;
- incident and problem management;
- platform and virtualization management;
- peer service management.

9.2.5.3.1 Service catalogue

The **service catalogue functional component** provides a listing of all the **cloud services** of a particular **cloud service provider**. A **service catalogue** can contain/reference all relevant technical information required to deploy, provision and run a **cloud service**.

9.2.5.3.2 Provisioning

The provisioning **functional component** provides the capabilities for provisioning services, both in terms of the provisioning of service implementations and of access end points and the workflow required to ensure that elements are provisioned in the correct sequence.

9.2.5.3.3 Monitoring and reporting

The monitoring and reporting **functional component** provides capabilities for:

- monitoring the **cloud computing activities** of other **functional components** throughout the **cloud service provider's** system. This includes the **functional components** that are involved in the direct use of **cloud services** by the CSC:cloud service users such as the service access and service implementation (e.g., the invocation of a **cloud service** operation by a particular user). This also includes **functional components** involved in the support of **cloud services**, such as **functional components** in the OSS itself like the service automation **functional component** (e.g., the provisioning of a service instance for a particular customer);
- providing reports on the behaviour of the **cloud service provider**'s system, which can take the form of alerts for behaviour which has a time-sensitive aspect (e.g., the occurrence of a fault, the completion of a task), or it can take the form of aggregated forms of historical data (e.g., service usage data);
- storage and retrieval of monitoring and event data as logging records.

There is a need to guarantee the **availability**, **confidentiality** and **integrity** of the logging records held by the monitoring and reporting **functional component**. For multi-tenant **cloud services**, there is also a need to design access to the records so that particular **tenants** can only gain access to information about their own tenancy and about no other tenancy.

9.2.5.3.4 Service policy management

The service policy management **functional component** provides capabilities to define, store and retrieve policies that apply to **cloud services**. Policies can include business, technical, security, privacy and certification policies that apply to **cloud services** and their usage by **cloud service customers**.

Some policies can be general and apply to a **cloud service** irrespective of the customer concerned. Other policies can be specific to a particular customer.

9.2.5.3.5 Service automation

The service automation **functional component** provides capabilities for service delivery including the management and execution of service templates and the orchestration of services. The service automation **functional component** holds the service templates which define the **cloud computing activities** and workflows required to provision and deliver a specific entry in the **service catalogue**.

Cloud service provisioning can be automated in order to support scalable resource operations, including configuration and charging.

Cloud service administration **activities** of the **cloud service customer** can be capable of being automated and need not require any intervention by the **cloud service provider**.

The service automation **functional component** works with the provisioning **functional component** and service integration **functional component** to achieve its goals.

9.2.5.3.6 Service level management

The service level management **functional component** provides capabilities for managing the service levels of a particular **cloud service**, aiming to ensure that the **cloud service** meets the requirements of the **SLA** which applies to the service.
The service level management **functional component** manages the capacity and performance relating to a **cloud service**. This can involve the application of service policies (e.g., a placement rule which aims to avoid single points of failure).

The service level management **functional component** obtains monitoring information from the monitoring and reporting **functional component** in order to measure and record key performance indicators (KPIs) for the **cloud service**. Capacity is allocated or de-allocated based on the basis of these KPIs.

The service level management **functional component** also keeps track of the overall state of allocated and available resources. The comparison of allocated capacity against **cloud service** performance KPIs can assist in the identification of current or potential bottlenecks, in support of capacity planning.

9.2.5.3.7 Incident and problem management

The incident and problem management **functional component** provides capabilities for the capture of incident or problem reports and managing those reports through to resolution.

Incidents and problems can be detected and reported by the **cloud service provider**'s systems, or they can be detected and reported by **cloud service customers**.

9.2.5.3.8 Platform and virtualization management

The platform and virtualization management **functional component** provides the capabilities for managing the underlying resources of the **cloud service provider** (compute, storage, networking) and for virtualizing the use of those resources (e.g., by means of hypervisors).

The resources are typically organized into resource pools with key characteristics:

- standardized hardware componentry and configuration;
- readily expandable through the additional of new hardware capacity;
- automated shifting of resources as workload needs change;
- protection and isolation of neighbouring workloads and data;
- reduce and/or eliminate downtime through movement of workloads and data between resources;
- manage resource consumption based on goals (e.g., performance, **availability**, licences, energy use).

9.2.5.3.9 Peer service management

The peer service management **functional component** provides capabilities for connecting the provider's operational support systems and business support systems to the administration capabilities and business capabilities of **peer cloud service providers**, in respect of **peer cloud services** that are used by the provider.

The peer service management **functional component** is responsible for establishing the communication path(s) required, and for passing appropriate identity and credentials with requests made to the **peer cloud service providers**.

9.2.5.4 Business support systems components

The business support systems **functional components** encompass the set of business-related management capabilities dealing with customers and supporting processes.

The business support systems **functional components** include:

- **product catalogue**;
- account management;
- subscription management;
- billing;
- accounts.

9.2.5.4.1 Product catalogue

The **product catalogue functional component** provides capabilities for **cloud service customers** to browse a list of available service offerings which they can purchase, plus a set of capabilities for the management of the content of the catalogue which are available to staff of the **cloud service provider**.

Product catalogue entries consist of technical information about each of the service offerings (capabilities provided by the service, interface definitions for the service including available service operations, security information), plus related business information such as pricing or rating.

9.2.5.4.2 Account management

The account management **functional component** provides capabilities for managing **cloud service customer** relationships, including:

- management of contracts;
- subscriptions to **cloud services**;
- entitlements;
- service pricing, which can involve customer-specific terms such as discounts;
- the policies that apply to the treatment of **cloud service customer data**.

The account management **functional component** and its related database(s) are subject to stringent requirements for **availability** and security due to the importance and the sensitivity of the data related to customer accounts.

9.2.5.4.3 Subscription management

The subscription management **functional component** handles subscriptions from **cloud service customers** to particular **cloud services**, aiming to record new or changed subscription information from the customer and ensure the delivery of the subscribed service(s) to the customer.

9.2.5.4.4 Billing

The billing **functional component** has capabilities for:

- the metering and rating of the use of **cloud services** by **cloud service customers** – where metering is the measurement of the consumption of **cloud services** by each **cloud service customer** and rating is the application of pricing schedules to the metering data. The form of the metering data depends on the nature of the **cloud service** and the pricing schedules can involve customer-specific terms (e.g., discounts) and require algorithmic application against the metering data;
- the generation of invoices based on the charges for the use of **cloud services** created by the metering and rating function, and the transmission of the invoices to the **cloud service customers**. Invoice data is also lodged with the accounts **functional component** and the account management **functional component**.

9.2.5.4.5 Accounts

The accounts **functional component** holds the capabilities relating to general ledger and general accounting functions, including accounts receivable and accounts payable. Note that the accounts **functional component** is used for accounting for the **cloud service provider** organization itself and does not deal with the maintenance of individual customer accounts (those are handled by the account management **functional component**).

9.2.5.5 Development support functional components

The development support **functional components** support the **cloud computing activities** of the cloud service developer. This includes support of the development and/or composition of service implementations, build management and test management.

The development support **functional components** include:

- developer environment;
- build management;
- test management.

9.2.5.5.1 Developer environment

The developer environment **functional component** provides the capabilities to support the development of the service implementation software. Development of software components for the service is supported, plus tools which assist in composing the service from a set of other services.

The developer environment **functional component** supports the use of the capabilities provided by the **cloud service provider**'s environment, including connections to resources and network, integration with other services (including services of **peer cloud service providers**), integration with monitoring and management capabilities, integration with security capabilities.

The developer environment **functional component** also supports the creation of configuration metadata relating to the service being developed and also supports the creation of scripts and related artefacts that are used by the provider's operational support systems to provision and configure the service.

9.2.5.5.2 Build management

The build management **functional component** supports the building of a ready-to-deploy software package which can be passed to the **cloud service provider** for deployment into the **cloud service** environment. The software package consists of both the service implementation software and also the configuration metadata and scripts.

9.2.5.5.3 Test management

The test management **functional component** supports the execution of test cases against any build of the service implementation. The test management **functional component** produces reports of the executed tests and these can be communicated to the **cloud service provider** along with a build of the service implementation.

It is typical for testing to be performed in a specialized test environment, which closely approximates to the production environment without interfering with the production environment. For **cloud computing**, the test environment can be made available by the **cloud service provider**.

10 Relationship between the user view and the functional view

10.1 General

As well as specifying the **roles** and **cloud computing activities** view in clause 8 and the functional view including architectural **functional components** in clause 9, this Recommendation | International Standard describes in this clause the logical relationships of the **roles** and **cloud computing activities** to the **functional components**.

Standards can be relevant to some of these relationships. Standards associated with a relationship can be used to (i) specify degrees of information flow or other types of **interoperability**; and/or (ii) ensure specified degrees of quality (e.g., security or service level).

Logical relationships defined in this architecture are a significant part of specifying the CCRA and its behaviour. The relationship describes matters such as the required information flows between the **functional components** in the CCRA.

10.2 Overview

Figure 10-1 provides an overview of the major elements of the CCRA – **roles, cloud computing activities** and **functional components**, in a common configuration.

Figure 10-1 uses the graphical conventions introduced in clause 5. The boxes with continuous rounded edges represent **roles**, the hexagons represent **sub-roles**, the rounded edged dotted boxes represent **cloud computing activities**, and the square ones with bricks are **functional components**. The "L" shaped boxes inside the service capabilities **functional component** represents the **cloud service** interfaces based on the fundamental **cloud capabilities types**. In Figure 10-1, it is apparent that **roles** are collections of **cloud computing activities**, and **cloud computing activities** themselves are implemented or realized by means of **functional components**.

The proximity of the graphical elements representing roles to each other is meaningful, and represents close interaction between roles assuming neighbouring **roles**. For example, the **cloud service provider role** is at the centre of the diagram to emphasize that it interacts with all other **roles**. The same is true about the positioning of the **cloud computing activities** inside a given **role**, as well as the relative positioning of **functional components** inside a given **activity**. For example, the service capabilities **functional component** is positioned above the resource abstraction and control **functional component**, to signal the dependency of the former on the latter.

The cross-cutting aspects of auditability, **availability**, governance, **interoperability**, maintenance and versioning, performance, portability, protection of **personally identifiable information**, regulatory, resiliency, **reversibility**, security, and service levels and **service level agreement** are indicated by the outermost box in Figure 10-1, which is intended to show that the cross-cutting aspects apply to all the other elements in Figure 10-1 – **roles, activities** and **functional components**. As an example, the CSC:cloud service user must have an identity, along with a set of credentials, which must be given to the user function **functional component** when performing the use cloud service **activity**. The identity and the credentials are presented to the access control **functional component** and authentication and authorization performed as part of the provide services **activity**, invoking the appropriate security **functional component** capabilities before the **cloud service** is provided to the CSC:cloud service user.

The service capabilities **functional component** of Figure 10-1 represents the implementation of the **cloud service** itself.

10.2.1 Service capabilities functional component

The **cloud service** is offered via a service interface and can offer one or more of the **cloud capabilities types**, represented by the "inverted L" shapes within the service capabilities **functional component**. The topmost L shape represents the **application capabilities type**, while the next lower L shape represents the platform capabilities type and the bottom L shape represents the infrastructure capabilities type.

The implication of the L shapes is that an **application capabilities type** can be implemented using the platform capabilities type or not (at the choosing of the **cloud service provider**) and that the platform capabilities type can be implemented using the infrastructure capabilities type or not.

For **SaaS** or **CaaS cloud service categories**, the service capabilities **functional component** contains the application-specific software or the communication applications which are deployed onto the resource layer in such a way that the service levels identified in the **SLA** are achieved.

For other **cloud service categories**, see cloud computing overview and vocabulary in Rec. ITU-T Y.3500 | ISO/IEC 17788.

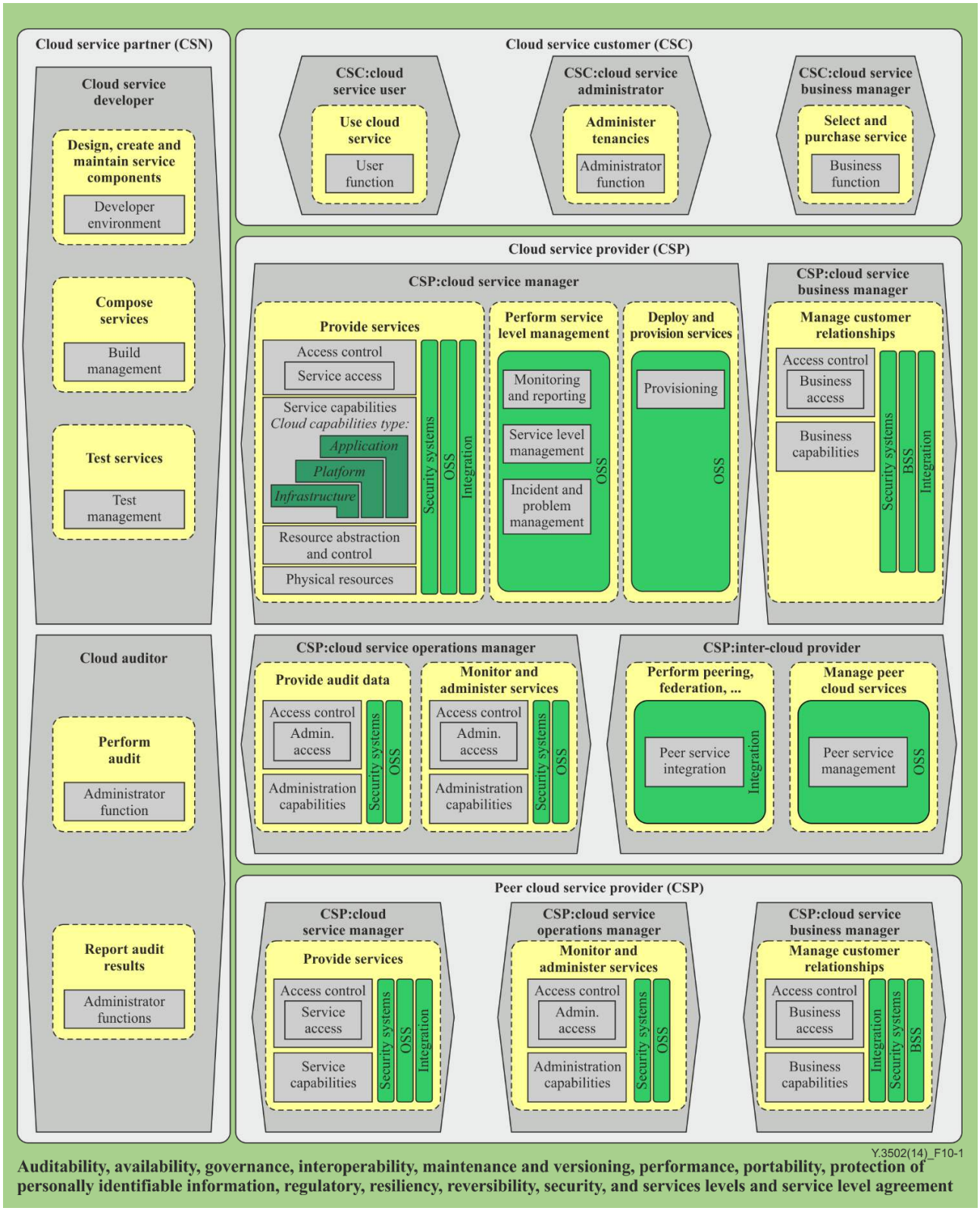


Figure 10-1 – Common view of roles, cloud computing activities and functional components

10.2.2 Common roles, activities and functional components

In Figure 10-1, the **cloud service provider** has a **sub-role**, CSP:cloud service manager, which performs the provide services **activity**, which provides the service for the CSC:cloud service user of the **cloud service customer** to actually use. But before the service can be used, the **cloud service** needs to be developed and deployed to be operational.

Two **sub-roles** of **cloud service partner** are involved in this case, cloud service developer and **cloud auditor**. The cloud service developer develops the implementation of the **cloud services** using the development tools **functional component** and tests the service using the test management **functional component**. The **cloud service** is then packaged with deployment information and given to the CSP:cloud service manager to perform the deploy and provision services **activity** resulting in a service capabilities **functional component** being offered in the provide services **activity**. The **cloud auditor**, in the meantime, performs the perform audit and report audit results **activities** on the cloud service developer, **cloud service provider** or **cloud service customer** according to the policies and governance regimens of each.

After the CSP:cloud service manager performs the deploy and provision services **activity**, the provide services **activity** uses the service capabilities **functional component**, which is the implementation of the service and which in turn uses the resource layer **functional components** for the compute, storage and network resources required to run the service. The provide services **activity** also involves integrating the service capabilities **functional component** with the security systems **functional component** to provide security and protection of **personally identifiable information** capabilities such as data encryption. The operational support systems **functional component** supports management, monitoring, automation and configuration for the services and resources. In addition, the CSP:cloud service manager performs the perform service level management **activity**. The perform service level management **activity** manages the **availability** and performance of the **cloud service** so that it meets the objectives defined in the **SLA** which applies to the **cloud service**. The service level management **functional component**, the monitoring and reporting **functional component**, and the incident and problem management **functional component** are used to accomplish this.

Sometimes, CSP:cloud service managers provide the service in collaboration with another CSP:cloud service manager, invoking **cloud services** in that **peer cloud service provider**. The CSP:cloud service manager then performs the manage **peer cloud services activity** to set up the contracts and **SLAs** for using the **peer cloud service**. The **peer cloud service provider** also offers administrative and use **cloud computing activities**: the provide services and the perform service level management **cloud computing activities**, just like any other **cloud service provider**.

These are a common set of **cloud computing activities** for a CSP:cloud service manager, but there are additional **cloud computing activities** that could be performed and are documented in this specification.

Once a **cloud service** is available for use, two **cloud service customer sub-roles** perform various activities. First, the CSC:cloud service administrator performs the administer tenancies activity using the administrator function **functional component**, to set up the tenancy and to grant access rights to CSC:cloud service users. Once this is done, CSC:cloud service users perform the use cloud service activity by leveraging the user function **functional component** to interact with the **cloud service**. Meanwhile, the CSC:cloud service administrator typically monitors the service to ensure that it is running correctly and meeting the terms of the **SLA**, again using the administrator function **functional component**.

Figure 10-2 provides a view of **roles**, **cloud computing activities** and **functional components** drawing links between **cloud computing activities** of multiple **roles**. Annex A provides a description of each of these relationships.

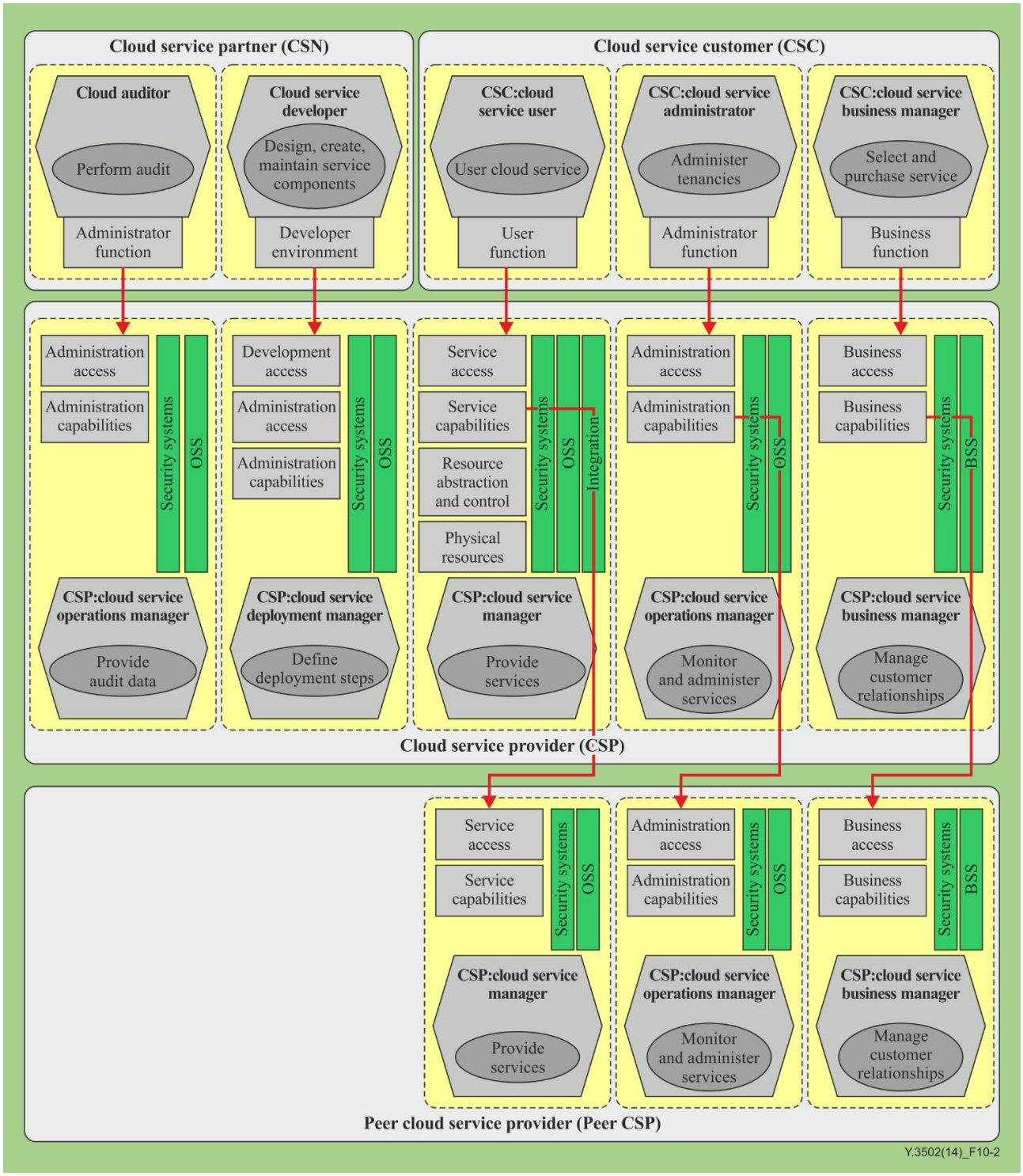


Figure 10-2 – Examples of relationships and interactions between activities and functional components

10.2.3 Multi-tenancy and isolation

Cloud computing involves the sharing of some resources, and this typically means the sharing of those resources with other customers of the **cloud services** involved. The terms **tenancy** and **multi-tenancy** are used to describe the situation where resources are shared.

A **tenant** of a **cloud service** is not quite the same as a **cloud service customer** – a **tenant** is a group of CSC:cloud service users sharing access to a set of physical and virtual resources. Typically, the group of CSC:cloud service users will be associated with a particular **cloud service customer**, but a **cloud service customer** can well have multiple **tenants** – groups of users from different departments within the customer organization, for example.

Multi-tenancy is the allocation of physical or virtual resources so that multiple **tenants** and their computations and data are isolated from and inaccessible to one another. In other words, the users who belong to one tenancy should be completely unaware of the presence of users from another tenancy.

Multi-tenancy does not only affect the **cloud services** themselves; it also affects the business and administration capabilities offered to **cloud service customers** by the **cloud service provider**. Information about user accounts, subscriptions, usage and billing must all be kept isolated and visible only to the customers who own the related tenancies. Particular care must be taken in relation to resources such as log files, which can contain records relating to multiple **tenants**. If a particular customer needs to access the log records, for example when an incident occurs, then the log records must be filtered so that the customer can only see records relating to its tenancies.

Annex A

Further details regarding the user view and functional view

(This annex forms an informative part of this Recommendation | International Standard.)

This annex provides further details regarding the relationship of the user view and functional view.

A.1 The cloud service customer–cloud service provider relationship

There are three key elements in the **cloud service customer**–**cloud service provider** relationship:

1) the CSC:cloud service user using provider **cloud services** to achieve their business goals;
2) the CSC:business manager using **cloud service provider** business capabilities to subscribe to **cloud services** and manage their use from a business perspective;
3) the CSC:cloud service administrator using the **cloud service provider** administration capabilities to administer the use of the **cloud services** from the **cloud service customer** perspective.

A.1.1 Functional relationship

The **cloud service** is made available to CSC:cloud service users via an end point and interface enabled by the service access **functional component**. The functions of this interface and the associated information flows are domain specific to the **cloud service** and are thus not in the scope of the reference architecture. However, there are some broad aspects that should be reflected in the service interface, in particular the need to identify and authenticate the CSC:cloud service user.

The CSC:cloud service user performs the use cloud service **activity** through the user function **functional component**, which then invokes the **cloud service** through the service access **functional component**. The service access **functional component** performs any authentication of the CSC:cloud service user and establishes authorization to use particular capabilities of the **cloud service**. If authorized, the service access **functional component** invokes the **cloud service** implementation which performs the request.

Figure A.1 illustrates the **functional component** relationships involved in the use **cloud service activity** of the CSC:cloud service user.

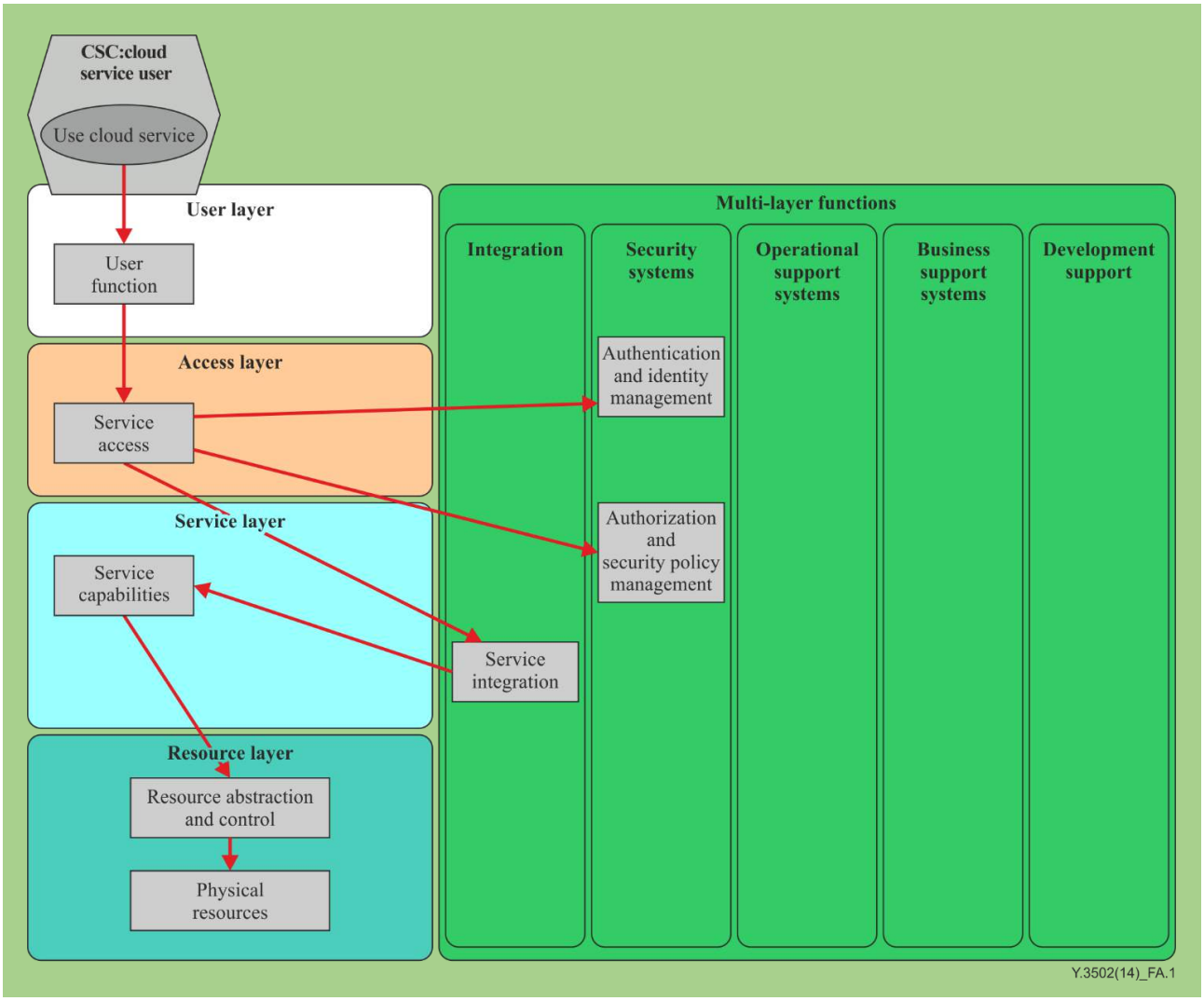


Figure A.1 – CSC:cloud service user relationship for the "use cloud service" activity

A.1.2 Business relationship

The CSC:cloud service business manager performs the **cloud computing activities** select and purchase service, perform business administration and request audit report through the business function **functional component** of the user layer. The business function **functional component** invokes the business capabilities of the **cloud service provider** through an end point and interface enabled by the business access **functional component**.

The business access **functional component** performs any authentication of the cloud CSP:cloud service business manager and establishes authorization to use particular functions of the business capabilities. The business capabilities **functional component** interacts with business support systems **functional components** to carry out requests made by the CSC:cloud service business manager – including the **product catalogue**, account management and subscription management **functional components**.

The information that relates to the business capabilities is typically:

- **product catalogue** entries for available **cloud services**, with related technical information, pricing, terms and conditions;
- subscription information concerning which service(s) the customer is subscribing to, with associated quantitative information, if relevant (e.g., numbers of users, volumes of data, amount of processing, etc.);
- billing information, which can include information about usage charges, payments and account status.

Figure A.2 illustrates the **functional component** relationships involved in the select and purchase service **activity** of the CSC:cloud service business manager.

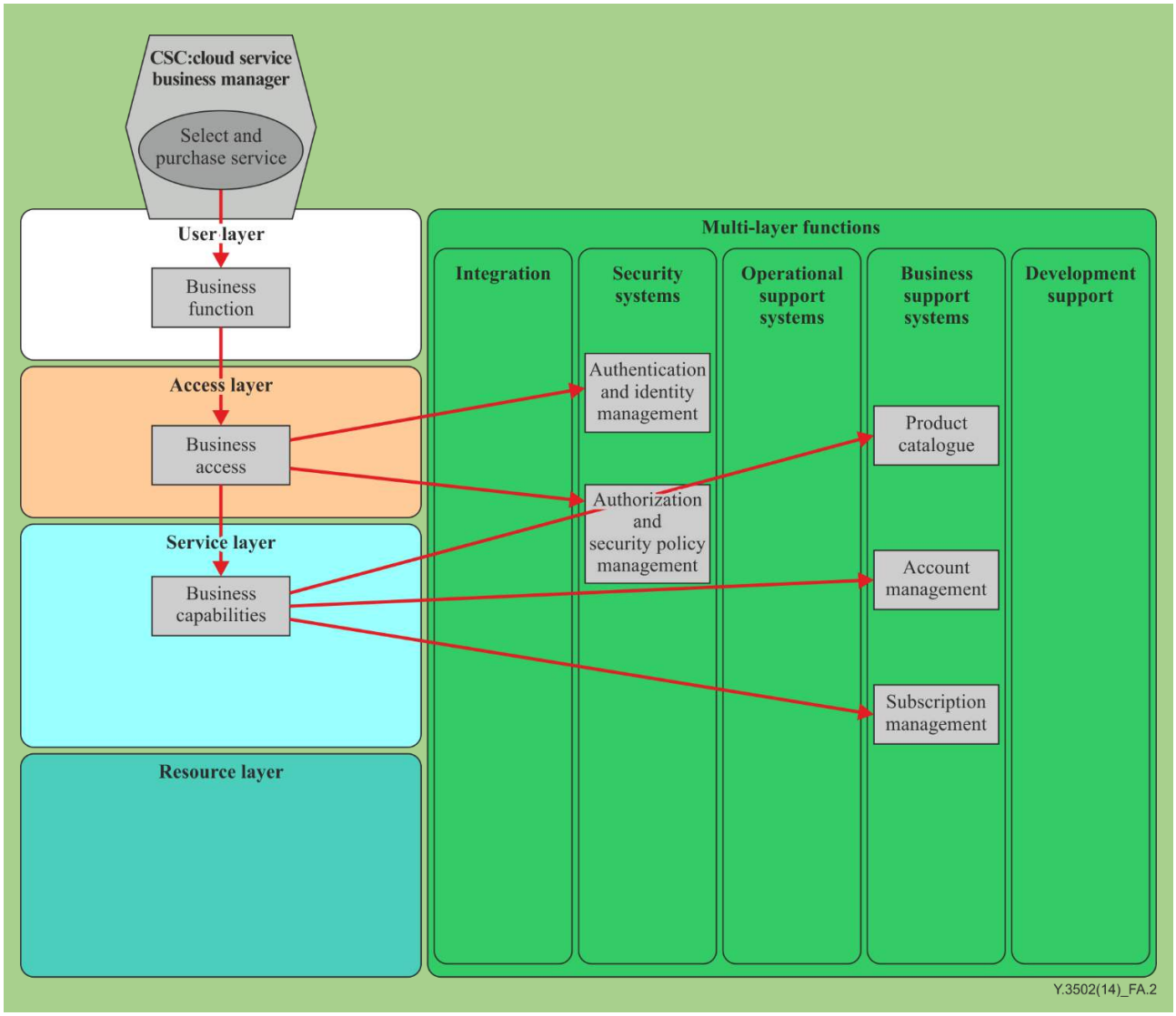


Figure A.2 – CSC:cloud service business manager relationship for " select and purchase service " activity

A.1.3 Administration relationship

The CSC:cloud service administrator performs the following cloud computing activities through the administrator function **functional component**:

- monitor service;
- provide billing and usage reports;
- administer tenancies;
- administer service security;
- handle problem reports. The administrator function functional component invokes the administration capabilities functional component of the **cloud service provider** through an end point and interface enabled by the administration access functional component.

The administration access **functional component** performs any authentication of the CSC:cloud service administrator and establishes authorization to use particular functions of the administration capabilities **functional component**. The administration capabilities **functional component** interacts with operational support systems **functional components** to carry out requests made by the CSC:cloud service administrator, for example, the monitoring and reporting **functional component**.

The information that relates to the administration capabilities includes:

- security information such as the set-up of user accounts and authorization data, the encryption of data;
- notifications concerning usage of services including statistics of usage, log records (e.g., for security purposes);
- exception reports/events (e.g., where some service **SLA** target is breached or a security incident occurs).

Figure A.3 illustrates the **functional component** relationships involved in the monitor service **activity** of the CSC:cloud service administrator.

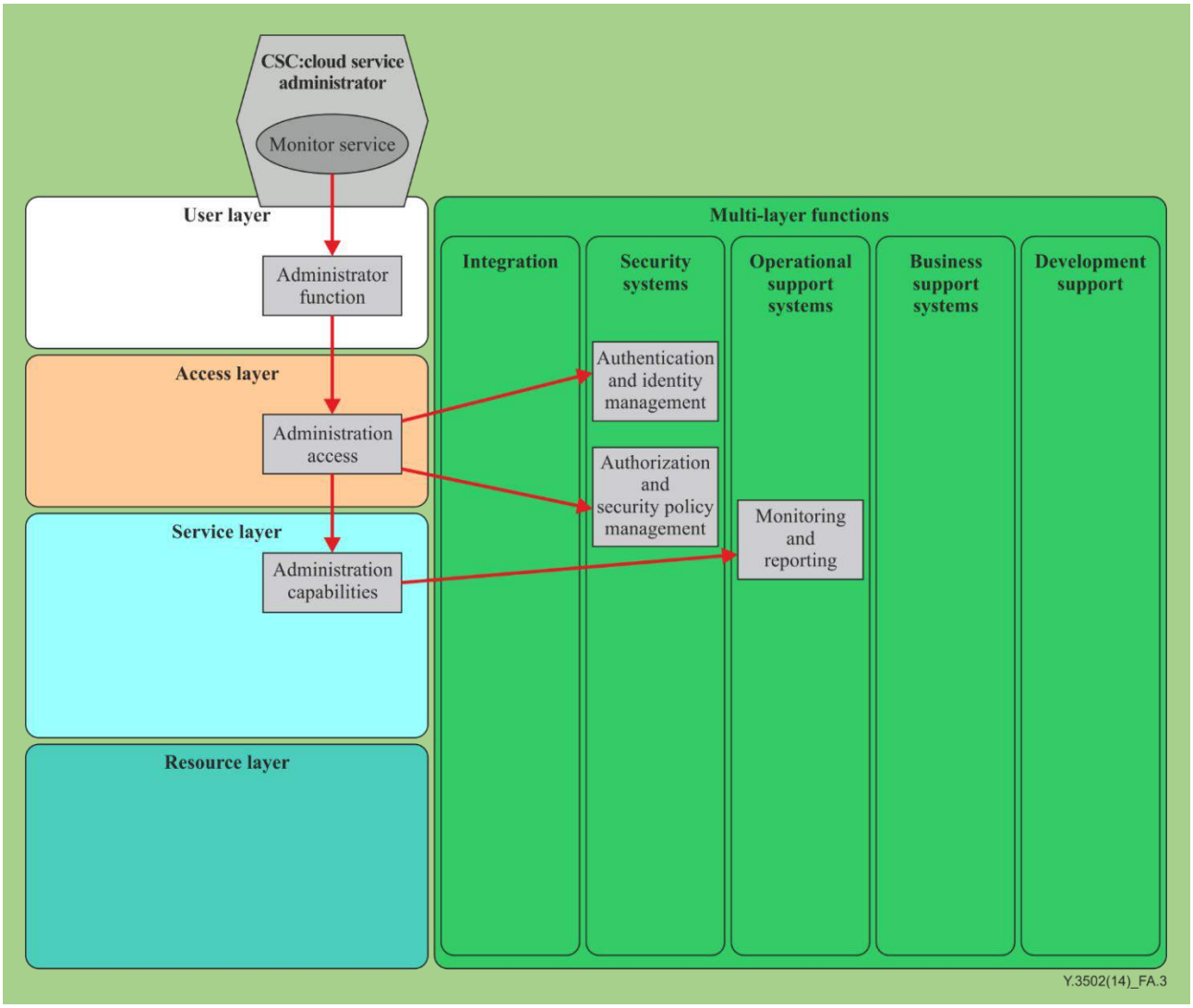


Figure A.3 – CSC:cloud service administrator relationship for the "monitor service" activity

Other elements relevant to the **cloud service customer–cloud service provider** relationship can include a customer to provider agreement, which can include an **SLA**, intellectual property issues and regulated matters such as the appropriate protection of personal data.

A.2 The provider–peer provider (or "inter-cloud") relationship

A **cloud service provider** can make use of one or more **cloud services** which are provided by other **cloud service providers**. This is described as a provider to **peer cloud service provider** relationship, or alternatively as an "inter-cloud" relationship – the provider making use of the services is termed a primary **cloud service provider** while a provider whose services are being used is termed a secondary **cloud service provider**.

As is the case with the **cloud service customer**-**cloud service provider** relationship there are two functional components to the relationship between two **cloud service providers**:

- the use of secondary provider **cloud services** by a primary provider;
- the use of secondary provider's business and administration capabilities by the primary provider's CSP:cloud service operations manager and CSP:cloud service manager to establish and control the use of the secondary provider's **cloud service**s.

For the secondary provider, the primary provider assumes the role of a **cloud service customer**. Services of the secondary **cloud service provider** are offered to and used by customers of the primary **cloud service provider**. The resulting linkage between the secondary **cloud service provider** and the **cloud service customer** of the primary provider requires specific consideration of issues such as security, protection of **PII**, and data ownership.

It is essential that the primary provider ensures that the **SLA** offered by the secondary provider's services is suitable for the requirements of the primary provider's services – and that any breaches of the **SLA** are managed appropriately.

There are three interfaces involved in the provider–peer provider relationship – the administration interface, the business interface and the service interface(s), which broadly provide the same capabilities as the equivalent interfaces in the **cloud service customer–cloud service provider** relationship. The way in which the administration interface is used is shown in Figure A.4 and the way in which the service interface is used is shown in Figure A.5 and the way in which the business interface is used is shown in Figure A.6.

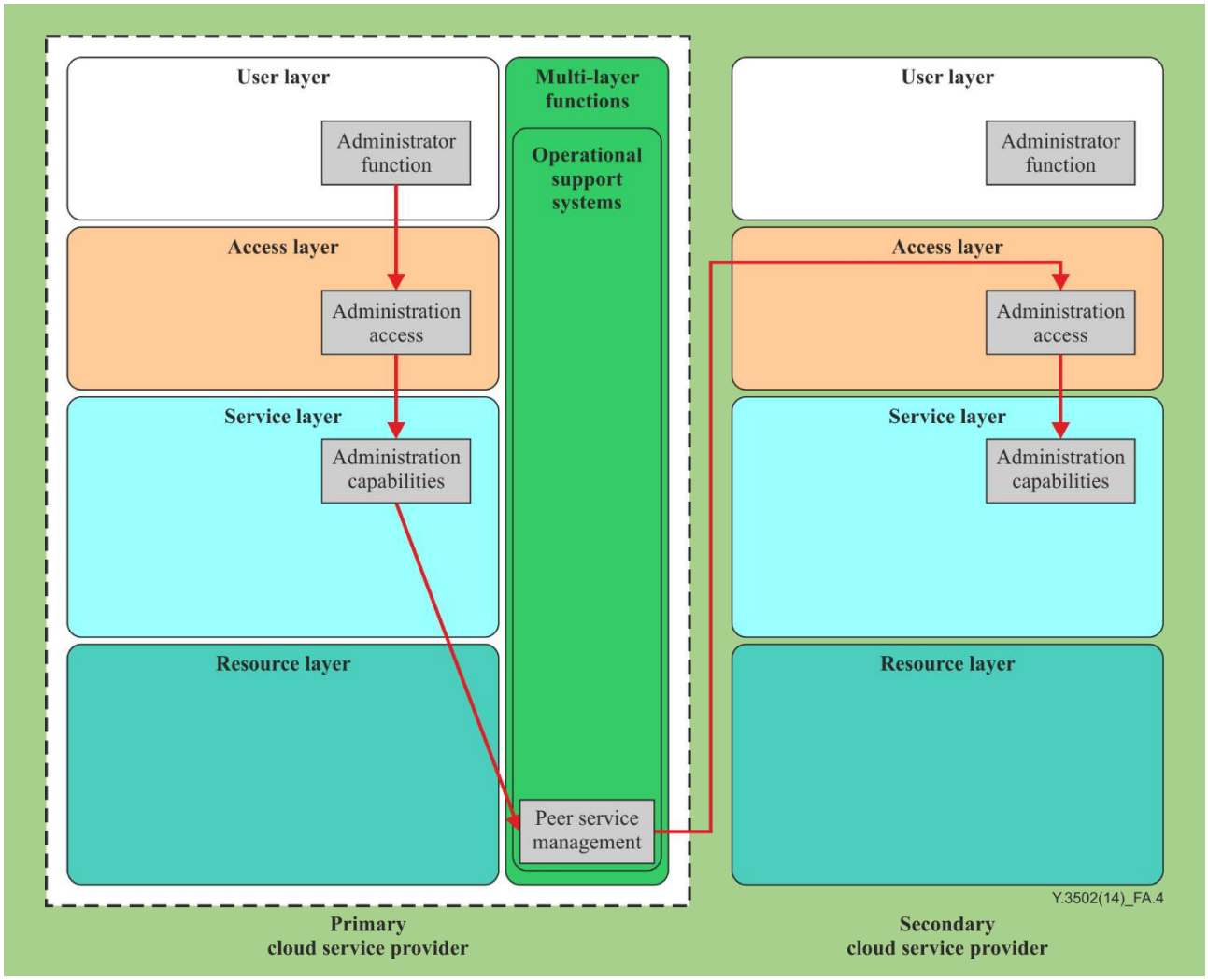


Figure A.4 – Provider–peer provider relationship for administrator activity

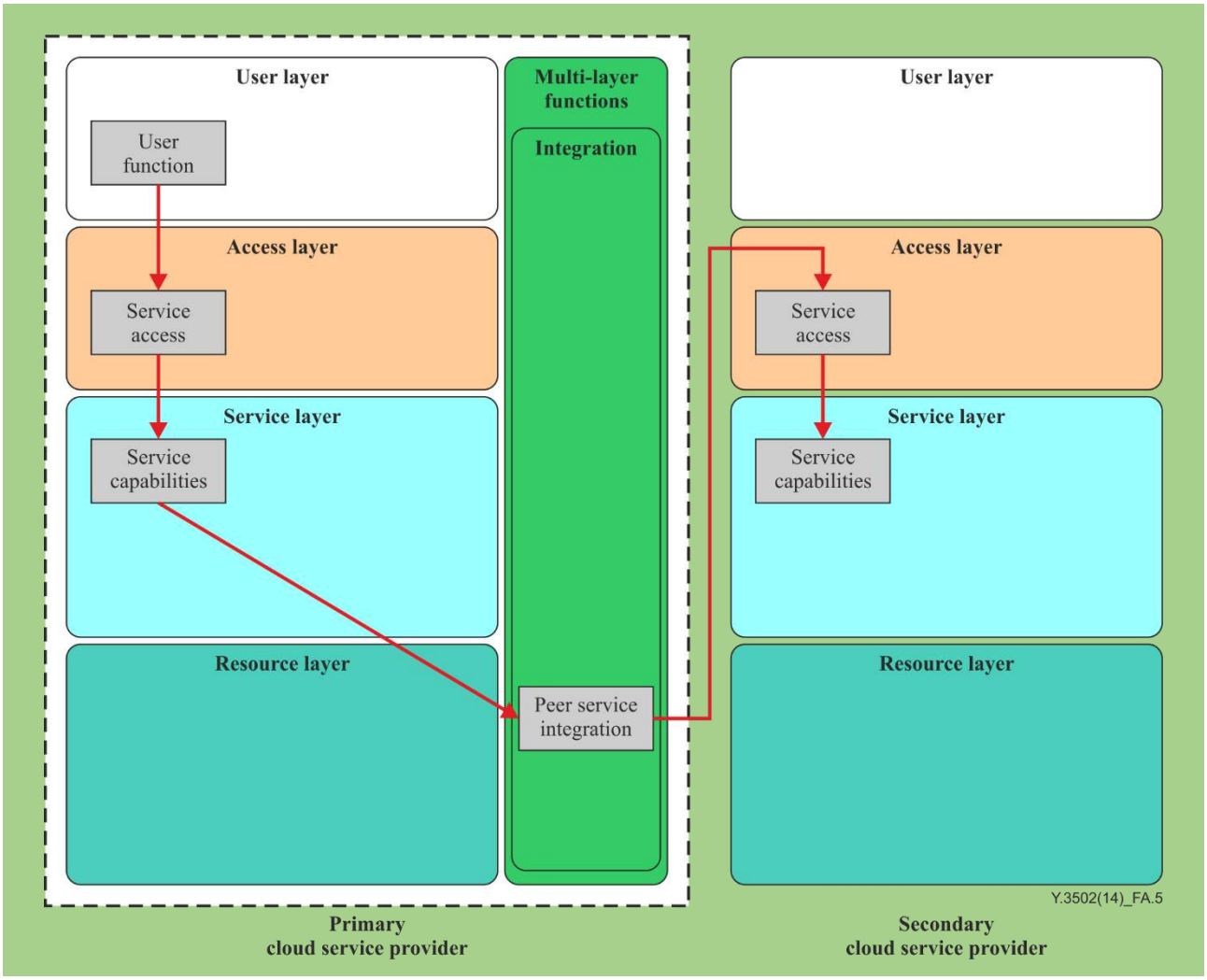


Figure A.5 – Provider–peer provider relationship for use service activity

A.3 The cloud service developer–cloud service provider relationship

Cloud service developers create and package service implementations and hand them to **cloud service providers** for deployment and operation. Therefore, the cloud service developer interacts with the **cloud service provider** to:

1) inspect the **cloud service provider's** environment for service execution;

2) test service implementations;

3) hand over service implementation packages.

The development support **functional components** support the **cloud computing activities** of the cloud service developer, including the develop service, test service and maintain service **cloud computing activities**. These **cloud computing activities** depend on the development environment, build management and test management **functional components**.

The lines in radiating from the developer environment component in Figure A.7 show that the cloud service developer develops the implementation of a **cloud service** and composes the service using the development environment **functional component** and then uses the build management system to build the service and its related artefacts into a deployable package. The arrows to/from the test management **functional component** indicate that the test management system performs appropriate testing against the built package, fetching the package from the build management system and interacting with the provider's environment via the development access **functional component** to deploy a test version of the service and execute the tests.

In Figure A.7, the lines from the development environment show that the development environment and build management system are used to create the software and related artefacts of the service implementation which offers the service interface. The cloud service developer can also create the service access implementation.

In order for the service implementation and service access to run in the target execution environment, the correct enablement for security, monitoring, management and automation needs to be developed, as well as enablement for integration into the service execution environment. The cloud service developer discovers the appropriate enablement for monitoring integration, security integration and service integration by using the development access capabilities. In addition, information and requirements for enabling authentication and identity management, as well as authorization and security policy management, is retrieved via the development access **functional component**.

The enablement of the **cloud service** implementation for deployment and provisioning is also done using the development environment and build management system (e.g., via scripts and configuration metadata files). The cloud service developer uses the development access **functional component** to discover what the provisioning and deployment requirements are.

The service implementation is packaged with the deployment and provisioning information and passed to the CSP:cloud service manager to perform the deploy services **activity** resulting in the service being available for use by customers in the provide services **activity**.

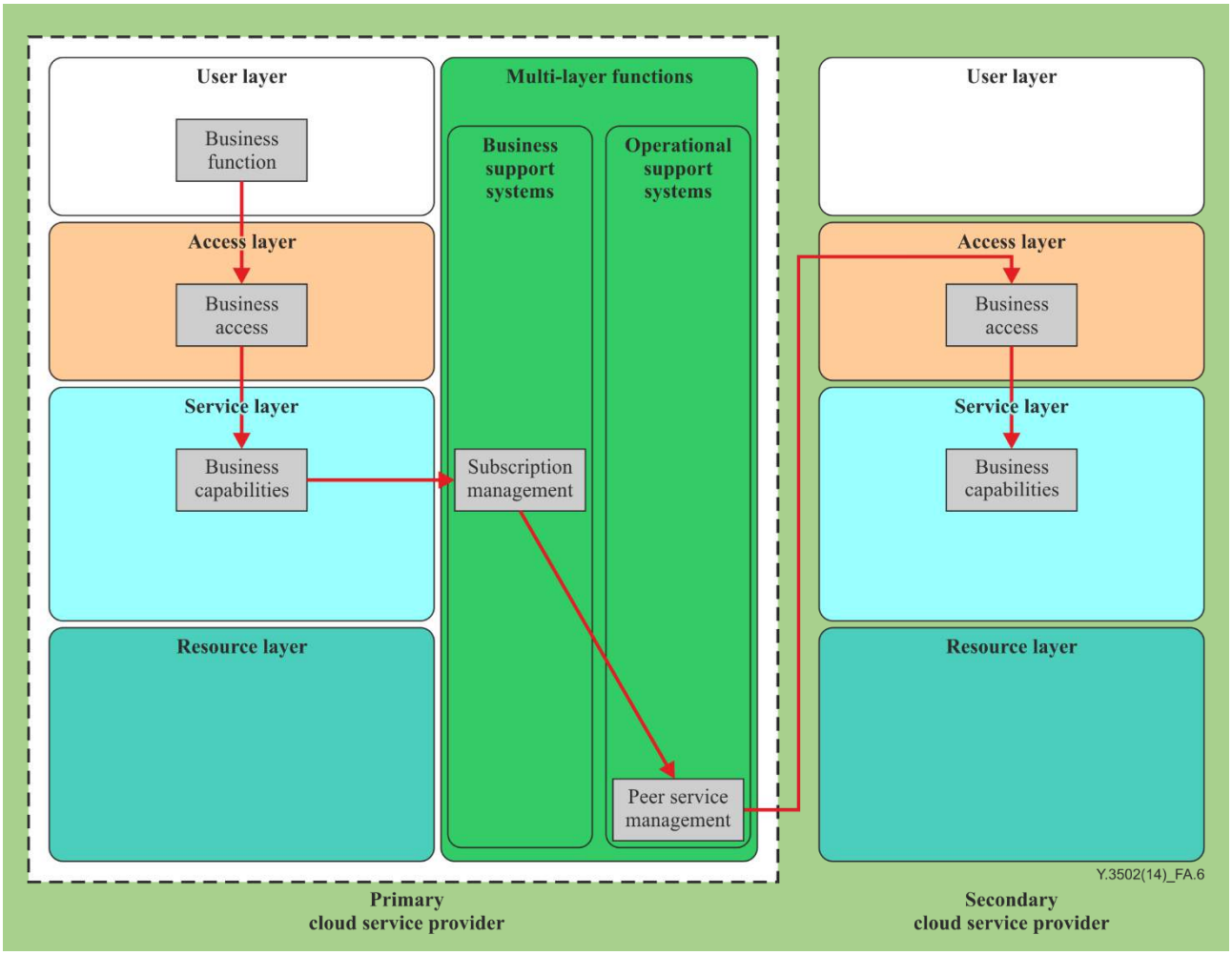


Figure A.6 – Provider–peer provider relationship for business interface

A.4 The cloud service provider–Auditor relationship

A **cloud auditor** should audit to agreed specifications, policies and agreements.

Audit specifications could be standards set by the **cloud service provider**, set by the auditor, or standards set independently, possibly as required by law. Whichever standard is used can depend on who the target of the auditor's audit result is. If the target of the audit result is a **cloud service customer** who wants some independent assurance then the audit should use an independently set standard.

Policies are set by the provider for auditing the provider's infrastructures and services. These policies are set by the business during the governance processes.

The **cloud service** agreement can include terms relating to the audit of the **cloud service provider** and possibly of the **cloud service customer**. Similar agreements can be in place between a primary **cloud service provider** and secondary **cloud service providers.** The responsibilities of the auditor are the same in each case.

The **cloud auditor's cloud computing activities** are security audit, privacy impact audit and performance audit. For all of these **cloud computing activities**, the **cloud auditor** can obtain audit evidence from the **cloud service provider**. The form of the audit evidence will vary depending on the type of audit and the standard(s) that apply to the audit. The evidence might take the form of procedural documents, or the form of log records. In any case, the **cloud service provider** can have a means by which the **cloud auditor** can obtain the required evidence.

In Figure 10-2, the perform audit **activity** of the **cloud auditor** makes requests for audit evidence to the **cloud service provider** through the administration access **functional component** of the **cloud service provider**, invoking the necessary administration capabilities.

A.4.1 Security audit

Various standards exist for system security audit. ISO/IEC 27001 is one such standard, covering **information security** management. There are also many other organizations which provide auditable standards for cloud security.

A.4.2 Privacy impact audit

Various data protection authorities (e.g., the Privacy Commissioner in Canada and the Information Commissioner in the UK) publish guidelines on the assessment and/or audit of the privacy impact of programs, policies or systems. The **protection of PII** is typically subject to regulation and/or legislation, but one of the issues relating to the **cloud service** is that the **cloud service customer** can be in a different jurisdiction to that which applies to the **cloud service provider**. The situation can be made more complex if the **cloud service provider** operates multiple data centres in different jurisdictions and moves data or service execution between these data centres (e.g., for the purposes of service continuity or for the efficient use of resources).

ISO/IEC 27018 is a standard which defines the **information security** controls applicable to a **cloud service provider** when acting as a data processor. ISO/IEC is also dealing with the wider aspects of privacy (see the ISO/IEC 29100 series of standards, for example).

A **cloud auditor** should assess the protection of **personally identifiable information** aspects of a **cloud service** and the **cloud service provider**'s operations against data protection regulations of the appropriate jurisdictions, following the guidelines issued by the data protection authorities and relevant standards.

A.4.3 Performance audit

Performance audit assesses the ability of the **cloud service provider** to meet the performance targets specified for their **cloud services**, typically documented in the **SLA**.

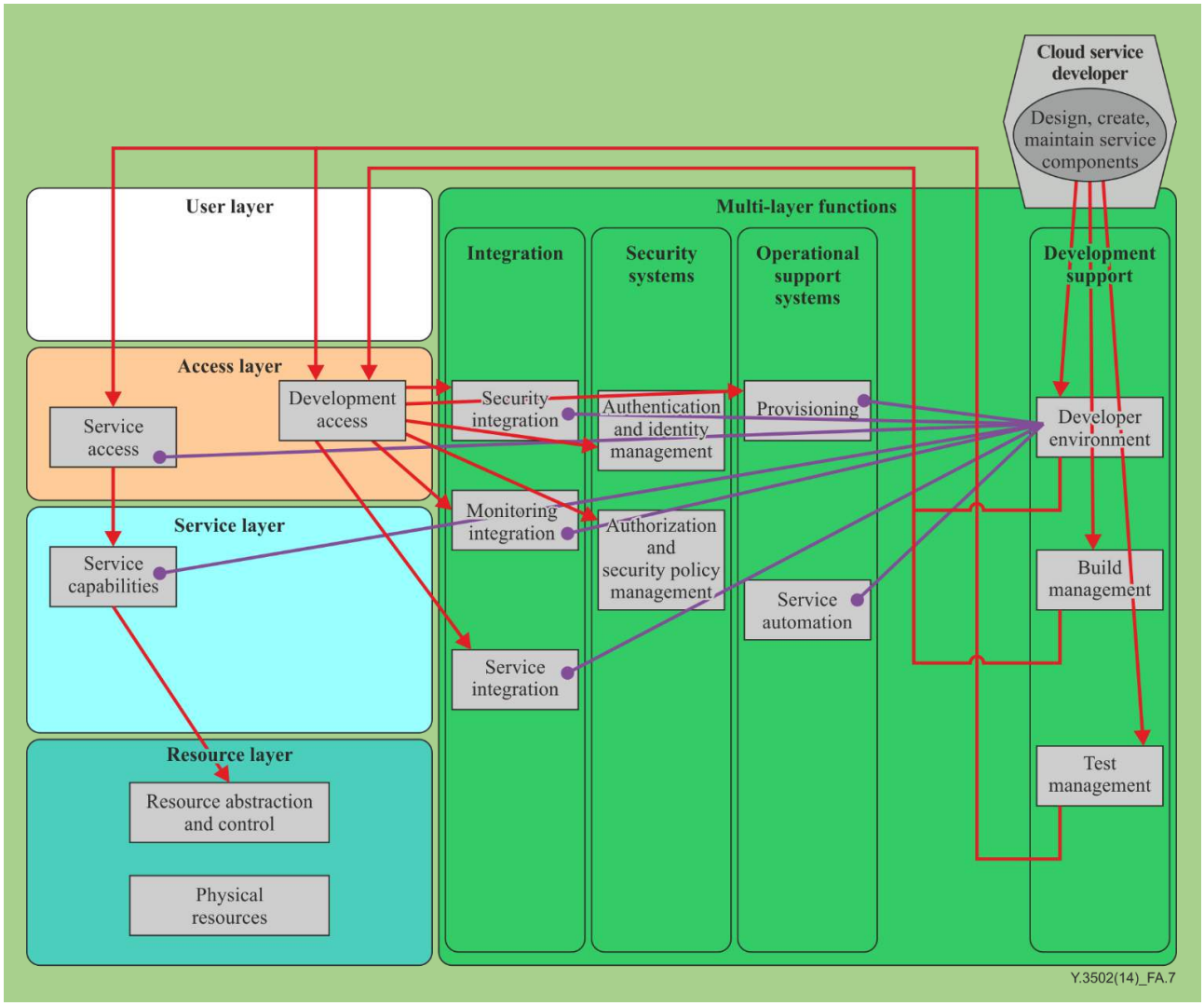


Figure A.7 – The cloud service developer–cloud service provider relationship

Bibliography

– ISO/IEC 27000:2014, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

– ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*.

– ISO/IEC 27002:2013, *Information technology – Security techniques – Information security management systems – Code of practice for information security management*.

– ISO/IEC 27018:2014, *Information technology – Security techniques – Information security management systems – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*.

– ISO/IEC/IEEE 24765:2010, *Systems and software engineering – Vocabulary*.

– ISO/IEC/IEEE 42010:2011, *Systems and software engineering – Architecture description*.

Cloud computing – Overview and functional requirements for data storage federation

Recommendation ITU-T Y.3505

(05/2018)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Summary

Recommendation ITU-T Y.3505 provides an overview and functional requirements for data storage federation. Data storage federation provides a single virtual volume from multiple data sources in heterogeneous storages. In this Recommendation, configuration for logical components and an ecosystem of data storage federation as well as cloud computing based data storage federation are introduced for data storage federation. Functional requirements are derived from use cases.

Keywords

Cloud computing, data storage federation, functional requirement.

Table of Contents

1 Scope

This Recommendation provides overview and functional requirements for data storage federation (DSF) including benefits, configuration for logical components and ecosystem of data storage federation as well as cloud computing based data storage federation. The functional requirements provided in this Recommendation are derived from use cases.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014), *Information technology – Cloud computing – Overview and vocabulary*.

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), *Information technology – Cloud computing – Reference architecture*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 **activity** [ITU-T Y.3502]: A specified pursuit or set of tasks.

3.1.2 **cloud computing** [ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications and storage equipment.

3.1.3 **cloud service customer** [ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

NOTE – A business relationship does not necessarily imply financial agreements.

3.1.4 **cloud service provider** [ITU-T Y.3500]: Party which makes cloud services available.

3.1.5 **metadata** [b-ISO/IEC 2382]: Data about data or data elements, possibly including their data descriptions, and data about data ownership, access paths, access rights and data volatility.

3.1.6 **role** [ITU-T Y.3502]: A set of activities that serves a common purpose.

3.1.7 **sub-role** [ITU-T Y.3502]: A subset of the activities of a given role.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 **data storage federation (DSF)**: A processing to provide a single virtual volume from the multiple heterogeneous data storages using storage virtualization.

NOTE – In this Recommendation, heterogeneous storage refers to DSF local storage.

3.2.2 DSF local storage: A physical storage to be integrated.

NOTE – DSF local storage includes on-premises storage such as main memory, non-volatile memory express (NVMe), solid state disk, hard disk drive, serial attached small computer system interface (SCSI), Internet SCSI storage and network-attached storage, object-based storage device, intelligent storage device, etc. and cloud storage with different management units such as block, object and file.

3.2.3 single virtual volume: A virtual storage unit provided in forms of a block device, disk, or object device.

NOTE – Customer of single virtual volume includes an end-user, server, operating system and application.

3.2.4 storage virtualization: An abstraction of storage resource to provide logical storage.

NOTE – The abstraction includes consolidating the different type of storages into a virtual storage pool as well as dividing a virtual storage pool into a single virtual volume.

3.2.5 virtual storage pool: A logical storage by integration of DSF local storage.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
CCRA	Cloud Computing Reference Architecture
CRUD	Create Read Update Delete
CSC	Cloud Service Customer
CSP	Cloud Service Provider
CSU	Cloud Service User
DMP	Data Manipulation Provider
DSF	Data Storage Federation
FTP	File Transfer Protocol
GUI	Graphical User Interface
iSCSI	Internet Small Computer System Interface
NFS	Network File System
NVMe	Non-Volatile Memory express
PCIe	Peripheral Component Interconnect express
SCSI	Small Computer System Interface
SFP	Storage Federation Provider
SFTP	SSH File Transfer Protocol
SMB	Server Message Block
SSD	Solid State Disk
SSH	Secure Shell

5 Conventions

In this Recommendation:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

6 Overview of data storage federation

6.1 Introduction to data storage federation

Increasing data services in many industries, which use big volumes of data with various data types has led to a tremendous growth in storage capacity needs. A storage user may encounter difficulties utilizing various storages due to the different access mechanisms and storage capabilities of each storage type. In order to resolve these difficulties, data storage federation (DSF) helps customers to utilize their data storages efficiently by federating heterogeneous storages including cloud storage and on-premises storage.

DSF integrates DSF local storage into a virtual storage pool and provides a single virtual volume in the virtual storage pool as shown in Figure 6-1.

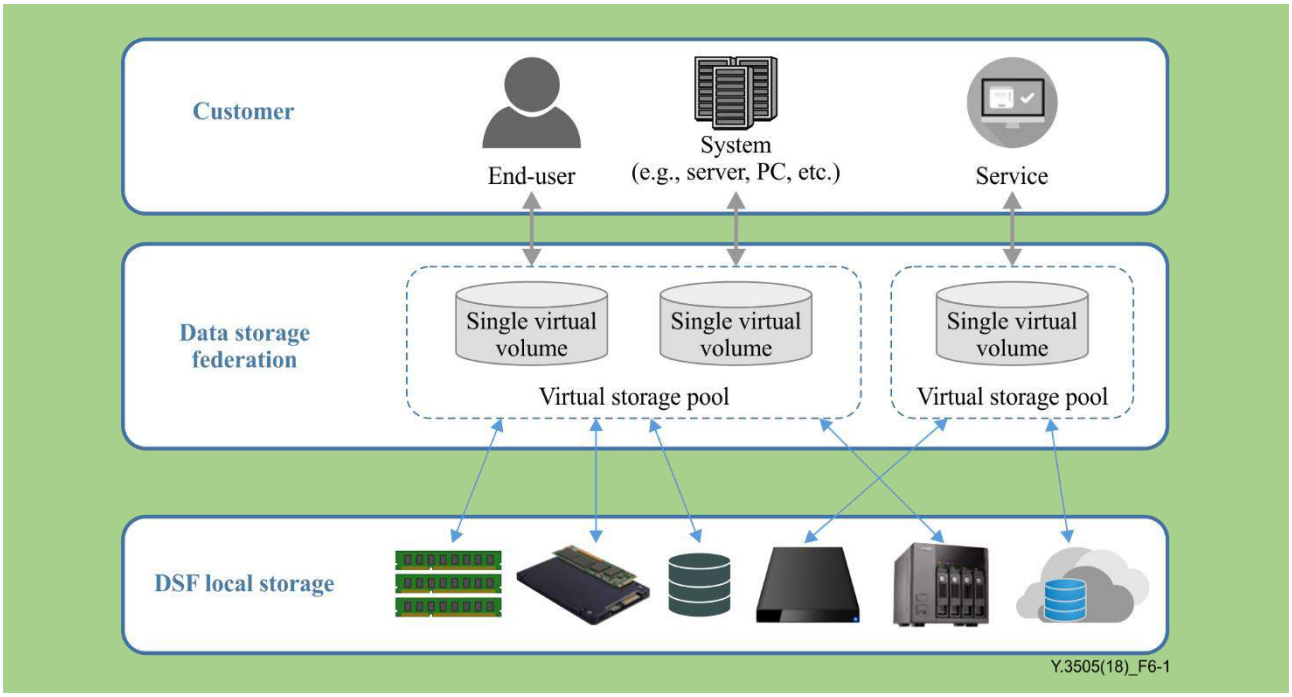


Figure 6-1 – Concept of data storage federation

DSF provides a single virtual volume for a customer with a single access point and also provides storage access mechanisms to DSF local storage.

When a customer requests the single virtual volume, DSF creates a single virtual volume in the virtual storage pool through storage operations. In accordance with customer requests to use the single virtual volume, storage operations such as creating, deleting and scaling are performed by DSF.

Examples of basic storage operations are described in detail as follows:

– **creating**: connecting DSF local storage, creating virtual storage pool and creating a single virtual volume;

– **deleting**: deleting a single virtual volume, deleting a virtual storage pool and disconnecting DSF local storage;

– **scaling**: extending a single virtual volume, extending a virtual storage pool and attaching another DSF local storage.

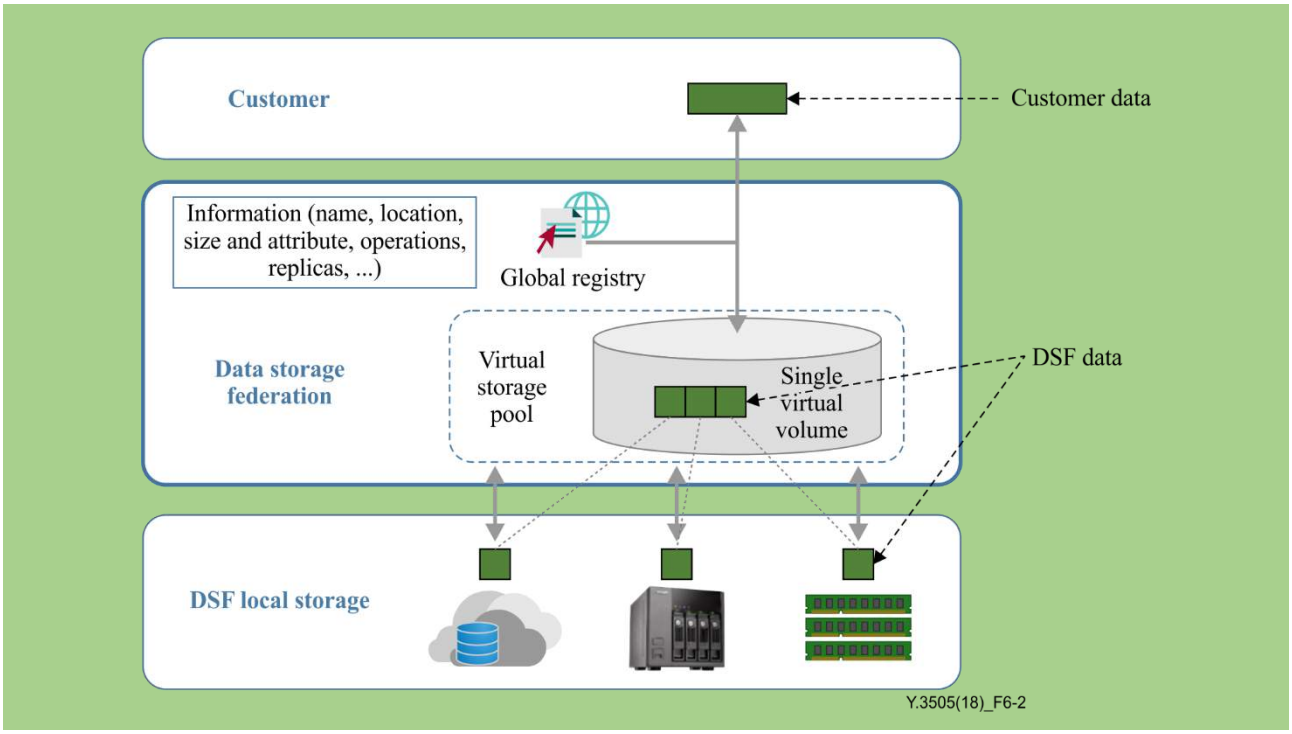


Figure 6-2 – Example of customer data manipulation in DSF

Figure 6-2 shows an example flow of customer data manipulation in DSF. When a customer stores customer data in a single virtual volume, DSF manipulates the customer data through data operations. Through the creating data operation, the customer data is fragmented into DSF data and stored in DSF local storage. The name and location of the customer data is registered to a global registry. The global registry is a data set for the information on customer data.

NOTE 1 – DSF data is a manipulated customer data in DSF and is permanently stored on DSF local storage. It includes fragmented, encrypted and compressed customer data.

NOTE 2 – The information on customer data includes the location, size and attributes, etc. This information is taken from data operation metadata and storage management metadata.

According to customer requests to use data in a single virtual volume, the basic data operations such as creating, reading, updating, deleting, searching and sharing are performed by DSF.

Examples of basic data operations in DSF are described as follows:

– **creating**: fragmenting customer data, storing it to DSF local storage and registering data name and locations to the global registry;

– **reading**: searching for a data name and location in the global registry, loading fragmented data from the DSF local storage and combining the fragmented data;

– **updating**: searching for a data name and location in the global registry, updating customer data to DSF local storage, updating changes to the global registry;

– **deleting**: searching for a data location in the global registry, removing data location from the global registry and deleting fragmented data in the DSF local storage;

– **searching**: searching for a data name in the global registry;

– **sharing**: searching for a data name and changing an attribute in the global registry to share data.

6.2 Benefits of data storage federation

DSF provides not only a single virtual volume federated from DSF local storage, but also from a customer perspective beneficial features such as cost, technical function, service enhancement and resource utilization. Beneficial features include:

– **Easy storage management**: simplified management by using a single user interface and centralized monitoring.

– **Cost-effectiveness**: reduction of storage usage costs by moving rarely used customer data to a cheaper DSF local storage.

– **Performance enhancement**: improvement of data access performance by storing data to high-speed storages such as solid state disk (SSD), main memory, etc.

– **Data reliability**: increased reliability by replicating the data storing to another DSF local storage.

– **Storage scalability**: support of on-demand storage capacity by scaling storage resources.

– **Storage utilization efficiency**: increased of storage capacity by combining two or more DSF local storages to store a large sized file.

– **Data security**: stores secure data by splitting important files into multiple fragments and storing them on different DSF local storages.

– **Data management transparency**: convenient data management for data discovery, use of data without knowledge of data location, storage type and data format.

6.3 Configuration of logical components for data storage federation

Figure 6-3 shows the general configuration environment for logical components of DSF. The logical components consist of customer, storage connection, data manipulation, data distribution and storage, DSF local storage management, provision and policy management and DSF local storage including cloud and on-premises storage.

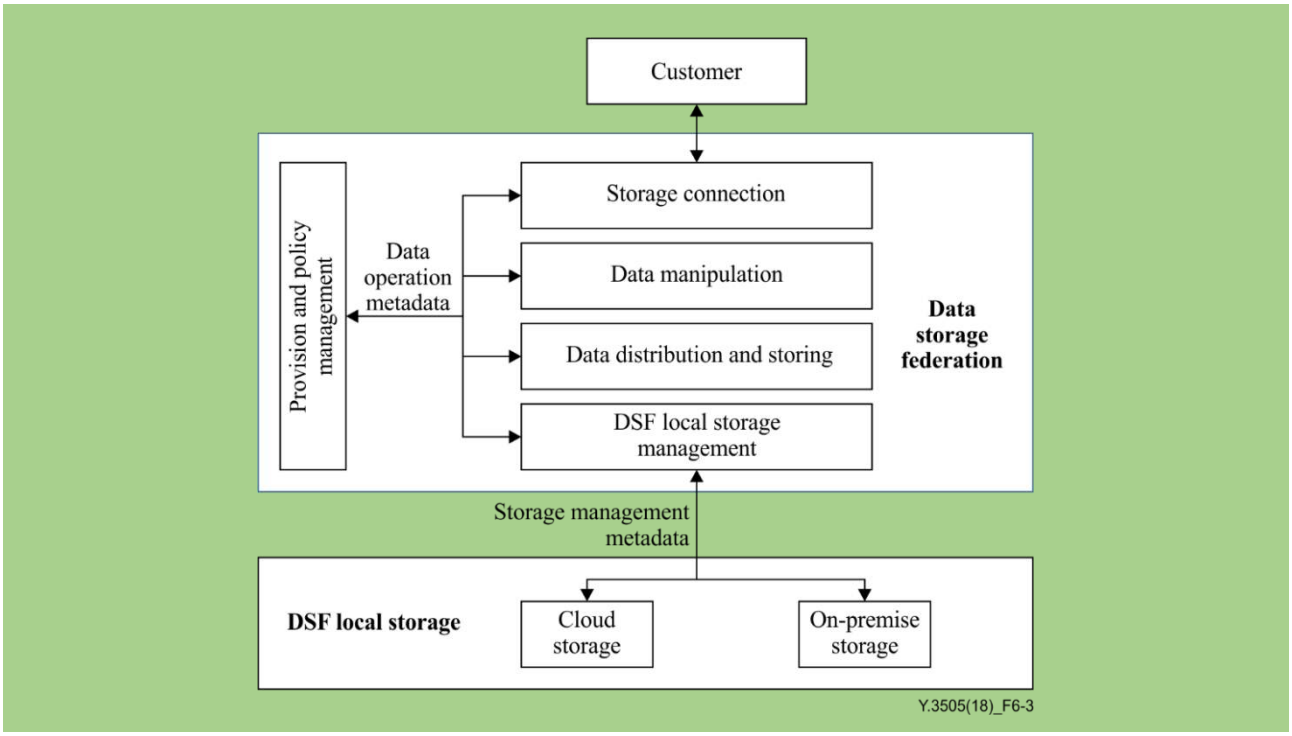


Figure 6-3 – General configuration for DSF

Storage connection component provides:

– an interface for a single virtual volume for a customer;

– a customer access mechanism to connect a single virtual volume;

NOTE 1 – The customer access mechanism includes the different types of protocols according to the storage type such as Internet small computer system interface (iSCSI) for block device storage, server message block (SMB), network file system (NFS), SSH file transfer protocol (SFTP), file transfer protocol (FTP) for file-based storage and the restful API for object-based storage, etc.

– corresponding protocols or I/O interfaces of a single virtual volume;

– performance acceleration of protocols.

Data manipulation component provides:

– virtual storage pool;

– configuration for virtual storage pool without considering the actual storage location of the data;

– the write buffer or read cache function for customer data;

– enhancement of the read and write response time using high-speed storages for buffer and cache;

NOTE 2 – The high-speed storage includes main memory, non-volatile memory express (NVMe), SSD and peripheral component interconnect express (PCIe) flash cards.

– data management for snapshots, fast replication and distributed transaction logs.

Data distribution and storing component provides:

– the optimization of writing data to DSF local storage to minimize writing and accessing time;

– data fragmentation to distribute and store in DSF local storage;

NOTE 3 – Data fragmentation is a method to distribute and store customer data in other storages.

– the encryption/decryption and compression/decompression of data fragments;

NOTE 4 – The encryption and compression are taken into account by customer's demands.

DSF local storage management component provides:

– connections to DSF local storage;

– storage tiering of data according to the storage performance, time of data usage and data access frequency;

NOTE 5 – Storage tiering is the action to distribute and collocate data across multiple storage tiers in a hierarchical manner.

NOTE 6 – This component automatically moves data between the various storage tiers according to the characteristics of the data.

NOTE 7 – When data is initially created, it is stored in high-speed storage. When data access frequency is low, it is moved to a lower-speed storage.

Provisioning and policy management component provides:

– the configurations and controls of logical components;

– the policy management of data storage and data manipulation;

NOTE 8 – Policy for data storage includes back-up, snapshot, scaling, recovery, data caching, thin-provisioning, tiering, storage type (file, block, object), etc.

NOTE 9 – Policy of data manipulation includes sharing support, read/write, replication, data migration, fragmentation, encryption, compression, de-duplication, etc.

– the provision of single virtual volume in a virtual storage pool.

Two kinds of metadata are shown in Figure 6-3 as follows:

– Data operation metadata is a description required to perform data operations. It includes the attributes of virtual storage pool and single virtual volume. It includes a transaction log and DSF data attributes of read/write caching, snapshot, replication, fragmentation, etc.

– Storage operation metadata is a description required to perform storage operations. It includes the location of DSF local storage, interface, API for customer data operation, read/write speed, storage capacity, etc.

6.4 Ecosystem of data storage federation

This clause identifies roles and sub-roles of the DSF ecosystem. In addition, relationships among roles and sub-roles are specified.

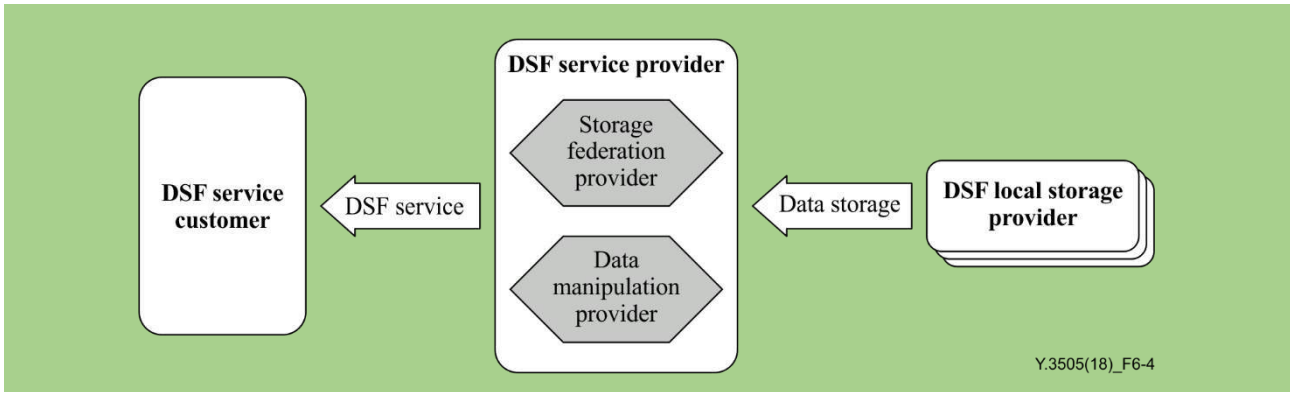


Figure 6-4 – Data storage federation ecosystem

DSF service is a service to provide single virtual volumes and policies and it is offered by a DSF service provider.

The DSF ecosystem includes the following roles as shown in Figure 6-4:

– DSF service customer;

– DSF service provider;

– DSF local storage provider.

6.4.1 DSF service customer

The DSF service customer uses a DSF service including a single virtual volume and policies from a DSF service provider. A DSF service customer's activity includes:

– Use of DSF service.

6.4.2 DSF service provider

The DSF service provider federates DSF local storages and provides a DSF service with an access mechanism.

The DSF service provider role consists of two sub-roles:

– Storage federation provider;

– Data manipulation provider.

6.4.2.1 Storage federation provider

The storage federation provider (SFP) provides a single virtual volume by federation of DSF local storages. A storage federation provider's activities include:

– provide virtual storage pool;

– provide single virtual volume;

– manage storage management metadata;

– manage data storage policy.

6.4.2.2 Data manipulation provider

The data manipulation provider (DMP) provides DSF data by manipulation and manages data operation metadata and data manipulation policy (see clause 6.3). A data manipulation provider's activities include:

– manipulate DSF data;

– manage data operation metadata;

– manage data manipulation policy.

6.4.3 DSF local storage provider

The DSF local storage provider provides DSF local storage and interfaces to use it. A DSF local storage provider's activity includes:

– provide DSF local storage.

7 Cloud computing based data storage federation system context

This clause describes how cloud computing can support the three main roles of the DSF ecosystem: DSF service customer, DSF service provider and DSF local storage provider.

By using cloud computing roles, sub-roles and activities, cloud computing based DSF supports more extensible features by facilitating on-premises storage resources which connect personal and enterprise storage resources.

The cloud computing based DSF context is defined with new sub-roles and activities based on cloud computing reference architecture (CCRA) [ITU-T Y.3502]. For cloud computing based DSF, CSP:storage federation provider (CSP:SFP) for federation of DSF local storage and CSP:data manipulation provider (CSP:DMP) for management of DSF data and policies are defined to utilize DSF local storage as shown in Table 7-1.

Table 7-1 – Mapping roles and sub-roles between data storage federation ecosystem and cloud computing based DSF system context

Roles and sub-roles of data storage federation ecosystem	Sub-roles of cloud computing based data storage federation system context
DSF service customer	CSC: cloud service user (CSC:CSU)
DSF service provider : storage federation provider, DSF service provider : data manipulation provider	CSP: storage federation provider (CSP:SFP), CSP: data manipulation provider (CSP:DMP)
DSF local storage provider	CSP: cloud service manager (CSP:CSM)

Figure 7-1 illustrates the cloud computing sub-roles related to DSF. This figure also identifies activities specific for DSF and assigns them to cloud computing sub-roles and illustrates how cloud computing supports DSF service from the perspective of CSP:SFP and CSP:DMP. The cloud computing based DSF utilizes other sub-roles of CSP.

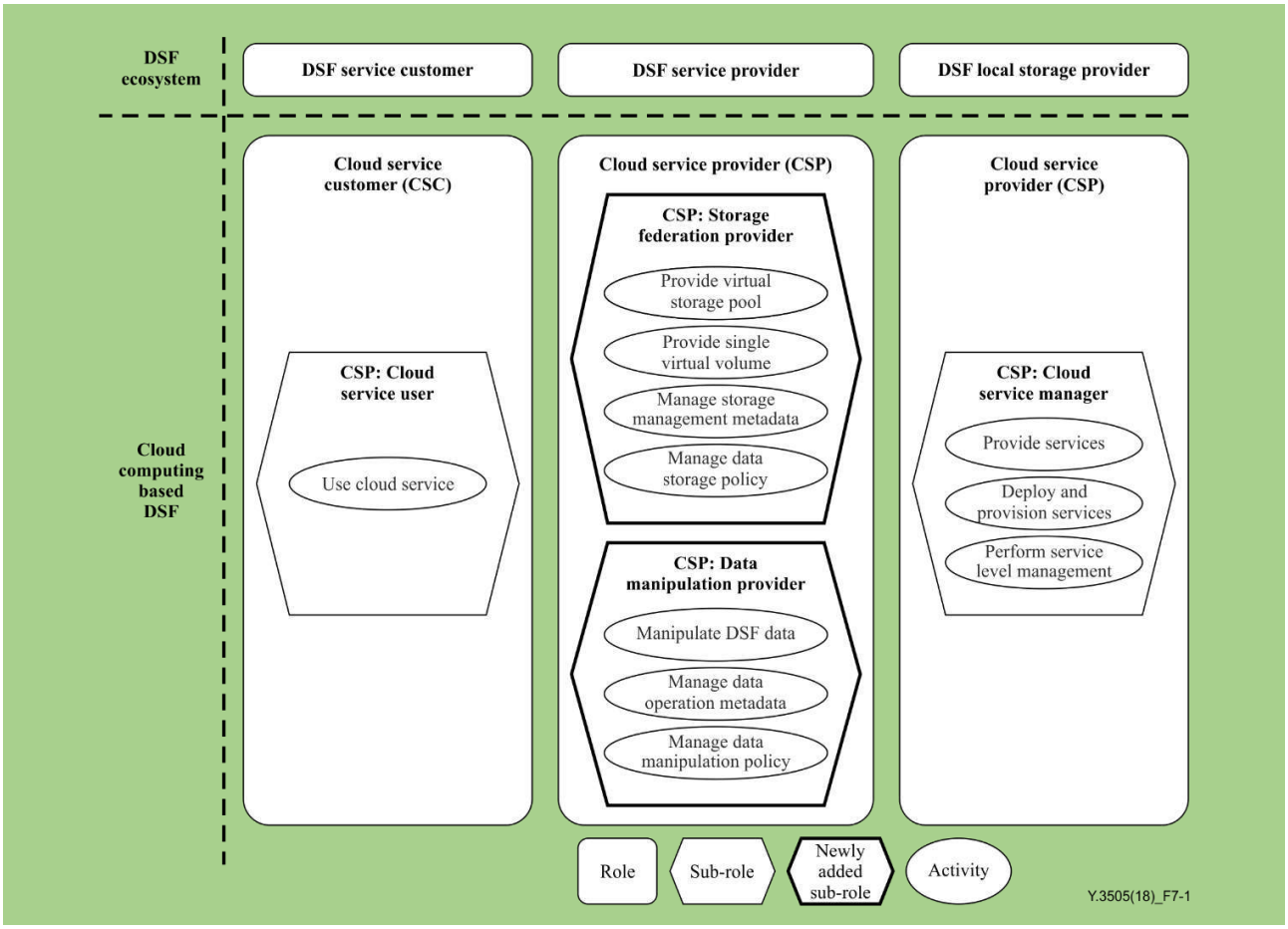


Figure 7-1 – Cloud computing based DSF context and its relationship with DSF ecosystem

7.1 CSP:storage federation provider (CSP:SFP)

CSP:storage federation provider (CSP:SFP) is responsible for the federation of DSF local storage. CSP:SFP's activities include:

– provide virtual storage pool;
– provide single virtual volume;
– manage storage management metadata;
– manage data storage policy.

7.1.1 Provide virtual storage pool

This activity involves integrating and managing DSF local storage to make a logical storage.

This activity involves:

– performing storage operation (see clause 6.1);
– managing virtual storage pool;
– delegating customer credentials of DSF local storage.

7.1.2 Provide single virtual volume

This activity involves providing and processing a way to use a single virtual volume for a CSC:CSU.

This activity involves:

– managing single virtual volume;
– providing a user access mechanism for CSC:CSUs;
– performing storage operation (see clause 6.1).

7.1.3 Manage storage management metadata

This activity involves creating, updating and deleting metadata (see clause 6.3) for a virtual storage pool and single virtual volume.

This activity involves:

– creating storage management metadata of DSF data;
– updating storage management metadata on changes;
– deleting storage management metadata.

7.1.4 Manage data storage policy

This activity involves management of data storage policy.

This activity involves:

– creating data storage policy;
– triggering data storage policy;
– updating data storage policy;
– deleting data storage policy.

7.2 CSP:data manipulation provider (CSP:DMP)

CSP:data manipulation provider (CSP:DMP) is responsible for operation for DSF data and management of data manipulation policy. CSP:DMP's activities include:

– manipulate DSF data;
– manage data operation metadata;
– manage data manipulation policy.

7.2.1 Manipulate DSF data

This activity involves DSF data operation for CSC:CSU by data virtualization.

This activity involves:

– performing data operation (see clause 6.1).

NOTE 1 – Data virtualization is an abstraction of multiple data resources into the logical data resource.

NOTE 2 – Multiple data resources include object storage, file storage and block storage.

7.2.2 Manage data operation metadata

This activity involves creating, updating and deleting metadata (see clause 6.3) for DSF data.

This activity involves:

– creating data operation metadata of DSF data;
– updating data operation metadata on changes;
– deleting data operation metadata.

7.2.3 Manage data manipulation policy

This activity involves management of data manipulation policy.

This activity involves:

– creating data manipulation policy;
– triggering data manipulation policy;
– updating data manipulation policy;
– deleting data manipulation policy.

8 Functional requirements for data storage federation

This clause describes the requirements for data storage federation.

8.1 Storage connection requirements

(1) It is required that CSP:SFP provide an interface to connect DSF local storage.

NOTE 1 – The interface to DSF local storage refers to the direct interfaces (i.e., object or block storage interface), or a proxy interface to configure several types of storages interface with a software program.

NOTE 2 – The software program includes software agent, daemon, web worker and RESTful API for an interface to DSF local storage.

NOTE 3 – The proxy interface connects DSF local storage by automatically detecting the interface with a software program.

(2) It is required that CSP:SFP provide a user interface for CSC:CSU to use a single virtual volume.

NOTE 4 – User interface includes graphical user interface, web application, or specific client for CSC:CSU to access a single virtual volume.

(3) It is recommended that CSP:SFP support the change of CSC:CSU's access mechanism according to the storage type of single virtual volume.

(4) It is required that CSP:DMP provide translation between data operation and a corresponding interface of DSF local storage.

NOTE 5 – Corresponding interface include API, I/O interface, etc.

(5) It is recommended that CSP:SFP provide a secure access mechanism to use a single virtual volume for CSC:CSU.

(6) It is required that CSP:DMP provide the registration of the CSC:CSU's requirements.

NOTE 6 – The requirements of CSC:CSU include data storage capacity, access mechanism, storage types of single virtual volume, policy, etc.

(7) It is required that CSP:SFP provide the seamless connection of DSF local storage interface to communicate with DSF local storage.

8.2 Data manipulation requirements

(1) It is required that CSP:DMP provide the execution of CSC:CSU's create, read, update, delete (CRUD) data operation.

NOTE 1 – CRUD data operation includes create, read, update and delete data.

(2) It is required that CSP:DMP provide a search data operation from CSC:CSU's data using query to a global registry.

(3) It is recommended that CSP:DMP provide a sharing data operation by updating of sharing status of DSF data in a global registry after checking sharing status of DSF data.

NOTE 2 – Data sharing means that the same DSF data is shared during data operation.

NOTE 3 – Sharing status of DSF data is information about whether DSF data is shared or not.

(4) It is recommended that CSP:DMP provide the capacity saving of data storage using de-duplication of DSF data.

(5) It is recommended CSP:DMP provide DSF data encryption/decryption for data transfer to DSF local storage.

(6) It is required that CSP:DMP provide data recovery of CSC:CSU from system failure.

NOTE 4 – Data recovery refers to restoring the most recently used CSC:CSU's data preventing data loss due to errors from the storage and network connection failure.

(7) It is recommended that CSP:DMP provide DSF data migration to available DSF local storage for resilience and cost efficiency of the storage space.

NOTE 5 – The data migration for the resilience and cost efficiency of the data storage space is automatically performed without user intervention or recognition.

(8) It is required that the CSP:DMP provide the validation of DSF data on data operation to check the data integrity.

(9) It is required that CSP:DMP support CSC:CSU's data consistency for replicated DSF data.

NOTE 6 – The data consistency means that CSP:DMP correctly backup current DSF data in order to recover CSC:CSU's data on storage failure.

(10) It is required that CSP:DMP support CSC:CSU's data transparency.

NOTE 7 – The data transparency means to access CSC:CSU's data without knowing location.

8.3 Storage federation requirements

(1) It is recommended that CSP:SFP provide the performance information of DSF local storage from storage management metadata.

NOTE 1 – Performance information are read/write I/O speed, network bandwidth, storage capacity, storage types, etc.

(2) It is recommended that CSP:SFP provide virtual storage pool optimization considering the performance of DSF local storage.

NOTE 2 – Virtual storage pool optimization includes storage mirroring, storage prioritization, CSC:CSU's access geo-location and their combinations.

(3) It is recommended that CSP:SFP provide single virtual volume optimization based on CSC:CSU's purpose.

NOTE 3 – Single virtual volume optimization include storage size, data safety, storage performance, mobility of the usage environment and their combinations.

(4) It is required that CSP:SFP provide the configuration of single virtual volume from CSC:CSU requests.

(5) It is required that CSP:SFP provide a read/write cache to access data.

NOTE 4 – The read/write cache enables to enhance the performance of the storage and the device storing the data is used by various devices for fast cache operation.

NOTE 5 – The various devices for fast cache are main memory, RAM based disk, SSD, etc.

(6) It is recommended that CSP:SFP provide hierarchical cache management using cache multi-tiering.

NOTE 6 – Cache multi-tiering means that for the high-speed access, cache hierarchy is extended to various devices for fast caching.

NOTE 7 – For capacity limit, if a main-memory cache area is exhausted, it is automatically expanded to a RAM based disk cache and expanded to SSD cache.

NOTE 8 – When CSC:CSU performs the data operation, the data operation is performed in the memory area in advance for fast write response.

(7) It is required that CSP:SFP provide the backup of global registry for high availability.

NOTE 9 – The backup of the global registry is synchronized with most recently updated CSC:CSU's data.

(8) It is recommended that CSP:SFP provide in-parallel access to DSF local storage.

(9) It is required that CSP:SFP provide the registration of CSC:CSU's credentials to a DSF local storage.

(10) It is recommended that CSP:SFP support monitoring the performance information of DSF local storage.

(11) It is required that CSP:SFP provide the management of DSF local storage interface.

(12) It is recommended that CSP:SFP support access to the secured storage interface for DSF local storage.

(13) It is required that CSP:SFP provide the storage operation for DSF local storage.

NOTE 10 – Storage operation for DSF local storage includes create, delete, scaling, partitioning and checking volume, etc.).

(14) It is required that CSP:SFP provide scaling of single virtual volume on CSC:CSU demand.

8.4 Metadata and policy management requirements

(1) It is recommended that CSP:SFP provide a configuration of a single virtual volume by data storage policy for CSC:CSU.

(2) It is recommended that CSP:SFP provide default data storage policies when policy is not configured.

NOTE 1 – Default data policy is reconfigured by customer's requests.

(3) It is recommended that CSP:DMP provide a transformation of DSF data by data manipulation policy.

NOTE 2 – Data manipulation policy for transformation of DSF data includes the policies of fragmentation, encryption, compression, de-duplication, etc.

(4) It is recommended that CSP:DMP provide a default data manipulation policy.

(5) It is required that CSP:SFP provide a global registry for customer data access.

(6) It is required that CSP:SFP provide high-speed access of global registry.

(7) It is required that CSP:DMP provide management of data operation metadata automatically according to execution of data operation.

(8) It is required that CSP:SFP provide storage management metadata to communicate with DSF local storage.

9 Security considerations

It is recommended that the security framework for cloud computing described in [b-ITU-T X.1601] be considered for data storage federation. [b-ITU-T X.1601] analyses security threats and challenges in the cloud computing environment and describes security capabilities that could mitigate these threats and meet security challenges.

[b-ITU-T X.1631] provides guidelines supporting the implementation of information security controls for cloud service customers and cloud service providers. Many of the guidelines guide the cloud service providers to assist the cloud service customers in implementing the controls and guide the cloud service customers to implement such controls. Selection of appropriate information security controls and the application of the implementation guidance provided, will depend on a risk assessment as well as any legal, contractual, regulatory or other cloud-sector specific information security requirements.

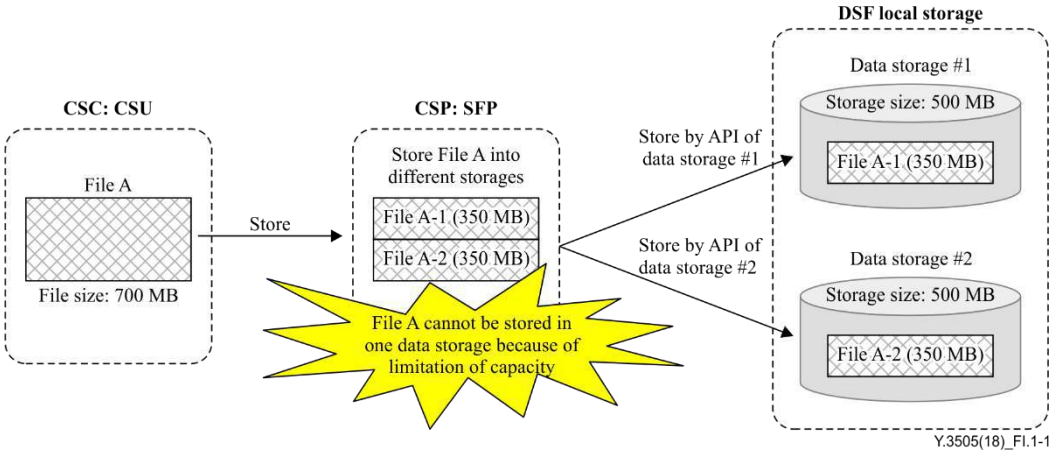
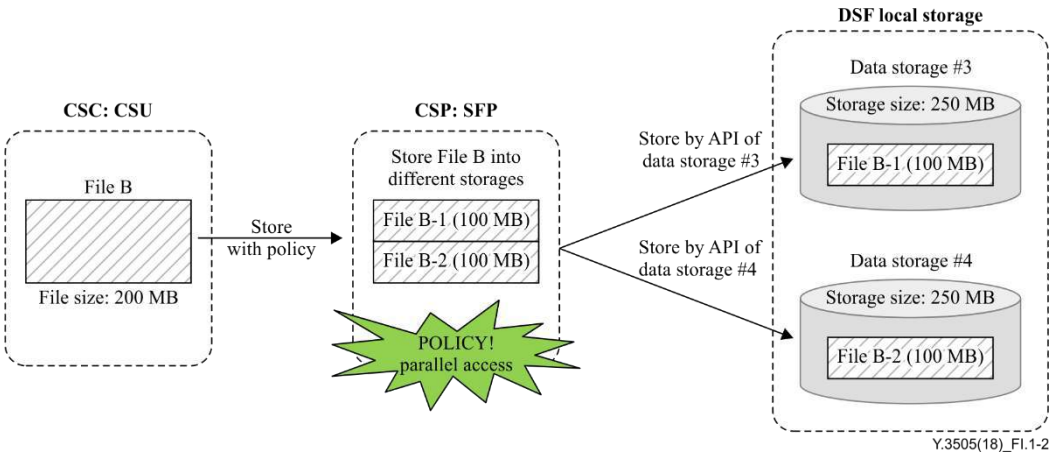
It is also recommended that the guidelines for cloud service customer data security described in [b-ITU-T X.1641] be considered. It provides generic security guidelines for the cloud service customer (CSC) data in cloud computing, analyses the CSC data security lifecycle and proposes security requirements at each stage of the data lifecycle.

Appendix I

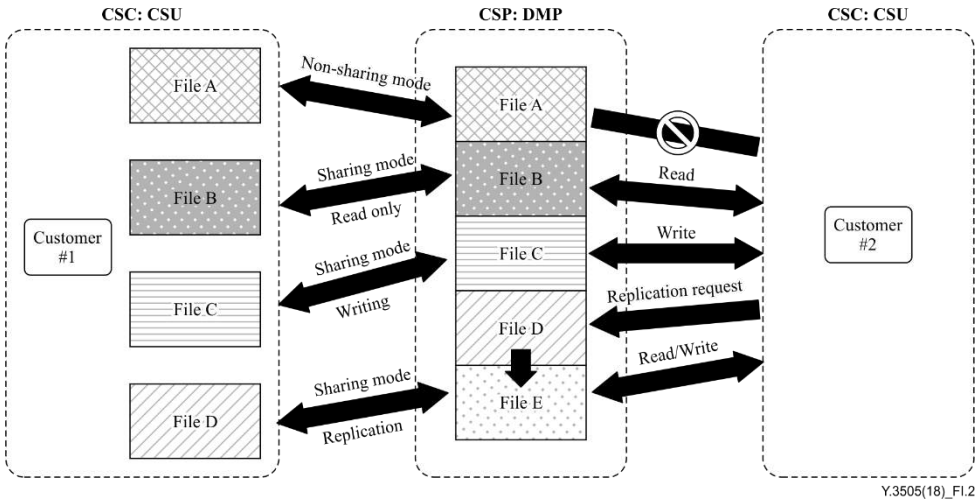
Use case of data storage federation

(This appendix does not form an integral part of this Recommendation.)

I.1 Storing a user file dispersedly

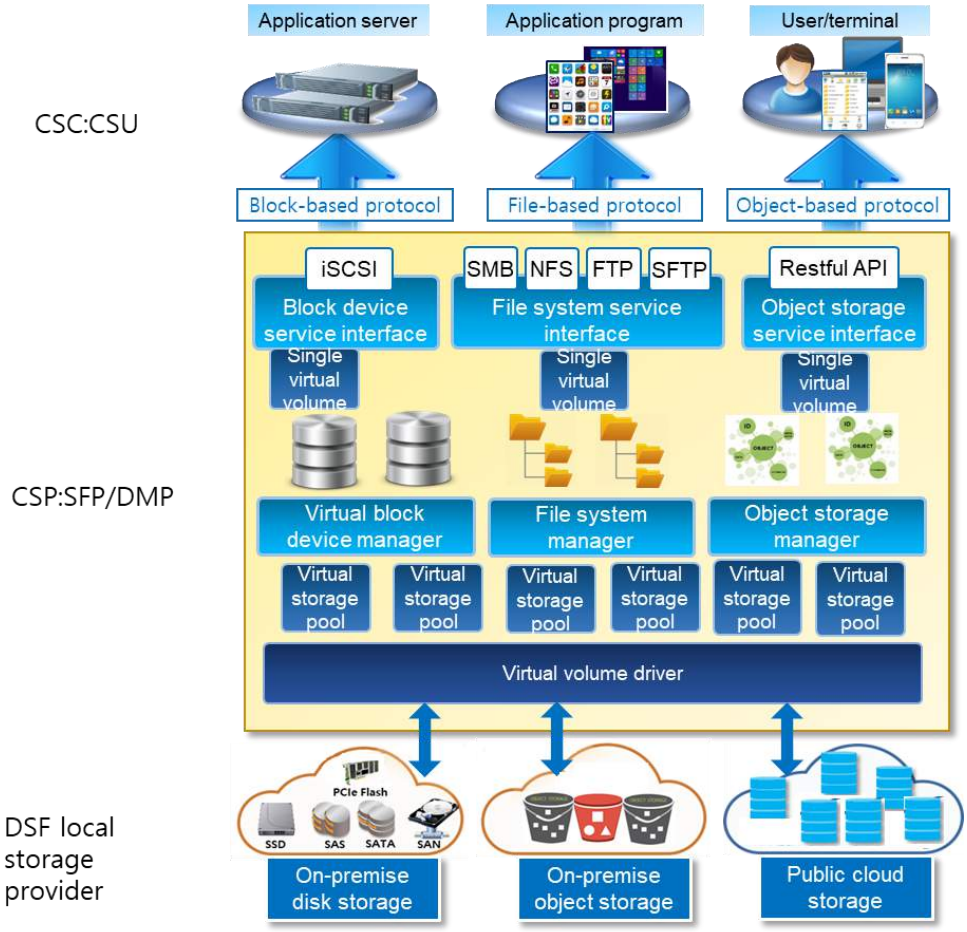
Title	Storing a user file dispersedly
Description	In this scenario, a data storage customer having two data storages on DSF local storage requests a large file storing from a DSF service provider. The DSF service provider splits the file into several parts in case that DSF local storage have not enough space (Case 1) or needs to access it in parallel for better performance (Case 2) and stores the parts into different distributed DSF local storages.
Role/Sub-role	DSF service provider (CSP:SFP) DSF service customer (CSC:CSU)
Figure (optional)	Case 1: limited capacity of data storage in DSF local storage  Case 2: CSC:CSU's parallel access requirement 
Pre-conditions (optional)	– CSP:SFP is available to access DSF local storage. – CSC:CSU requests a single virtual volume to CSP:SFP.
Post-conditions (optional)	
Derived requirements	– Clause 8.1 requirement (2) – Clause 8.4 requirement (2) – Clause 8.1 requirement (4)

I.2 Data sharing between customers

Title	Data sharing between customers
Description	In this scenario, the DSF service customer #1 stored file A~D with data sharing mode policy setting. The file A is non-sharing mode, the file B is read-only data sharing mode, the file C is over-writable data sharing mode and the file D is replicable data sharing mode. The other DSF service customer #2 uses file A~D with data sharing policy set by DSF service customer #1. DSF service customer #2 cannot access file A because of non-sharing mode policy setting and DSF service customer #2 can read file B but it is not writable. In file C case, DSF service customer #2 can overwrite it and store it with changes. In file D case, by a replication request by DSF service customer #2, the original file D is preserved and a new file E is generated and stored to DSF service customer #2's single virtual volume.
Role/sub-role	DSF service provider (CSP:DMP) DSF service customer (CSC:CSU)
Figure (optional)	
Pre-conditions (optional)	
Post-conditions (optional)	
Derived requirements	– Clause 8.1 requirement (2)

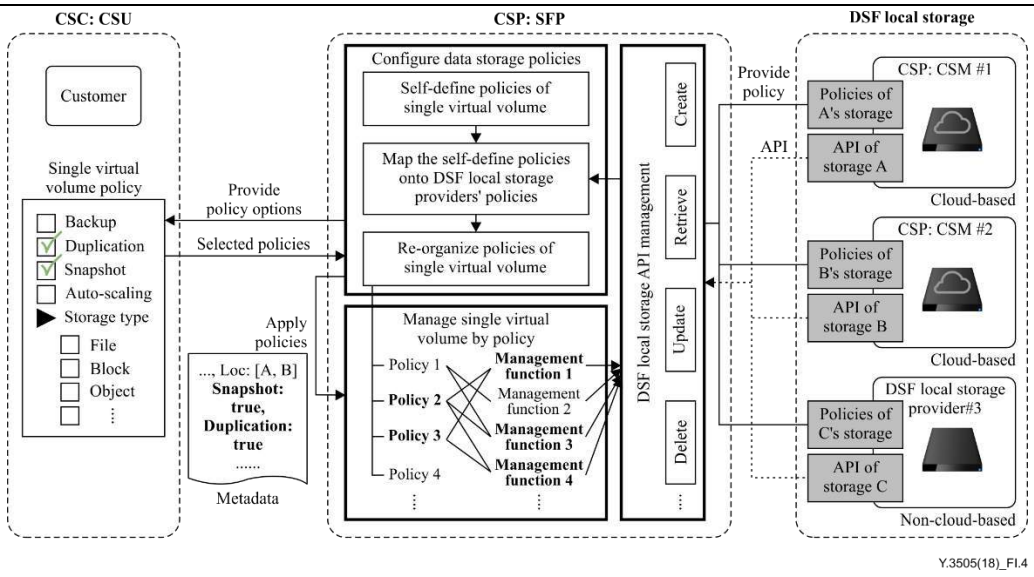
I.3 Multiple storage types and access mechanisms for data access

Title	Multiple storage types and access mechanisms for data access
Description	In this scenario, a DSF service customer requests a variety of service interfaces and storage types from a DSF service provider. Also, the DSF service provider provides service interfaces to the DSF service customer with the corresponding access mechanisms.
Role/Sub-role	DSF service customer (CSC:CSU) DSF service provider (CSP:SFP, CSP:DMP)

Figure (optional)	
Pre-conditions (optional)	– CSC:CSU use its own storage types – CSC:CSU can be general users (which own storage individually), some application programs, application servers and another cloud system.
Post-conditions (optional)	
Derived requirements	– Clause 8.4 requirement (3) – Clause 8.1 requirement (3)

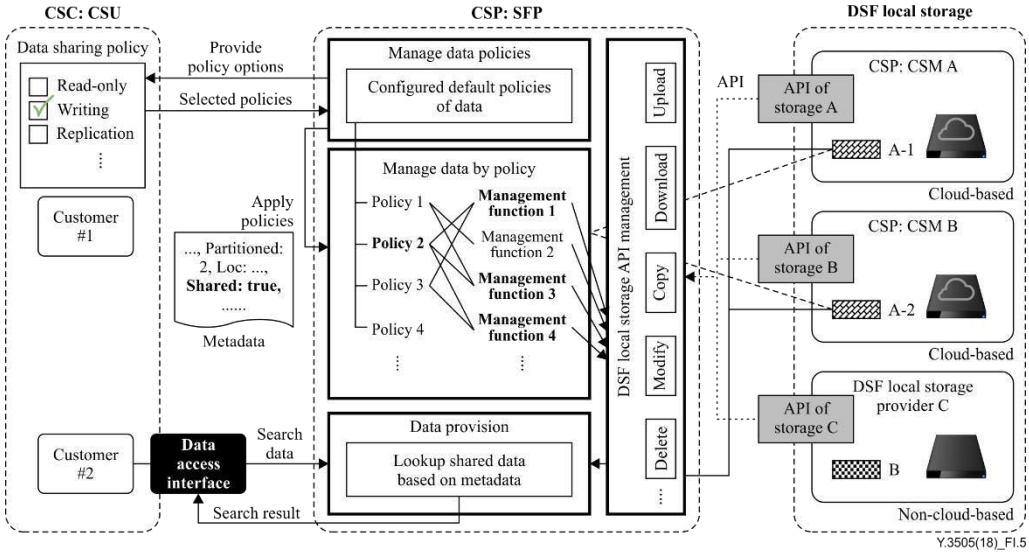
I.4 Policy-driven provision and management of DSF local storage

Title	Policy-driven provision and management of DSF local storage
Description	A DSF service provider manages and provides a single virtual volume based on DSF local storage policies. The DSF service provider organizes DSF local storage policies by using default policies configured by DSF service provider and re-configured by DSF service provider from multiple data storages. That is, the DSF service provider's policies are dependent on storage provider storage policies in DSF local storage. DSF service provider provides the default policies as multiple options (e.g., backup, replication, snapshot, auto-scaling and storage type). DSF service customer selects options and DSF service provider applies options onto metadata. The options are matched onto corresponding storage policies in DSF local storage. The DSF service provider manages the DSF local storage by matched functions onto storage policies. All communications with DSF local storage between the DSF service provider and DSF local storage provider are performed by storage APIs.

Role/Sub-role	DSF service customer (CSC:CSU) DSF service provider (CSP:SFP, CSP:DMP) DSF local storage provider (CSP:CSM)
Figure (optional)	
Pre-conditions (optional)	
Post-conditions (optional)	
Derived requirements	– Clause 8.4 requirement (1) – Clause 8.4 requirement (4)

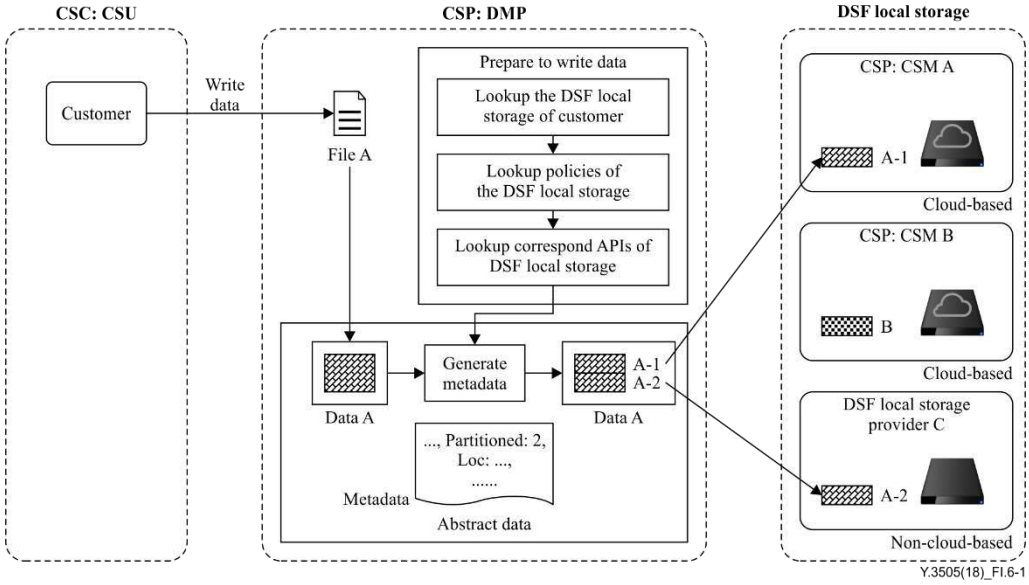
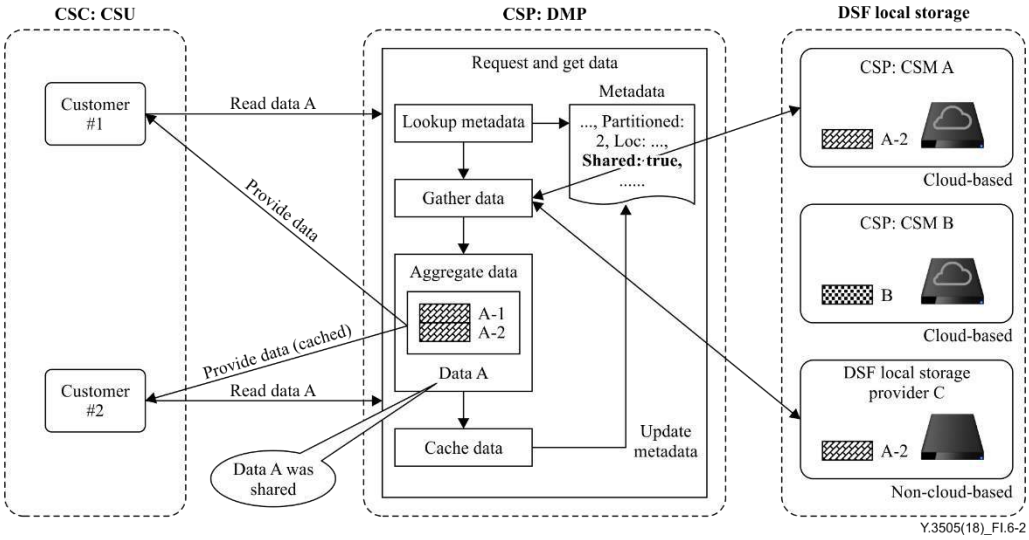
I.5 Policy-driven provisioning and management of data

Title	Policy-driven provisioning and management of data
Description	DSF service provider provides a **unified** interface to use DSF local storage and options to set data manipulation policies. DSF service provider configures the data manipulation policies because the data manipulation policies are independent from multiple data storages in DSF local storage. DSF service customer uses a single virtual volume (e.g., upload, download, copy, modify, delete and so on) and sets data manipulation policies (e.g., non-sharing, read-only, overwrite, replicate and so on) to saved files. DSF service provider applies data manipulation policies onto data operation metadata. DSF service provider manipulates data by corresponding functions and APIs with data manipulate policies. DSF service customer #1 sets data manipulation policy. DSF service provider modifies data operation metadata of target data. Another DSF service customer (e.g., DSF service customer #2) searches and gets data by using catalogue. In this procedure, the data operation metadata is used in order to lookup data from DSF local storage.
Role/Sub-role	DSF service customer (CSC:CSU) DSF service provider (CSP:SFP) DSF locals storage provider (CSP:CSM)

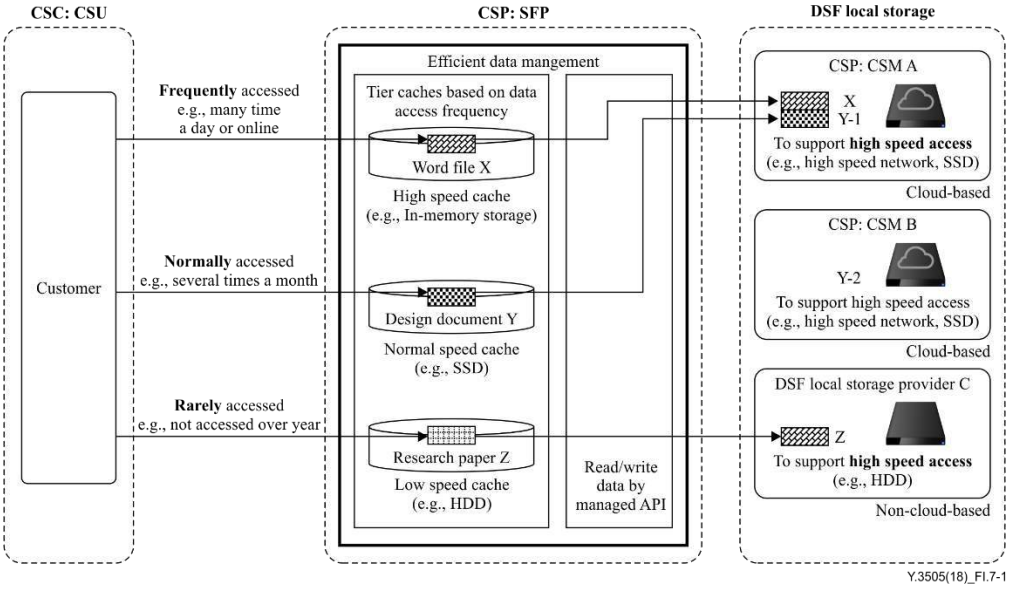
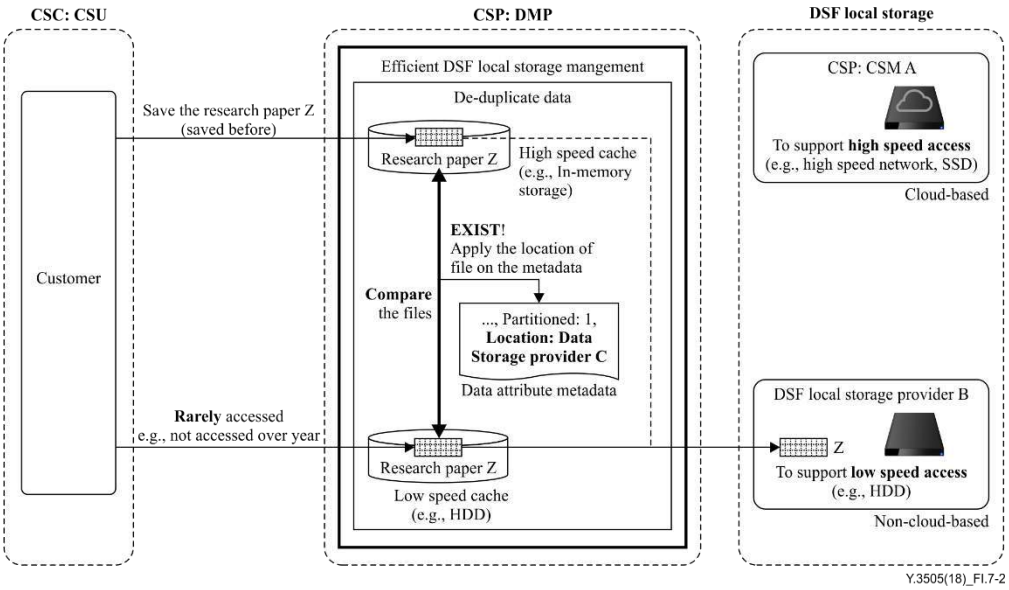
Figure (optional)	
Pre-conditions (optional)	– Policies for data storage are configured by CSP:SFP and selected by CSC:CSU, or set to default. – CSC:CSU save files on a single virtual volume.
Post-conditions (optional)	
Derived requirements	– Clause 8.1 requirement (7) – Clause 8.2 requirement (2) – Clause 8.2 requirement (3)

I.6 Data virtualization CSP:SFP

Title	Data virtualization by CSP:SFP
Description	This scenario shows data virtualizations through the description of read and write data. DSF service customer #1 writes a file through the DSF service. DSF service provider prepares to write data because file A, shown in Figure 1, is saved on a single virtual volume. As the preparation information (e.g., owner, policies and corresponding APIs of data storage, etc.), data operation metadata for the file A is generated. The file A namely data A, is saved and managed by the data operation metadata, such as number of data portioning, data location, etc. In this procedure, the file A was abstracted for data provisioning and management by policies. DSF service customer #1 reads a file through the DSF service. DSF service provider gathers data based on the data operation metadata. DSF service provider aggregates partitions of data and then data is provided to DSF service customer #1. It is possible for the provided data to be used again. Therefore, the data is cached and reflected on data operation metadata. For this reason, DSF service customer #2 quickly reads the cached data. In this procedure, data A was virtualized because the partitioned data A was aggregated as if originally single data A was and then was used for multiple DSF service customers. That is, DSF service customer #1 and #2 read same data.
Role/Sub-role	DSF service customer (CSC:CSU) DSF service provider (CSP:SFP) DSF local storage provider (CSP:CSM)

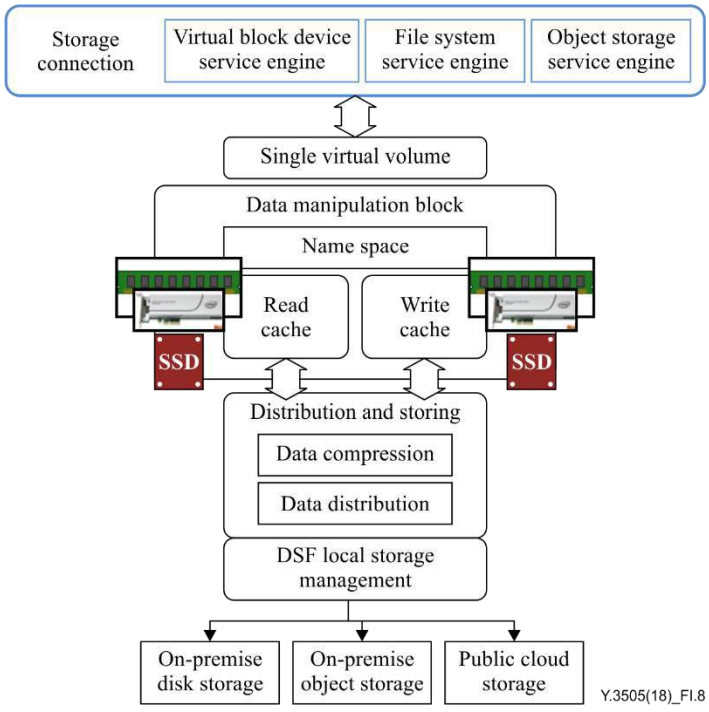
Figure (optional)	 **Figure 1 – Writing data by abstracting data**  **Figure 2 – Read data by virtualized data**
Pre-conditions (optional)	– CSC:CSU has one or more data storage. – CSC:CSU sets policies for DSF local storage. – The data A is shared in Figure 2.
Post-conditions (optional)	
Derived requirements	– Clause 8.4 requirement (7) – Clause 8.4 requirement (7) – Clause 8.4 requirement (8) – Clause 8.1 requirement (2) – Clause 8.2 requirement (10) – Clause 8.2 requirement (9)

I.7 Efficient data storage management

Title	Efficient data storage management
Description	As shown in Figure 1, DSF service provider efficiently manages data to support better storage access performance and to reduce management burden. Tiering is a technique to fulfil efficient data management. By organizing tiered caches, frequently accessed files are stored in high speed cache. While access files are rarely stored in a low speed cache. Cached files are stored on corresponding data storages by managed API. As shown in Figure 2, a DSF service customer saves a same file on a single virtual volume. To avoid waste of data storage capacity DSF service provider performs a de-duplicate data operation. For example, when a file is stored, data replication checking is accomplished. As the result of the checking, a file is stored. If a same file is already stored, the file is managed by data operation metadata.
Role/Sub-role	DSF service customer (CSC:CSU) DSF service provider (CSP:SFP)
Figure (optional)	 **Figure 1 – Tiered caches for access performance**  **Figure 2 – De-duplication data for saving storage capacity**

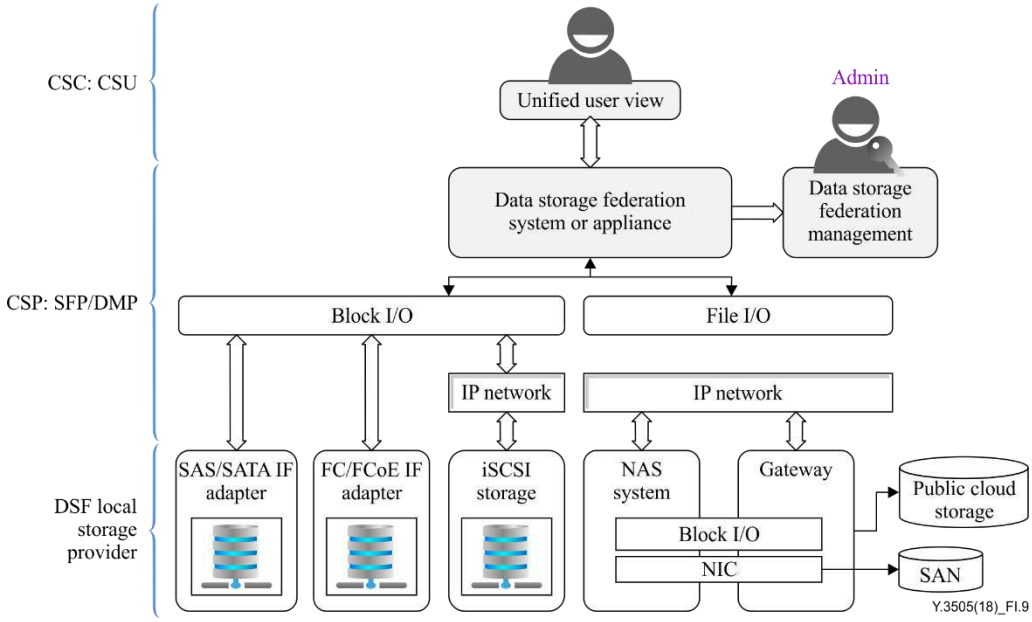
Pre-conditions (optional)	
Post-conditions (optional)	
Derived requirements	– Clause 8.3 requirement (10) – Clause 8.3 requirement (6) – Clause 8.2 requirement (4)

I.8 The data read/write cache and parallel distributed file for performance enhancement

Title	The data read/write cache and parallel distributed file for performance enhancement
Description	DSF service provider provides a cache function for data stored in a public cloud storage. Data stored in public cloud storage is slower than on-premises storage because data is transmitted over the Internet. In addition, since the data is automatically distributed to the public cloud storage in the state DSF service customer does not recognize, the data stored in the public cloud storage needs a high-speed access function. DSF service provider caches the data stored in the public cloud storage to the storage device inside the cloud integrated storage operating platform to provide an on-premises storage-level access speed to the public cloud storage.
Role/Sub-role	DSF service provider (CSP:SFP, CSP:DMP) DSF local storage provider (CSP:CSM)
Figure (optional)	 NOTE – This figure is aligned with logical component.
Pre-conditions (optional)	– CSC:CSU requests single virtual volume to CSP:SFP and has own data storage. – CSP:SFP provide storage system, appliance or device to federate the other storages
Post-conditions (optional)	

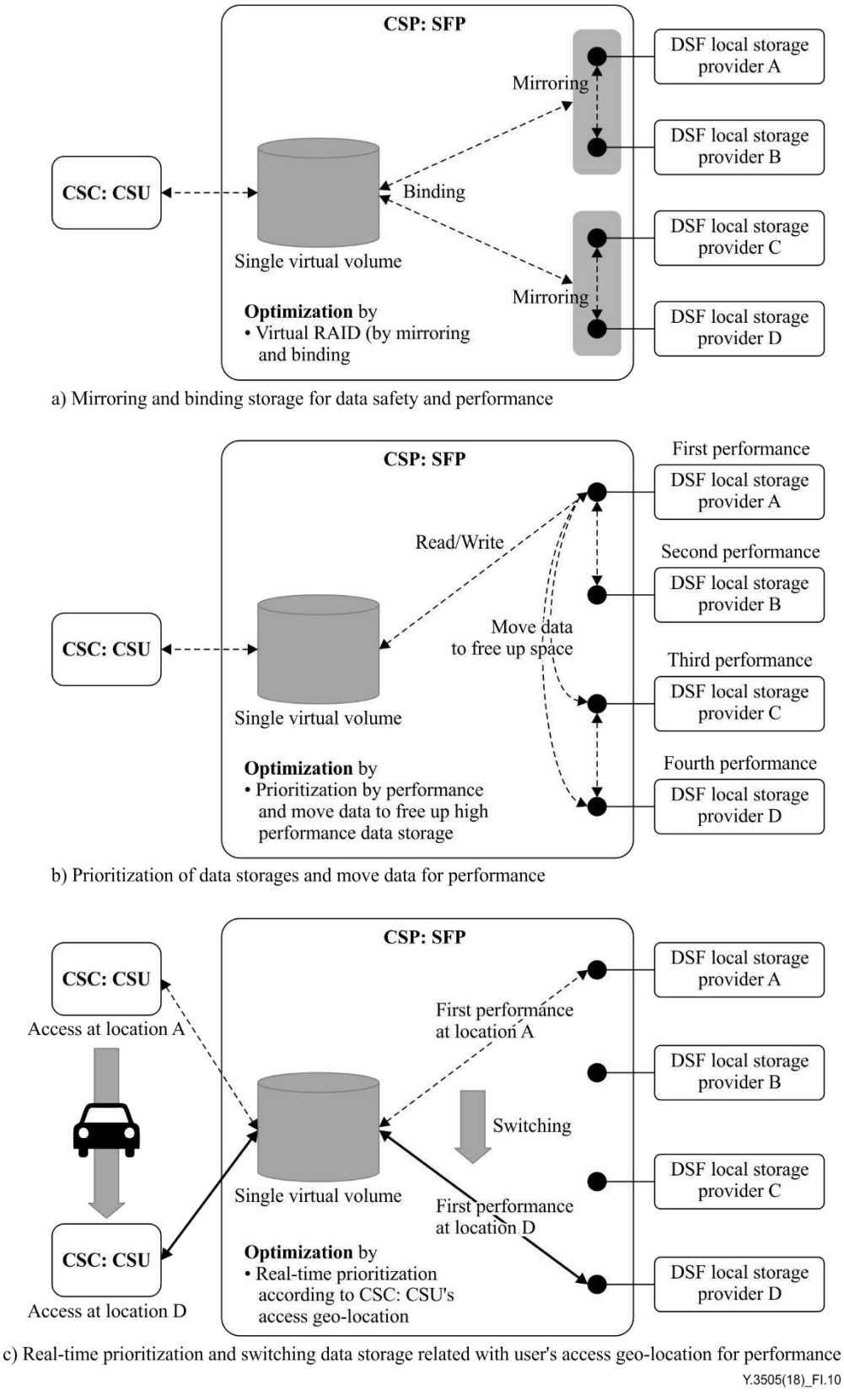
Title	The data read/write cache and parallel distributed file for performance enhancement
Derived requirements	– Clause 8.3 requirement (5) – Clause 8.4 requirement (16) – Clause 8.3 requirement (7) – Clause 8.2 requirement (5) – Clause 8.3 requirement (8) – Clause 8.3 requirement (9)

I.9 Data storage federation and management

Title	The use case for data storage federation and management
Description	In this scenario, it is a use case for one storage system connected to various storage types. In the figure on this use case, no matter what type of storage the storage system has, the DSF service customer is seen as the federated storage and DSF service customer does not care about what storage they use. Thus, a federated storage system or appliance in this figure is responsible for making multiple storage systems of a storage visible to a single system. Similarly, management has a unified management interface.
Role/Sub-role	DSF service customer (CSC:CSU) DSF service provider (CSP:SFP/DMP) DSF local storage provider (CSP:CSM)
Figure (optional)	
Pre-conditions (optional)	– CSC:CSU requests a data storage to DSF service provider and has own data storage. – CSP:SFP provide storage system, appliance or device to federate the other storages
Post-conditions (optional)	
Derived requirements	– Clause 8.2 requirement (7) – Clause 8.3 requirement (14) – Clause 8.1 requirement (2) – Clause 8.2 requirement (6) – Clause 8.4 requirement (5) – Clause 8.1 requirement (8) – Clause 8.2 requirement (8)

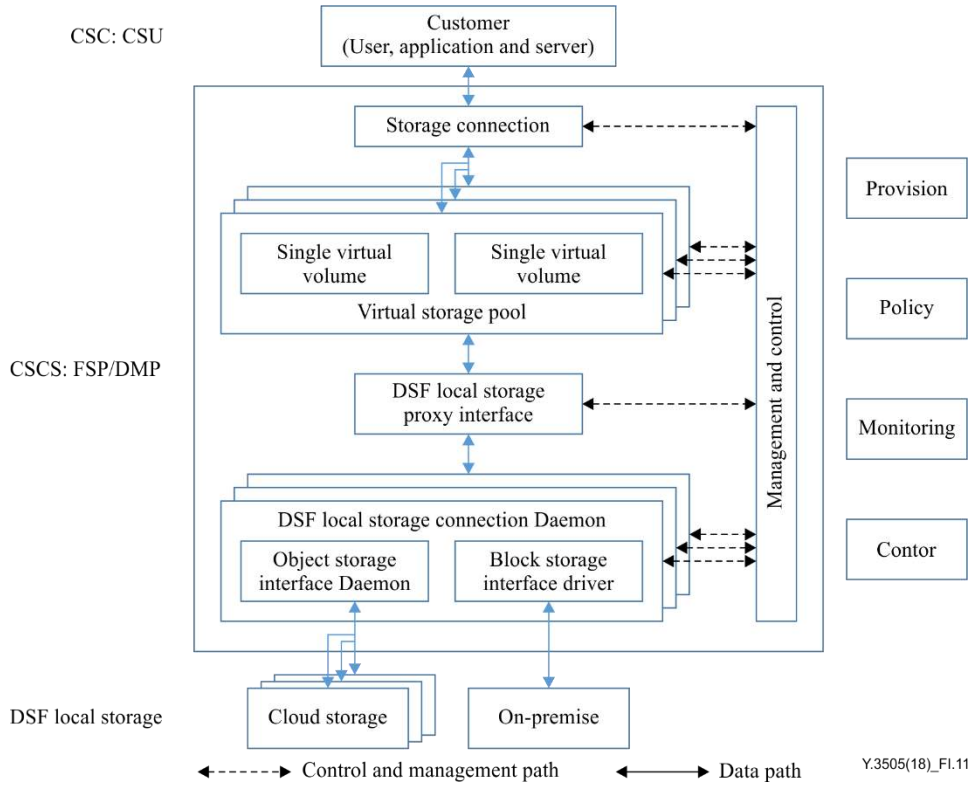
I.10 A use case of storage optimization

Title	A use case for storage optimization based on the customer's purpose in data storage federation
Description	When a DSF local storage provider provides the information of his/her cloud storage services with a DSF service provider, the DSF service provider optimizes a single virtual volume according to the requirements of the user, such as data safety and storage performance. A detailed explanation is as follows: The DSF service provider configures the single virtual volume based on the cloud storages provided by DSF local storage provider. The following optimization policies can be applied and the decision of the optimization policy can be done by the DSF service customer according to his requirements. (1) The DSF local storage provider registered multiple cloud storages to the DSF service provider. (2) DSF service provider provides optimization tool for a single virtual volume. (3) DSF service customer chooses optimization policy related with; A. **data safety and storage performance (a)**: DSF service providers provide a binding function that configures a virtual, single data storage for efficient management of distributed data storage that is available to customers. In addition, DSF service providers provide real-time monitoring of the performance of each data storage and use it with a mirroring mechanism to provide optimized services for stability and performance. For example, when a DSF service customer uses his or her own data, virtual data storage provides a service by selecting a data storage that can provide optimal service among the mirrored data storage; B. **enhancement of performance without storage mirroring (b)**: DSF service provider provides real-time performance monitoring for each data storage. Using this, the DSF service provider determines the priority of the data storage that can provide the optimal service and then transfers the data to that storage in appropriate timing. Therefore, customers can always receive service from optimal data storage; C. **enhancement of performance considering user mobility (c)**: Basically, since the DSF service is affected by the data transmission performance of the network, the performance of the DSF service can be greatly influenced by the location of the customer. Therefore, the DSF service provider provides optimization not only for the performance for each data storage but also for the network situation at the user's location. Virtual data storage provides real-time switching function to the best possible data storage depending on the customer's location. (4) Based on the optimization policy selected by the customer, the DSF service provider optimizes the service. After this processing, (5) DSF service customers use services optimized for their purposes.
Role/Sub-role	DSF service provider (CSP:SFP) DSF service customer (CSC:CSU) DSF local storage provider (CSP:CSM)

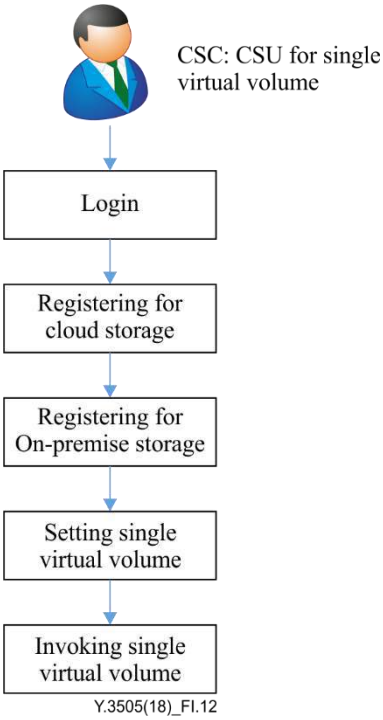
Figure (optional)	
Pre-conditions (optional)	– CSP:SFP has an access interface with multiple DSF local storage.
Post-conditions (optional)	

Derived requirements	– Clause 8.1 requirement (1) – Clause 8.3 requirement (1) – Clause 8.3 requirement (2) – Clause 8.3 requirement (3)

I.11 The use case for data storage federation management

Title	The use case for data storage federation management
Description	The management is generally separate from the data path and the management control path and management is driven through the provisioning and policy management. The management provides the ability to display, create, modify and delete the contents of on-premises and public cloud services integrated into a single storage. In backend storage management, the storage configuration is different from the on-premises and the public cloud storage service. The interfaces for backend storage are made in the form of the separate software daemon. When there are multiple cloud storage devices, DSF local storage management can be configured and a proxy interface can be configured to interface with them and an interface for registering and using on-premises storage is provided.
Role/Sub-role	DSF service customer (CSC:CSU) DSF service provider (CSP:SFP/DMP) DSF local storage provider (CSP:CSM)
Figure (optional)	
Pre-conditions (optional)	– Each logical component consists of one server or several servers. – Each logical component is organized into a network through servers, virtual machines or containers
Derived requirements	– Clause 8.3 requirement (11) – Clause 8.1 requirement (5)

I.12 Registration of data storage for federation service

Title	Registration of data storage for federation service
Description	A DSF service customer requests data storage service from a DSF service provider. For the data storage registration, DSF service customer logs in through the already registered authentication information and registers the cloud storage and on-premises storage to use. The registration process is provided by DSF service provider through the graphical user interface (GUI). DSF service customer registers the service name, storage specification, data storage service protocol and cloud storage name and cloud storage type through the GUI for setting virtual data storage and creates the virtual data storage.
Role/Sub-role	DSF service customer (CSC:CSU) DSF service provider (CSP:SFP/DMP)
Figure (optional)	 The example operation of CSP for data storage service
Pre-conditions (optional)	– CSC:CSU for virtual data storage is a registered user to CSP:DMP. – CSP:DMP has each of the cloud storage service interfaces
Derived requirements	– Clause 8.1 requirement (6) – Clause 8.3 requirement (4)

Appendix II

Comparison analysis between cloud computing and data storage federation

(This appendix does not form an integral part of this Recommendation.)

Table II.1 shows the mapping between data storage federation ecosystem and the CCRA user view. The DSF service customer has two sub-roles and these sub-roles are mapped onto the CSC:cloud service user because two sub-roles have a relationship of using service. The DSF local storage provider and CSP:cloud service manager and CSP:cloud service operations manager, which provide data storage, are mapped in the perspective of providing service. However, for the DSF service provider, the additional considerations in data storage perspective are needed in cloud computing. To federate and provide data storage from DSF local storages, such as cloud storage and non-cloud storage, they are properly described in CSP as new sub-roles, activities and involvements.

Table II.1 – Mapping between data storage federation ecosystem and CCRA user view

ITU-T Y.3505 (DSF)		ITU-T Y.3502 (Cloud computing)		Note
Roles	**Activities**	**Sub-roles**	**Activities**	
DSF service customer	• use DSF service	CSC:cloud service user	• use cloud service	• The additional considerations in data storage and data perspective on the federated storage environment are needed.
DSF service provider	• provide virtual storage pool • provide single virtual volume • manage storage management metadata • manage data storage policy	–	–	• The additional considerations in data storage perspective are needed as sub-roles and activities in CSP. • The sub-roles and activities support the data storage federation service.
	• manipulate DSF data • manage data operation metadata • manage data manipulation policy	–	–	• The additional considerations in data storage perspective are needed as sub-roles and activities in CSP. • The sub-roles and activities support the data storage federation service.
DSF local storage provider	• provide DSF local storage	CSP:cloud service manager	• provide services e	• Activities and their involvements of the two sub-roles in ITU-T Y.3502 are supported to provide cloud data storage.

Bibliography

[b-ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing.*

[b-ITU-T X.1631] Recommendation ITU-T X.1631 (2015), *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services.*

[b-ITU-T X.1641] Recommendation ITU-T X.1641 (2016), *Guidelines for cloud service customer data security.*

[b-ISO/IEC 2382] ISO/IEC 2382 (2015), *Information technology – Vocabulary*.


END DEVICES
SERVICES
CONSUMERS
AVAILABILITY
FLEXIBILITY
CLOUD
COMPUTING
STANDARDS
INNOVATION
SECURITY
BUSINESS

Cloud computing – Functional requirements for cloud service brokerage

Recommendation ITU-T Y.3506

(05/2018)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Summary

Cloud service brokerage is a service that arbitrates, delivers and manages cloud services provided by cloud service providers for cloud service customers. Recommendation ITU-T Y.3506 provides functional requirements for cloud service brokerage. To provide functional requirements for cloud service brokerage, this Recommendation specifies the overview including service model and configuration of the cloud service brokerage. Various use cases are also identified to derive the functional requirements.

Keywords

Cloud computing, cloud service brokerage, cloud service broker, functional requirement.

Table of Contents

1 Scope

This Recommendation provides functional requirements for cloud service brokerage (CSB). It addresses the following subjects:

– Overview of cloud service brokerage;

– Functional requirements of cloud service brokerage;

– Use cases of cloud service brokerage.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing.*

[ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014), *Information technology – Cloud computing – Overview and vocabulary*.

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), *Information technology – Cloud computing – Reference architecture.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 cloud service customer [ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

3.1.2 cloud service provider [ITU-T Y.3500]: Party which makes cloud services available.

3.1.3 cloud service broker [ITU-T Y.3500]: Cloud service partner that negotiates relationships between cloud service customers and cloud service providers.

3.1.4 inter-cloud provider [ITU-T Y.3502]: A sub-role of cloud service provider that relies on one or more peer cloud service providers to provide part or all of the cloud services offered to cloud service customers.

3.1.5 product catalogue [ITU-T Y.3502]: A listing of all the cloud service products which cloud service providers make available to cloud service customers.

3.1.6 service level agreement [b-ISO/IEC 19086-1]: Documented agreement between the cloud service provider and cloud service customer that governs the covered service(s).

NOTE – A cloud service agreement can consist of one or more parts recorded in one or more documents.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 cloud service brokerage: A service that arbitrates, delivers, and manages cloud services provided by CSPs for CSCs.

NOTE – Cloud service brokerage is realized by cloud service broker with new activities. The new activities are (i) assist CSC for accessing service and (ii) check and control service status.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API Application Programming Interface
CSB Cloud Service Brokerage
CSC Cloud Service Customer
CSN Cloud Service Partner
CSP Cloud Service Provider
ID Identification
OS Operating System
SLA Service Level Agreement
SLO Service Level Objectives
URL Uniform Resource Locator

5 Conventions

In this Recommendation:

The keywords "is required" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

6 Overview of cloud service brokerage

6.1 Introduction to cloud service broker

The cloud service broker is a sub-role of cloud service partner (CSN) that negotiates relationships between cloud service customers (CSCs) and cloud service providers (CSPs). The cloud service broker is not itself a cloud service provider and should not be confused with the role of inter-cloud provider [ITU-T Y.3502]. The role of cloud service broker could be combined with or operate independently of the role of inter-cloud provider. Only three activities of cloud service broker have been identified in [ITU-T Y.3502] such as (i) acquire and assess customers, (ii) assess marketplace and (iii) set up legal agreement. A detailed description for these activities follows:

– **acquire and assess customers**: The cloud service broker provides CSCs with available cloud services accompanied by associated information such as service level agreements (SLAs) and contract terms. The cloud service broker also assesses CSC's needs and requirements;
– **assess marketplace**: The cloud service broker constructs product catalogues by surveying the product offerings with technical and business information from CSPs. Any changes of the contents of corresponding product catalogues are notified to the cloud service broker. If there is a request on cloud service from a CSC, the cloud service broker performs a matching process between product offerings and CSC's requirements including technical, business and regulatory aspects;
– **set up legal agreement**: The cloud service broker negotiates service agreements between the CSC and the CSP in terms of legal agreements as well as terms and prices to complete a contract.

After the contract between a CSC and a CSP by the "set up legal agreement" activity, the CSC uses the selected cloud services. In order for the CSC to use the cloud services, additional considerations are required as follows:

– A CSC uses cloud services from CSPs through access information delivered by the cloud service broker;
– The cloud service broker also manages and monitors the cloud services.

To enhance the operations of the cloud service broker, its activities defined in [ITU-T Y.3502] need to be extended to cover features such as how to access cloud services, how to manage and how to monitor the cloud services.

6.2 Introduction to cloud service brokerage

A cloud service brokerage (CSB) is a service between CSCs and CSPs, in which the cloud service broker arbitrates, delivers and manages the cloud services from the CSPs to the CSCs. The objectives of CSB are to provide a single access, easily managed and value-added service to CSCs from multiple CSPs.

As shown in Figure 6-1, the CSB premises the multiple CSCs and CSPs environment. In CSB, a CSP registers cloud services to a cloud service broker and the cloud service broker configures a product catalogue with the registered cloud services. The cloud service broker also registers cloud services during the configuration of the product catalogue. Three service models (see clause 6.3) are implemented depending on how the product catalogue is configured in cloud service brokerage.

When, a CSC requests a cloud service with CSC's requirements to the cloud service broker, the cloud service broker searches for best-matched cloud services.

Once the CSC agrees with the conditions (e.g. terms and price) of a cloud service by the cloud service broker, the cloud service broker makes a contract with the CSC for brokering a cloud service. On behalf of the CSC, the cloud service broker requests to launch a cloud service to the CSPs and the access information from the CSPs is delivered to the CSC. Using the access information, the CSC accesses and utilizes the cloud service. During the use of the cloud service, the cloud service broker monitors and controls the cloud service on behalf of the CSC.

NOTE – The more detailed overall behaviour of the cloud service brokerage with specific steps is described in Table I.1 and Table I.9 of Appendix I for a general use case and a use case for cloud service management, respectively.

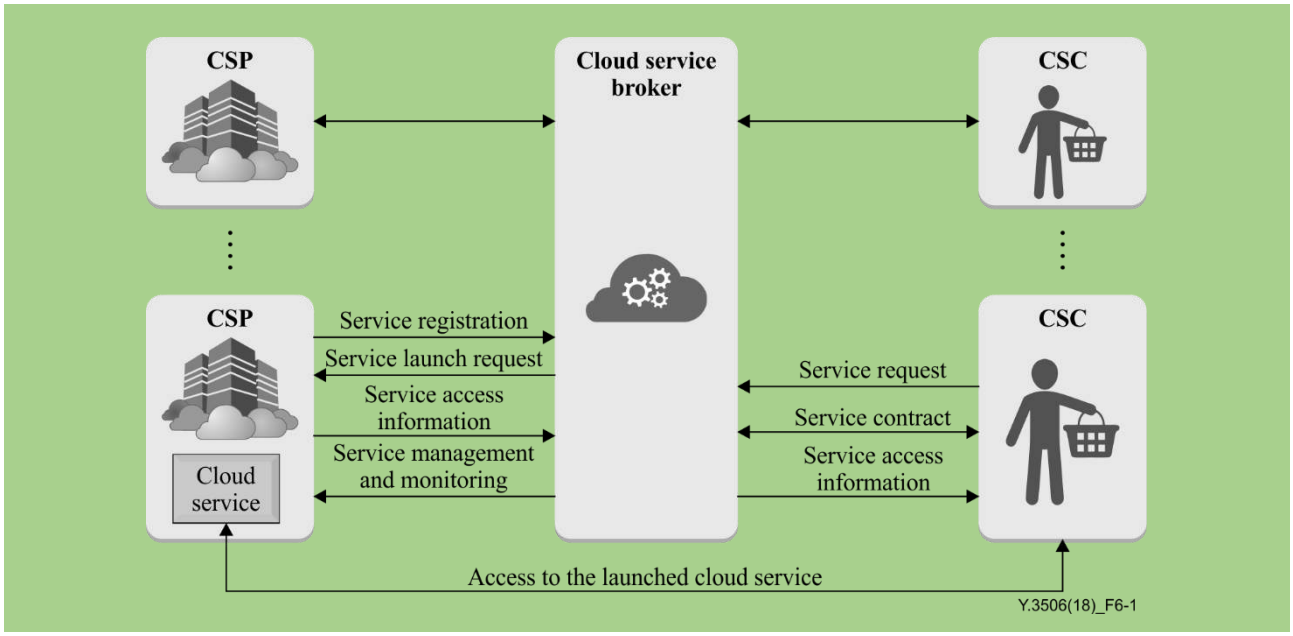


Figure 6-1 – Basic concept of cloud service brokerage

In addition to the three activities of the cloud service broker of [ITU-T Y.3502], the cloud service brokerage needs new activities of the cloud service broker. These new activities are described below.

– **Assist CSC for accessing service**: It includes acquiring access information for a cloud service from CSPs who provide the cloud service, and forwarding the access information to the CSC who requests the cloud service to understand access and usage of the cloud service. In order to assist a CSC to access a cloud service, access information is transmitted securely.

– **Check and control service status**: It supports CSCs to control cloud services, such as stopping, resuming and terminating the cloud services. Also, this activity involves checking the status of running cloud services by monitoring so that the cloud service broker enforces service qualities agreed in a SLA instead of CSCs.

6.3 Service model of cloud service brokerage

The cloud services registered in the product catalogue of cloud service brokerage are categorized in the following three service models:

– **Cloud service aggregation**: As shown in Figure 6-2, cloud service aggregation brings together cloud services from multiple CSPs to CSCs without any changes in a product catalogue. The detailed description of cloud service aggregation is introduced in Table I.2 of Appendix I;

– **Cloud service integration**: As shown in Figure 6-3, cloud service integration collects registered cloud service in a product catalogue, making them work together to provide new cloud services in a product catalogue. The detailed description of cloud service integration is introduced in Table I.3 of Appendix I;

– **Cloud service customization**: As shown in Figure 6-4, cloud service customization performs customized development by a cloud service broker on existing multiple cloud services in a product catalogue according to CSCs' demands. The detailed description of cloud service customization is introduced in Table I.4 of Appendix I.

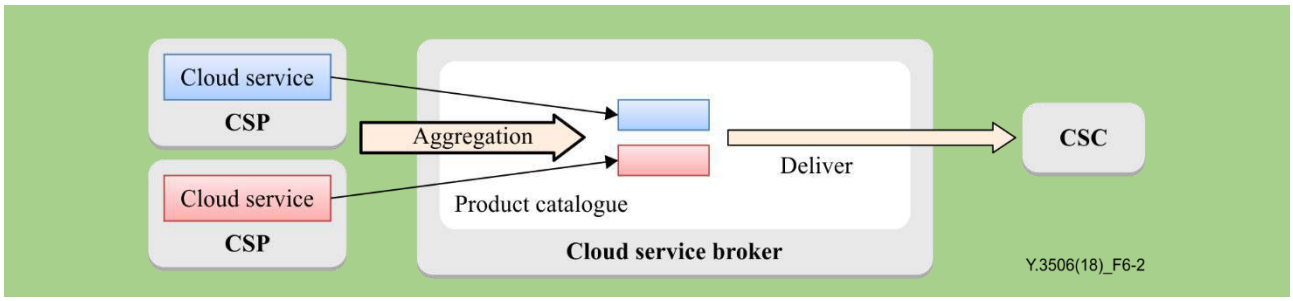


Figure 6-2 – Cloud service aggregation model

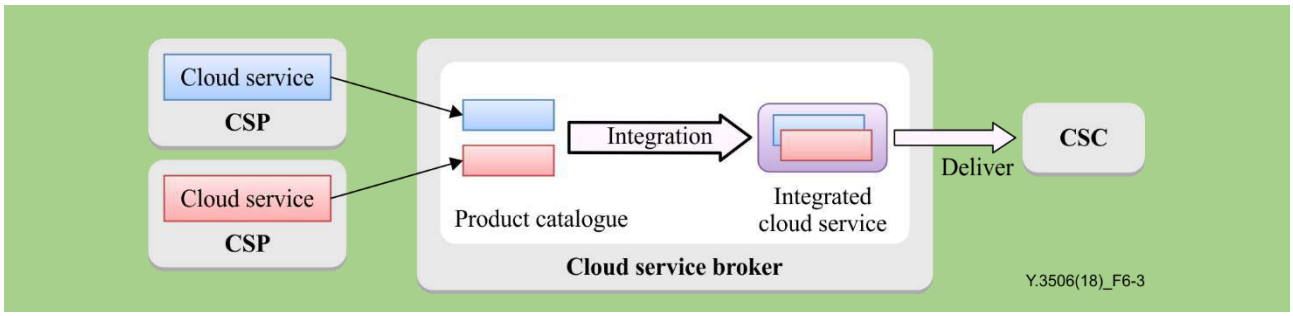


Figure 6-3 – Cloud service integration model

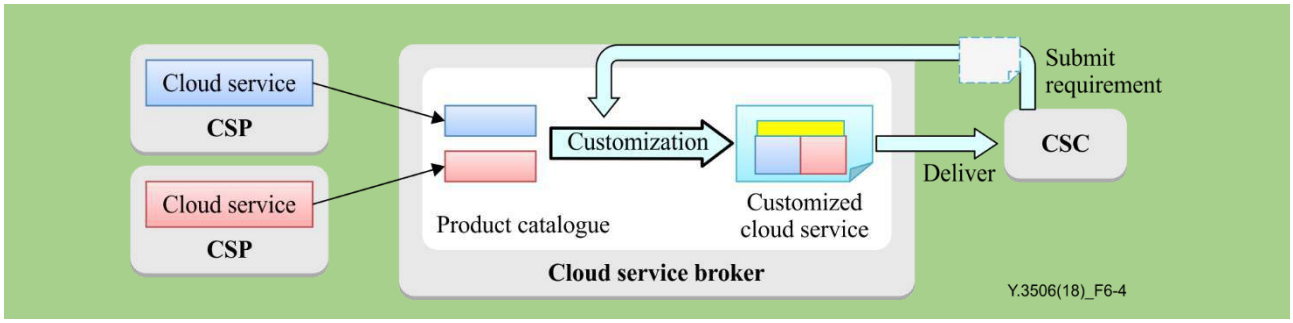


Figure 6-4 – Cloud service customization model

6.4 Configuration of cloud service brokerage

Figure 6-5 shows logical components of CSB. The logical components consist of workspace, product catalogue management, contract management, service access management and service management.

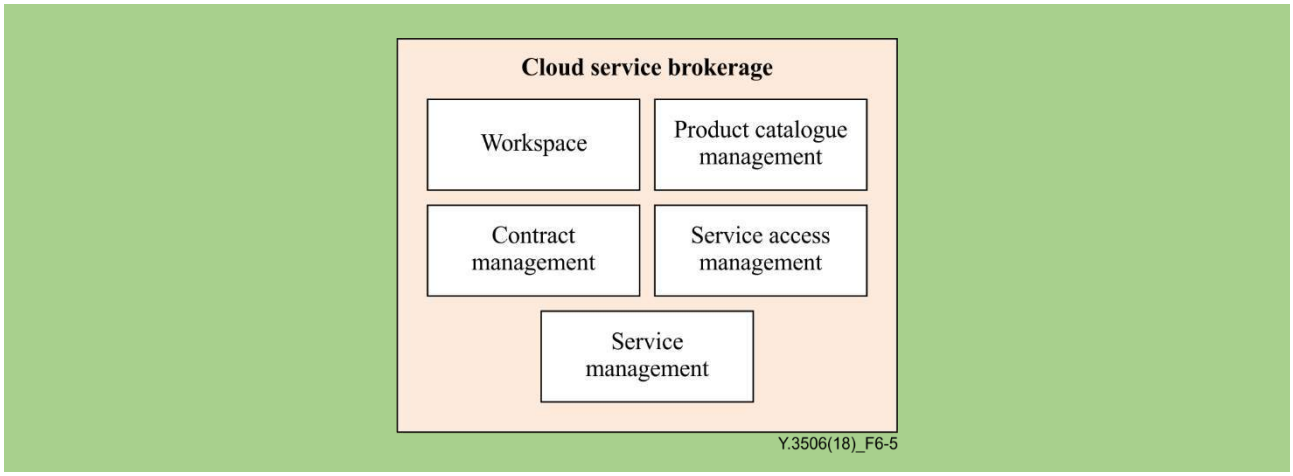


Figure 6-5 – Configuration of cloud service brokerage

NOTE – Relationship between the logical components and the activities of the cloud service broker for CSB is described in Appendix II.

6.4.1 Workspace

A workspace logical component manages user accounts in CSB and provides user interfaces for CSPs and CSCs. This logical component handles authentication of users (i.e., CSPs and CSCs) and grants authorization for them to access other logical components in CSB. CSPs and CSCs perform requests and responses for all their operations through the user interfaces provided by this logical component.

NOTE 1 – CSP's operations include registering and deregistering cloud service. CSC's operations include delivering cloud service requirements, requesting a cloud service launching, checking status of launched cloud services and paying for the usage cost.

NOTE 2 – Since there are CSPs who provide cloud services and CSCs who use the cloud services, a market trading cloud services is formed in a CSB. Whereas marketplace mentioned in [ITU-T Y.3502] is not a logical component of CSB, a CSB itself becomes a marketplace in that CSPs provide cloud services and CSCs use cloud services in the CSP through CSB and the workspace is used as a user interface of marketplace. A CSP registers cloud services to a product catalogue and a CSC use CSP's cloud service by using workspace.

6.4.2 Product catalogue management

A product catalogue management logical component provides registering, deregistering and searching cloud services within a product catalogue in CSB to select cloud service by CSCs. Cloud services from multiple CSPs through workspace are registered and deregistered in the product catalogue. This logical component performs supporting the three service models of CSB described in clause 6.3 by managing registration into the product catalogue.

NOTE – To support service models of CSB, this logical component performs (i) aggregation of cloud services by registering original cloud services from multiple CSPs into the product catalogue, (ii) integration of cloud services by registering a new integrated cloud service that consists of multiple cloud services into the product catalogue and (iii) customization of cloud services by registering a new customized cloud service into the product catalogue to comply with CSC's requirements.

This logical component also provides searching for the best matched cloud service.

6.4.3 Contract management

A contract management logical component manages contracts between CSPs and CSCs in terms of cloud SLA.

NOTE – Cloud SLA includes entire agreements regarding contracts such as specification of cloud services, service level in terms of quality, price of cloud service, remedies for failures to meet the terms of the SLA and so on.

For the establishment of a contract, this logical component needs to create a cloud SLA document by using CSP's SLA and notifies it to the contracted CSC. This logical component registers an agreed service level to the service management logical component to guarantee the contracted service quality. If the cloud service fails to meet the service level, this logical component enforces remedies for failures to meet the terms of the SLA.

6.4.4 Service access management

A service access management logical component requests to launch a contracted cloud service to the designated CSP. This logical component also manages access information of cloud services. In order to use to a cloud service, a CSC requires to get access information. After a CSP launches a cloud service, the CSP provides access information to a cloud service broker and this logical component manages the information and delivers the access information to the CSC.

NOTE – The access information is required for a CSC to access a cloud service. The access information may include an access point such as Internet protocol address or uniform resource locator (URL) of the cloud service and authentication methods such as a certificate or identification (ID) and password to access the cloud service.

6.4.5 Service management

A service management logical component manages the controls and status of running cloud services. This logical component delivers control requests for the running cloud services to CSPs in order to stop, resume and terminate them on behalf of a CSC. This logical component also checks the status of running cloud services by monitoring and enforces the service level agreed in a SLA. If a cloud service fails to meet the service level, this logical component needs to take an action to handle the situation by interacting with a contract management logical component.

7 Functional requirements of cloud service brokerage

7.1 Functional requirements for workspace

– **Authentication and authorization for workspace**: It is required that a CSN: cloud service broker have authentication and authorization mechanisms to authorize CSPs and CSCs access to workspace.

– **Account management**: It is required that a CSN: cloud service broker manage the accounts of CSCs and CSPs.

– **User interface for CSCs**: It is recommended that a CSN: cloud service broker provide a user interface for CSCs to search, select, request, launch, monitor, manage and pay for the cloud services from the multiple CSPs.

– **User interface for CSPs**: It is recommended that a CSN: cloud service broker provide a user interface for CSPs to register information about the CSPs and cloud services to a CSN: cloud service broker.

NOTE – The information about a CSP includes a name of the CSP, entry point URL of the CSP at which a CSN: cloud service broker gains access to and communicates with the CSP, geographical location of the CSP, access account to the CSP and so on.

7.2 Functional requirements for product catalogue management

– **Registration of cloud service**: It is required that a CSN: cloud service broker provide registration of cloud services in the product catalogue.

NOTE 1 – Depending on the service models, the subject and way of registration are different. For a cloud service aggregation model, cloud services in CSPs are registered in a product catalogue. For cloud service integration and customization models, a CSN: cloud service broker registers new cloud services to a product catalogue by integrating the registered cloud services according to the broker and CSC's requirements, respectively.

– **Cloud service deregistration**: By the agreement between a CSP and a CSN: cloud service broker, it is required that the CSN: cloud service broker deregister the cloud services in a product catalogue.

NOTE 2 – The deregistration of a cloud service includes disabling the cloud service from the product catalogue, notifying the deregistration of the cloud service to related CSCs, stopping all running cloud services and deleting the cloud service from the product catalogue.

– **Automation of service deregistration**: It is recommended that a CSN: cloud service broker provide automatic cloud service deregistration to perform deregistration procedures conveniently and safely.

– **Notification of service deregistration**: It is required that a CSN: cloud service broker provide the notification of the service deregistration to CSCs not to use the deregistered service.

– **Request for maintaining cloud service**: It is recommended that a CSN: cloud service broker request the related CSP to maintain the deregistered service until the CSCs finish using the cloud service.

– **Providing cloud service requirement template**: It is recommended that a CSN: cloud service broker provide a template for service requirements to CSCs for receiving CSC's requirements.

NOTE 3 – The requirement template reflects information about CSC's requirements.

NOTE 4 – The CSC's requirement includes SLA information of the cloud service such as quality, price of cloud service, remedies for failures to meet the terms of the SLA and so on. The CSC's requirement also includes information about specifications of the cloud service such as virtual machine, operating system (OS) type, applications, etc.

– **Cloud service requirement validation**: It is recommended that a CSN: cloud service broker provide validation of the contents in the cloud service requirement template.

– **Cloud service search**: It is required that a CSN: cloud service broker provide searching a cloud service in the product catalogue to meet the requirements of CSCs.

NOTE 5 – The requirements of a CSC are used as search criteria that include specifications and service level of a cloud service that a CSC wants to use.

– **Providing the best matched cloud service**: It is recommended that a CSN: cloud service broker provide CSCs with the best matched cloud services and information about the CSPs who provide the cloud services reflecting the CSC's requirements.

– **Cloud service alteration**: It is recommended that a CSN: cloud service broker request CSPs to alter registered services for cloud service customization.

– **Cloud service substitution for integrated cloud service**: It is recommended that a CSN: cloud service broker provide alternative cloud services in a product catalogue for an integrated cloud service.

NOTE 6 – Based on the alternative cloud services in a product catalogue, a CSN: cloud service broker provides the substitution of cloud service as a member of an integrated cloud service.

– **Equivalent cloud service selection**: It is recommended that a CSN: cloud service broker provide an equivalent cloud service in the product catalogue with the registered service to migrate to keep service equivalence after migration.

7.3 Functional requirements for contract management

– **Cloud service charging**: It is recommended that a CSN: cloud service broker provide billing information to CSCs by reorganizing billing information gathered from related CSPs.

NOTE 1 – The billing information is used to generate invoices for the usage of a cloud service. The billing information includes business information related to payment, such as methods for payment and biller and costs for the usage of the cloud service based on price and metering.

– **Configuration of cloud service for contract**: It is recommended that a CSN: cloud service broker configure a cloud service through selecting elements of the cloud service by a CSC.

NOTE 2 – Examples of elements for cloud service specification are virtual machines, OS type, applications, etc.

– **Service level objectives (SLO) selection**: It is recommended that a CSN: cloud service broker provide selection of service level objectives to a CSC according to business requirements of the CSC.

– **SLA document management**: It is recommended that a CSN: cloud service broker provide generation of a SLA document according to the agreement to share the SLA document with the related CSC.

– **SLA description model**: It is recommended that a CSN: cloud service broker provide a SLA description model to describe terms and conditions.

NOTE 3 – Examples of terms and conditions are guaranteed service levels and remedies for failures to meet the terms of the SLA.

– **Remedies for failures to meet the terms of the SLA**: It is recommended that a CSN: cloud service broker provide agreed remedies for failures to meet the terms of the SLA.

NOTE 4 – Examples of a remedies are migration, scale up, performance extension and so on.

7.4 Functional requirements for cloud service access management

– **Delivering cloud service provision request**: It is recommended that a CSN: cloud service broker deliver the provisioning request to CSPs as requested by the CSC.

– **Delivering cloud resource request**: When a CSC needs more cloud resources of a cloud service, it is recommended that a CSN: cloud service broker deliver the CSC's request for resources to a CSP.

– **Access information forwarding**: It is required that a CSN: cloud service broker forward the access information of a cloud service from a CSP to the authorized CSC.

– **Prohibiting access information storing**: It is recommended that a CSN: cloud service broker provide prohibiting of the access information for a cloud service not to open or store.

7.5 Functional requirements for cloud service management

– **Cloud service SLA management**: It is recommended that a CSN: cloud service broker provide SLA management of running cloud service across multiple CSPs.

– **Cloud service monitoring**: It is recommended that a CSN: cloud service broker monitor the status of cloud services by using gathered monitoring information of the cloud service from multiple CSPs.

NOTE 1 – The monitoring information is gathered periodically or aperiodically at runtime to check conditions or status of cloud services. The monitoring information includes measured data for metrics of service levels in SLA or resource utilization of cloud services.

NOTE 2 – A CSN: cloud service broker monitors status of logical resources (e.g., virtual machine) of cloud services.

– **Delivering request of cloud service control**: It is recommended that a CSN: cloud service broker deliver requests of control actions for a cloud service from a CSC to a CSP for managing status of the cloud service.

– **Validation of result for request of cloud service control**: It is recommended that a CSN: cloud service broker validate the status of cloud service whether the status is changed correctly or not in accordance with the delivered request for a control action of a cloud service by a CSC.

NOTE 3 – Since changing status of cloud service takes time according to the circumstance of the CSP, a CSN: cloud service broker does not know the result of the control request instantly. Therefore, to validate the status of cloud service, the CSN: cloud service broker needs to check periodically the current status of cloud service by communicating with the CSP until the validation is finished.

– **Initiation of validation**: It is recommended that a CSN: cloud service broker initiate cloud service control status validation only after the CSN: cloud service broker receives an acknowledgement for a cloud service control request from a CSP.

NOTE 4 – The acknowledgement for a service control request is a message from a CSP to inform receipt of a request for a service control from a CSN: cloud service broker.

– **Status checking period for validation**: It is recommended that a CSN: cloud service broker provide checking periods in service control status validation by predicting the completion time of the cloud service control to reduce communication overhead between the CSN: cloud service broker and a CSP.

NOTE 5 – Service control checking period is the duration of time of one cycle for checking status of the service. The checking period is determined probabilistically by statistically predicting the completion time of the cloud service control.

NOTE 6 – To predict the completion time of a cloud service control, statistical methods, such as moving average and variance, are applied to accumulated history of completion time of previous control requests for the same or similar services. Using the statistical methods, a CSN: cloud service broker generates a probability distribution for completion of service control at a given time.

NOTE 7 – The service control checking periods are determined by a normal probability distribution. The CSN: cloud service broker increases the frequency of checking status of service when the probability of service control completion is high. The CSN: cloud service broker decreases the frequency when the probability of service control completion is low.

– **History of cloud service control status validation**: It is recommended that a CSN: cloud service broker manage history of validation results as well as required time for completing cloud service controls.

– **Notification of result for request of cloud service control**: It is recommended that a CSN: cloud service broker provide notification of the result of cloud service control to a CSC.

– **Detection of failures to meet the terms of the SLA**: It is required that a CSN: cloud service broker detect failures to meet the terms of the SLA through monitoring and to verify the service level.

NOTE 8 – To detect failures to meet the terms of the SLA, monitoring includes one or more measurable information such as storage speeds, memory capacity and performance, computing speeds, network speeds, service response time, etc.

NOTE 9 – If a failure to meet the terms of the SLA is found in the integrated cloud service, a CSN: cloud service broker identifies the cloud service that caused the failure.

– **Prevention of service termination during migration**: It is recommended that a CSN: cloud service broker provide postponing of the termination of a running cloud service until the CSN: cloud service broker verifies ready status of a new service to prevent loss of data during migration process.

8 Security considerations

Security aspects for consideration within the cloud computing environment, are addressed by security challenges for the CSPs as described in [ITU-T X.1601]. In particular, [ITU-T X.1601] analyses security threats and challenges and describes security capabilities that could mitigate these threats and meet the security challenges.

Appendix I

Use cases of cloud service brokerage

(This appendix does not form an integral part of this Recommendation.)

Table I.1 – A general use case for cloud service brokerage

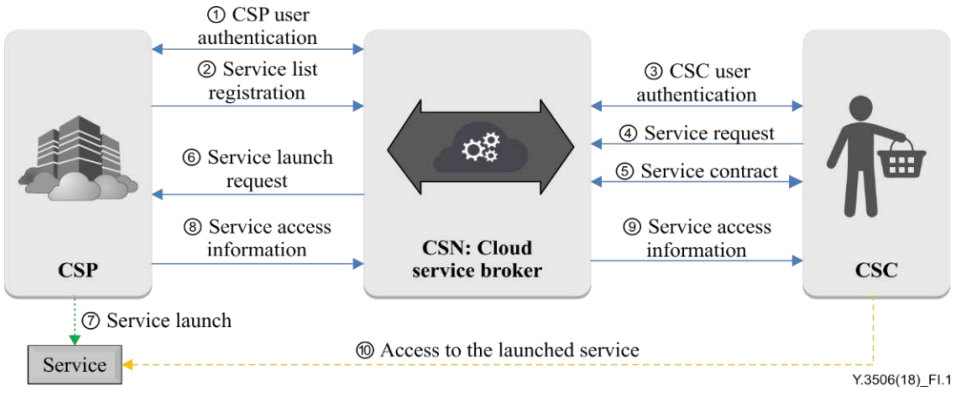
Title	A general use case for cloud service brokerage.
Description	(1) A CSP determines to sell cloud services though a CSN: cloud service broker and accesses a workspace operated by the CSN: cloud service broker such as a web portal by using an authorized account. (2) The CSP registers cloud service list to a product catalogue of the CSN: cloud service broker though a user interface of the workspace. (3) A CSC accesses the workspace by using an authorized account to find and use a cloud service through the CSN: cloud service broker. (4) The CSC requests a cloud service with service requirements to the CSN: cloud service broker. Then, the CSN: cloud service broker searches the best-matched cloud service out of the CSN: cloud service broker's product catalogue. (5) The CSN: cloud service broker notifies the searched result and suggests detailed cloud service conditions to the CSC. Once the CSC agrees with the suggested condition, the CSN: cloud service broker makes a contract with the CSC for brokering a cloud service. (6) On behalf of the CSC, the CSN: cloud service broker requests to launch a cloud service to the CSP who can accommodate the service requirements. (7) The requested CSP launches a cloud service according to the service requirements (8) The CSP informs on a launch of the cloud service and provides information for accessing the cloud service such as service access point, ID and password to the CSN: cloud service broker. (9) The CSN: cloud service broker forwards the access information to the authorized CSC. (10) Using the access information, the CSC accesses and utilizes the launched cloud service.
Roles/sub-roles	CSP, CSN: cloud service broker, CSC
Figure	
Pre-conditions (optional)	The CSP is a member of the CSN: cloud service broker and has an account for accessing CSB workspace. The CSC is a member of the CSN: cloud service broker and has an account for accessing CSB workspace.
Post-conditions (optional)	The CSN: cloud service broker monitors status of the brokered service to comply with the contracted service agreement.

Table I.1 – A general use case for cloud service brokerage

Derived requirements	– Authentication and authorization for workspace (See clause 7.1) – Account management (See clause 7.1) – User interface for CSCs (See clause 7.1) – User interface for CSPs (See clause 7.1) – Access information forwarding (See clause 7.4) – Prohibiting access information storing (See clause 7.4)

Table I.2 – A general use case of cloud service aggregation

Title	A general use case of cloud service aggregation.
Description	The CSN: cloud service broker aggregates the various cloud services of the multiple CSPs and publishes these services to the CSCs without any change. The difference between the general use case for cloud service brokerage in Table I.1 and this use case is that cloud service aggregation brokerage provides the CSC a product catalogue which consists of multiple services hosted by CSPs and an aggregated management view, i.e., workspace, for ordered multiple services. The CSPs register cloud services to the CSN: cloud service broker in product catalogue, which is the unique one provided to a CSC by the CSN: cloud service broker with all CSPs' cloud services. The synchronization of the product catalogue can be triggered by the registered CSPs or the CSN: cloud service broker itself in case of modification in the cloud services. The CSC accesses the CSB workspace, selects and purchases different cloud services from multiple CSPs. The CSN: cloud service broker completes ordering processing of multiple CSPs, instead of the CSC. After the CSC individually selects and orders multiple services from the product catalogue, the CSN: cloud service broker shows the list of ordered multiple services to the CSC so that the CSC can request controls for the cloud services to the CSN: cloud service broker. The CSC can use workspace to manage the ordered multiple services together or individually. For instance, the CSC can pause all the aggregated services at once and checks the overall usage cost of the aggregated services. The CSN: cloud service broker can help the CSC to provision all the selected cloud services together to simplify the process. For instance, to launch multiple virtual machines in multiple CSPs' cloud environment. The CSN: cloud service broker can manage controls and status of multiple cloud services in aggregated manner and/or each cloud services individually. All monitor information can be collected by the CSN: cloud service broker to provide the CSC with an overall view of cloud services together. The unified charges can be proved to the CSC by the CSN: cloud service broker.
Roles/sub-roles	CSP, CSN: cloud service broker, CSC

Table I.2 – A general use case of cloud service aggregation

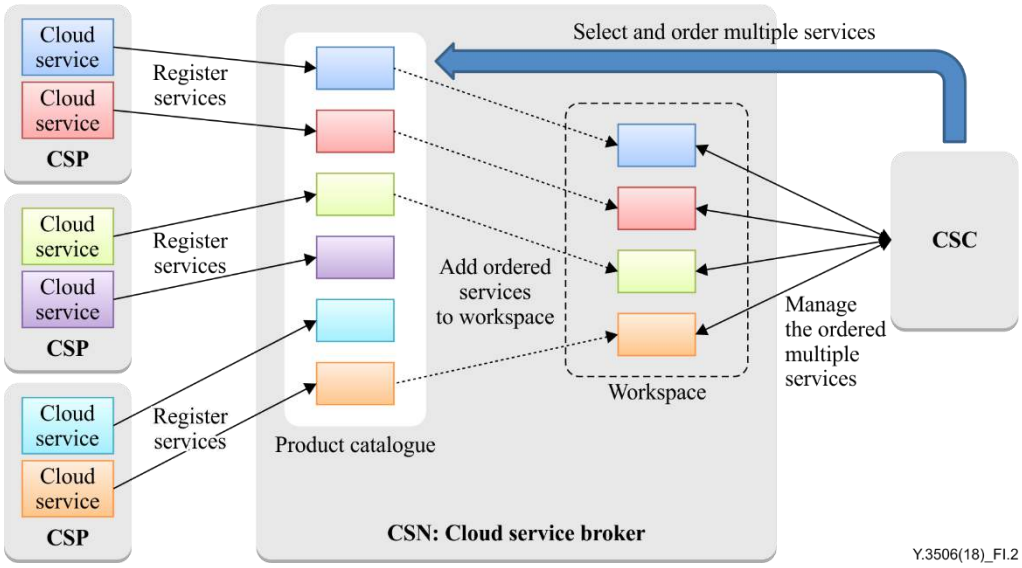
Figure	
Pre-conditions (optional)	The CSN: cloud service broker and multiple CSPs achieve a cooperation agreement and the CSN: cloud service broker can sell these CSPs' cloud services. The CSN: cloud service broker adapts the different cloud application programming interfaces (APIs) of multiple CSPs.
Post-conditions (optional)	The CSCs can order and use the cloud services of multiple CSPs through a CSB workspace.
Derived requirements	– User interface for CSCs (See clause 7.1) – Delivering cloud service provision request (See clause 7.4) – Cloud service SLA management (See clause 7.5) – Cloud service charging (See clause 7.3) – Cloud service monitoring (See clause 7.5) – Registration of cloud service (See clause 7.2)

Table I.3 – A general use case of cloud service integration

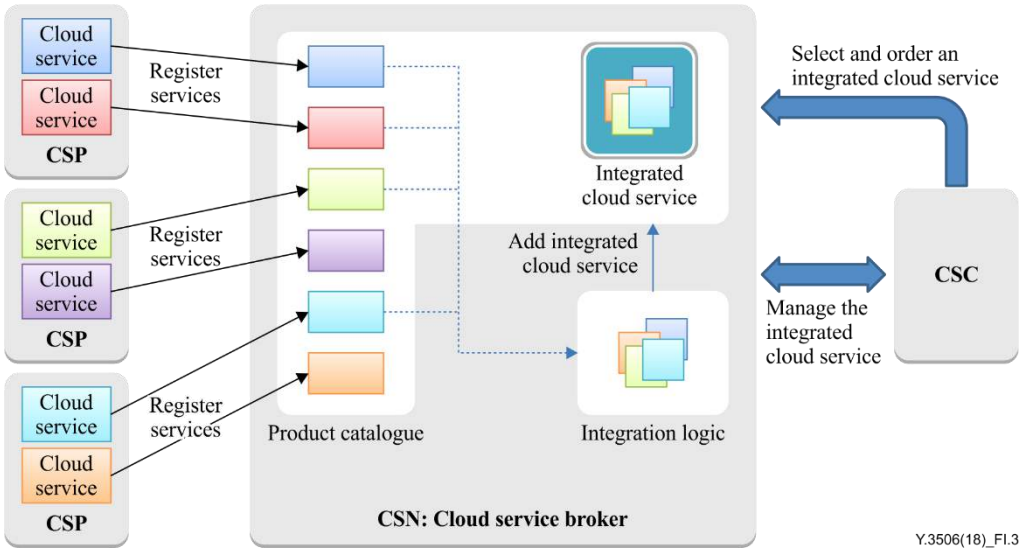
Title	A general use case of cloud service integration.
Description	The CSN: cloud service broker collects multiple cloud services provided by different CSPs, orchestrates the multiple cloud services and provides value-added cloud services to CSCs through The CSN: cloud service broker's cloud product catalogue. The CSPs register cloud services to the CSN: cloud service broker in product catalogue, which is the unique one provided to the CSC by the CSN: cloud service broker with all CSPs cloud services. The synchronization of the product catalogue can be triggered by the registered CSPs or the CSN: cloud service broker itself in case of modification in the cloud services. The CSN: cloud service broker integrates the cloud services from CSPs by an integration logic and provides the value-added services in the product catalogue. NOTE – The integration logic describes interactions among the cloud services and specifies the method to enable the interactions. After the CSC selects and orders the integrated cloud service from the product catalogue, the CSN: cloud service broker makes requests for service creation to CSPs for all cloud services which are subservices of integrated cloud service. After all cloud services are created, the CSN: cloud service broker enables interactions among cloud services by utilizing the integration logic. Once the integration procedure has been finished, the CSN: cloud service broker sends service access information to the CSC so that the CSC can accesses to the integrated cloud services. The CSN: cloud service broker manages controls and status of the integrated cloud service and each subservice is managed simultaneously. The cloud services on multiple CSPs are interacted with each other based on the service integration logic. All monitor information can be collected by the CSN: cloud service broker to provide the CSC with an overall view of cloud services together. The unified charges can be proved to the CSC by the CSN: cloud service broker.
Roles/sub-roles	CSP, CSN: cloud service broker, CSC
Figure	
Pre-conditions (optional)	The CSN: cloud service broker and multiple CSPs achieve a cooperation agreement and the CSN: cloud service broker can sell these CSPs' cloud services. The CSN: cloud service broker adapts the different cloud APIs of multiple CSPs.
Post-conditions (optional)	The CSCs can build application systems upon integrated cloud environment upon multiple CSPs based on the brokerage capabilities provided by the CSN: cloud service broker.

Table I.3 – A general use case of cloud service integration

Derived requirements	– User interface for CSCs (See clause 7.1) – Delivering cloud service provision request (See clause 7.4) – Cloud service monitoring (See clause 7.5) – Registration of cloud service (See clause 7.2)

Table I.4 – A general use case of cloud service customization

Title	A general use case for cloud service customization in cloud service brokerage.
Description	This use case describes a general use case for cloud service customization. Cloud service customization in cloud service brokerage is a service model to search, compose and provide a customized cloud service to a CSC according to the CSC' service requirements. If a CSN: cloud service broker cannot discover a service that fulfils CSC's service requirements in the product catalogue, the CSN: cloud service broker integrates and configures existing services to composite a new customized service. Such as, layering new data and process functions, visibility and analytics, or incorporating a new look and feel to the service. CSC's service requirements can consist of multiple parameters such as service names, the amount of required resources, required service levels, required software, required configurations and so on. The CSN: cloud service broker collects multiple cloud services provided by different CSPs, performs customization on these cloud services according to CSCs' requirements. (1) When a CSC could not find a satisfied service from the product catalogue, the CSC requests a cloud service with service requirements to a CSN: cloud service broker. (2) The CSN: cloud service broker searches a cloud service, which fulfils the CSC's requirements, from product catalogue. (3) If the CSN: cloud service broker cannot find an appropriate service from the service list registered in the product catalogue, the CSN: cloud service broker initiates customization process in order to generate a customized service according to the CSC's requirements. The CSN: cloud service broker integrates and/or configures (such as, layering new data and process functions) existing services. (4) Then, the CSN: cloud service broker registers the customized service in the product catalogue. (5) Finally, through workspace, the CSN: cloud service broker notifies description of the customized service to the CSC so that the CSC determines whether to use the customized service or not.
Roles/sub-roles	CSP, CSN: cloud service broker, CSC

Table I.4 – A general use case of cloud service customization

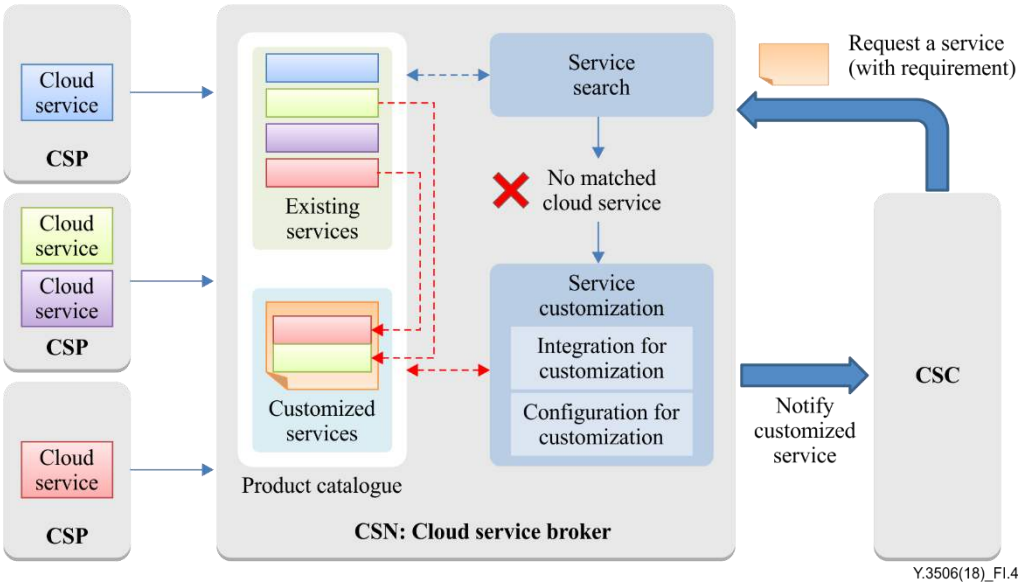
Figure	
Pre-conditions (optional)	The CSP has an account for accessing CSB workspace. There are existing services registered in the product catalogue. The CSC has an account for accessing CSB workspace. The CSC could not find a satisfied service from the product catalogue.
Post-conditions (optional)	The CSC selects a customized service to utilize. The CSN: cloud service broker and CSC establish an SLA for using the customized service. The CSC accesses to the customized service and performs necessary operations.
Derived requirements	– Providing cloud service requirement template (See clause 7.2) – Cloud service requirement validation (See clause 7.2) – Cloud service search (See clause 7.2) – Registration of cloud service (See clause 7.2) – Cloud service alteration (See clause 7.2)

Table I.5 – A use case for registration of cloud services at CSP side

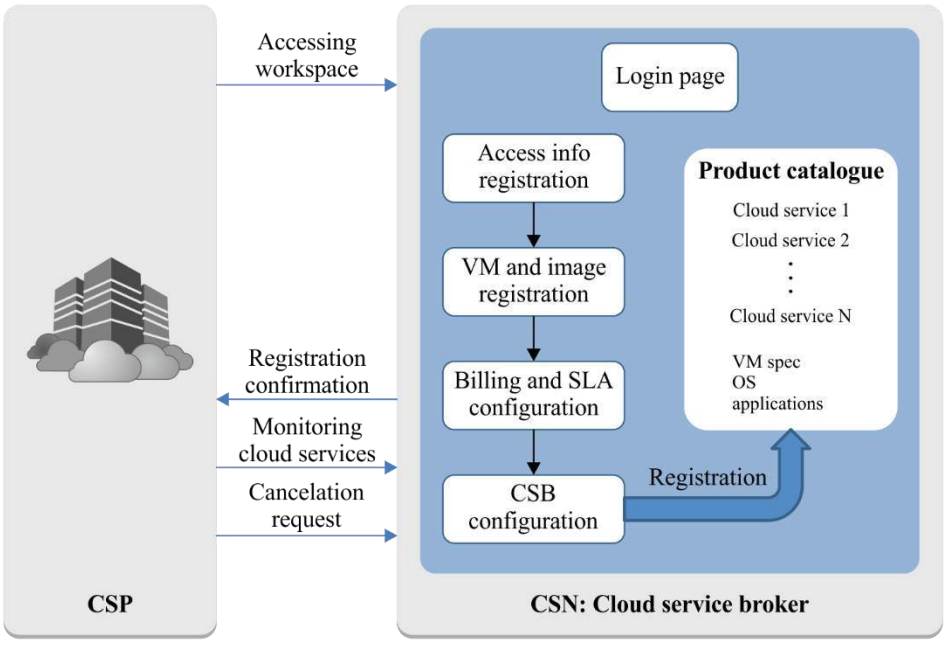
Title	A use case for registration and deregistration of cloud services at CSP side.
Description	A CSP accesses a login page in the CSB workspace using previously registered IDs and passwords. The CSP registers access information of the cloud services that will be listed in the product catalogue. The access information of the cloud services would be connection ID, connection password, endpoint URL and location. Then, the CSP defines the unit of cloud service by enrolling the information of its cloud services. The unit of cloud service encompasses its name, specification of virtual machine, images including a particular OS, agent software and related applications. The CSP can defines various types of unit of cloud services in the workspace. For example, the specification of virtual machine can varies depending on the number of virtual central processing unit (CPU), size of random access memory and size of storage. The images also can be diverse in accordance with OS types, OS version and presence of specific applications. On each constructed unit of cloud services, the CSP registers the billing information and SLA. After registering cloud services, the CSP asks a CSN: cloud service broker to add the cloud services into product catalogues in the workspace in the CSC side. The CSN: cloud service broker validates each SLA and security aspects of the cloud services and, if there is no problem, performs the confirmation of the registration.
Roles/sub-roles	CSP, CSN: cloud service broker
Figure	
Pre-conditions (optional)	The CSP is a member of the CSN: cloud service broker and has an account for accessing CSB workspace.
Post-conditions (optional)	The CSC can select cloud services on product catalogue.
Derived requirements	– Registration of cloud service (See clause 7.2) – User interface for CSPs (See clause 7.1)

Table I.6 – A use case of cloud service selection and configuration from CSC

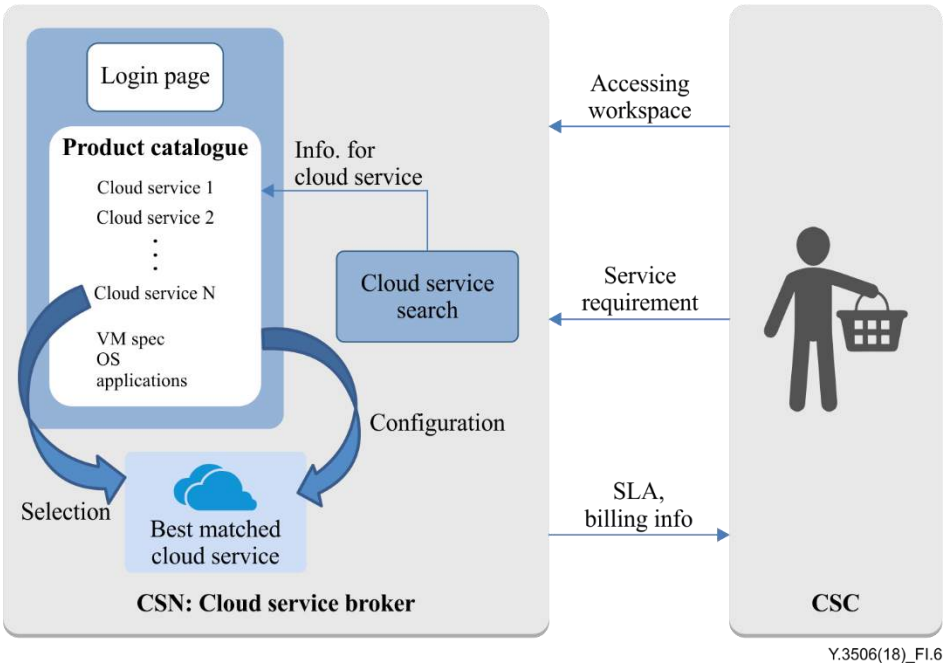
Title	A use case of cloud service selection and configuration from CSC.
Description	A CSC accesses a workspace provided by a CSN: cloud service broker with previously registered IDs and passwords. Cloud services shown in a product catalogue are usually managed in the form of images that packages a virtual machine, OS and applications. To search cloud services that the CSC wants to use, the CSC inputs information of the cloud services into the workspace. The information of the cloud services would be CSP's location, prices, hardware specification of virtual machine, OS types, applications, SLA, etc. The CSN: cloud service broker can automatically find the services best matched with search terms from the CSC. The CSB workspace also provides the interfaces where the CSC can search the cloud services in a product catalogue manually. In some cases, a CSC can configure a cloud service by selecting separate elements of the cloud service not by choosing a full packaged cloud service. After searching or configuring a cloud service, a CSC receives corresponding SLAs and billing information adjusted by the CSN: cloud service broker. On CSC's acceptance, the contract phase begins, otherwise the CSC can search and configure cloud services again.
Roles/sub-roles	CSP, CSN: cloud service broker, CSC
Figure	
Pre-conditions (optional)	The CSC is a member of the CSN: cloud service broker and has an account for accessing CSB workspace.
Post-conditions (optional)	The contract between the CSC and CSN: cloud service broker is established.
Derived requirements	– Providing the best matched cloud service (See clause 7.2) – Configuration of cloud service for contract (See clause 7.3)

Table I.7 – A use case for cloud service cancellation

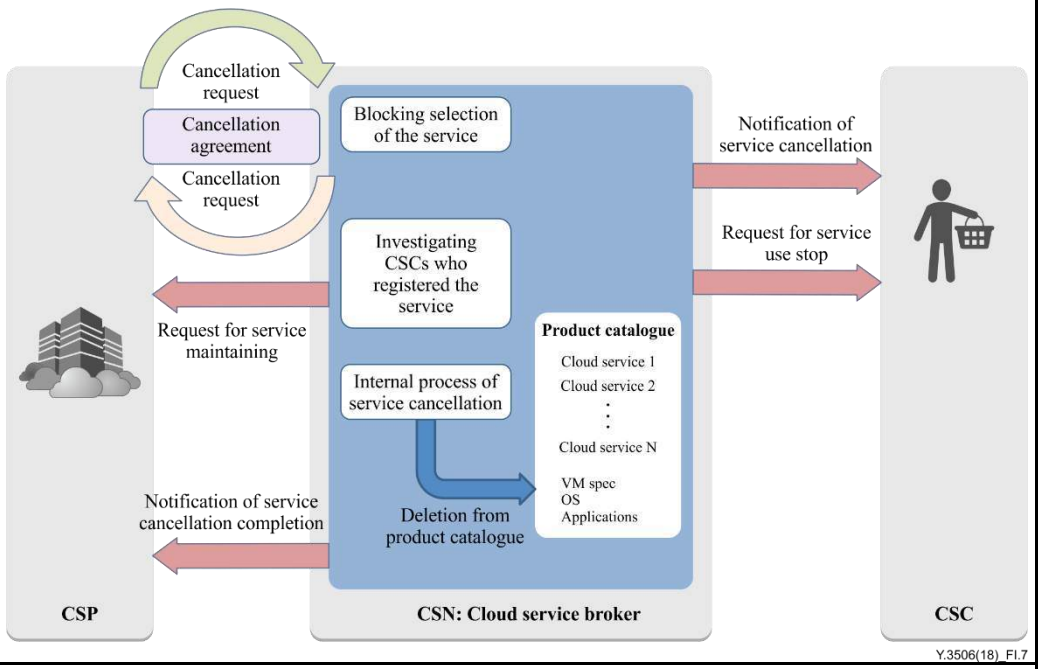
Title	A use case for deregistration of cloud services
Description	This use case assumes that cloud service deregistration is performed when the contract between a CSP and a CSN: cloud service broker is cancelled during normal contract agreement. The contract cancellation is out of scope and the abnormal situations such as bankruptcy and service disruption of the CSP are not considered in this contribution. Service deregistration can be done by the request from a CSP or a CSN: cloud service broker. A CSP initiates deregistration of the cloud service for some internal situations (e.g., modification or unavailability of the cloud service) during the cloud service. A CSN: cloud service broker can also request to deregister the cloud service, e.g., violation of contract requirement by CSPs. When the service deregistration is agreed with each other between a CSP and a CSN: cloud service broker and it is confirmed, the CSN: cloud service broker stops the CSCs search and selects the service targeted to be deregistered and stops posting the service list at the workspace from the product catalogue. The CSN: cloud service broker also investigates the CSCs that have contacted to use the service and, if they exist, notifies deregistration of the service to the registered CSCs. When CSCs are using the service currently, the CSN: cloud service broker requests the CSP to maintain the service until the CSCs finish using the service. After that, the CSN: cloud service broker cancels the contract corresponding to the cloud service between the CSN: cloud service broker and the CSC and, if needed, renews the contract between them. To complete the service deregistration, the CSN: cloud service broker can start the internal process of deregistration. The CSN: cloud service broker deregisters the service on a product catalogue and invalidates all related information such as monitoring, metering, CSC's account, SLA, etc. CSP's APIs that allow the CSC to interact with the CSP are also disabled so as not to access the service any more. The CSN: cloud service broker finally notifies the CSP deregistration that the cloud service is completed.
Roles/sub-roles	CSP, CSN: cloud service broker, CSC
Figure	
Pre-conditions (optional)	A CSP registered a cloud service to the list of a product catalogue in a CSN: cloud service broker. A CSC signed a contract with a CSN: cloud service broker for cloud service.
Post-conditions (optional)	A CSC cannot search the cloud services on product catalogue and cannot use the cloud service.

Table I.7 – A use case for cloud service cancellation

Derived requirements	– Cloud service deregistration (See clause 7.2) – Automation of service deregistration (See clause 7.2) – Notification of service deregistration (See clause 7.2) – Request for maintaining cloud service (See clause 7.2)

Table I.8 – A use case for SLA establishment in cloud service brokerage

Title	A use case for SLA establishment in cloud service brokerage.
Description	This use case describes SLA establishment among a CSN: cloud service broker, CSPs and CSCs. SLA is a part of the cloud service agreement that includes cloud service level objectives (SLO) and cloud service qualitative objectives for the covered cloud service(s) [b-ISO/IEC 19086-1]. Since a CSC communicates with a CSN: cloud service broker to consume a cloud service, the CSN: cloud service broker is responsible for establishing a SLA with the CSC. Also, CSPs need to provide service level information to the CSN: cloud service broker so that the CSN: cloud service broker understands feasible service levels. A CSP determines to sell cloud services though a CSN: cloud service broker and the CSP registers cloud service information including service level in CSB workspace. For instance, the CSP can provide "service availability" service level which can be expressed as a percentage of uptime to total usage time of a cloud service. The CSP registers a lower limit for the availability service level (ex: 99.99%) and remedies (e.g., discounting service price) for failure to meet the SLA to the CSN: cloud service broker. The CSN: cloud service broker verifies that all services with service level descriptions are correctly registered by the CSP. The CSN: cloud service broker repackages services, registered by the CSP, into brokerage services according to business needs such as service customization or service integration. The CSN: cloud service broker needs to provide service levels of a service which the CSC requests to the CSN: cloud service broker. For instance, the CSN: cloud service broker repackages a service and offers 99.98% of service availability where the service level of the original service registered by the CSP is 99.99%. The CSC, who needs an IaaS service satisfying at least 99.90% availability, connects to CSB workspace and selects a cloud service according to the business requirements. After the CSC selects a cloud service, the CSN: cloud service broker generates a SLA document and shares the SLA document to CSC. Once the CSC accepts terms and conditions in the SLA document, a SLA between the CSN: cloud service broker and the CSC is established. After the SLA between the CSN: cloud service broker and the CSC is established, the CSN: cloud service broker makes a request to the CSP to initiate the service. When the CSN: cloud service broker makes the request, it is assumed that a SLA between the CSP and the CSN: cloud service broker is established according to the service level descriptions registered by the CSP.
Roles/sub-roles	CSP, CSN: cloud service broker, CSC

Table I.8 – A use case for SLA establishment in cloud service brokerage

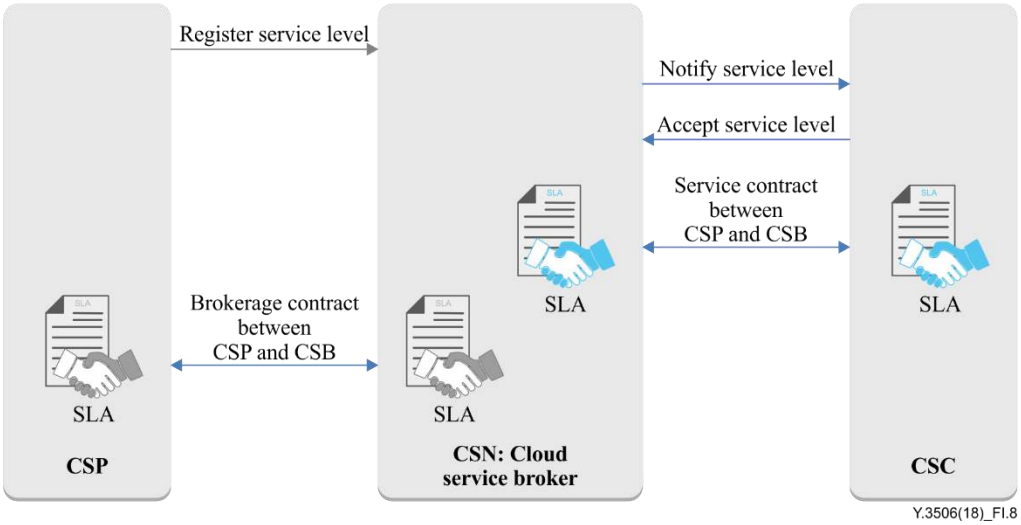
Figure	
Pre-conditions (optional)	The CSP is a member of the CSN: cloud service broker and has an account for accessing CSB workspace. The CSC is a member of the CSN: cloud service broker and has an account for accessing CSB workspace. The CSP registered cloud service information including service level in CSB workspace.
Post-conditions (optional)	The CSN: cloud service broker makes a request for provisioning of a service, which complies with the contracted SLA, to a CSP. The CSN: cloud service broker monitors status of the brokered service to comply with SLA.
Derived requirements	– Service level objectives selection (See clause 7.3) – SLA document management (See clause 7.3) – SLA description model (See clause 7.3)

Table I.9 – A use case for cloud service management in CSB

Title	A use case for cloud service management in CSB.
Description	This use case describes providing a cloud service to a CSC and a service management during the service period. (1) On behalf of the CSC, the CSN: cloud service broker requests to create a service to the CSP that can accommodate the service requirements. (2) The requested CSP creates a service according to the service requirements. (3) The CSP informs on a creation of the service and provides information for accessing the service such as service access point, ID and password to the CSN: cloud service broker. (4) The CSN: cloud service broker forwards the access information to the authorized CSC. (5) Using the access information, the CSC accesses and utilizes the created service. (6) During the service period, the CSN: cloud service broker manages SLA. A. The CSN: cloud service broker periodically monitors the service about service level (e.g., availability should be higher than 99.98%) described in the SLA established between the CSN: cloud service broker and the CSC. B. When the CSN: cloud service broker detects service level is lower than the agreed service level (e.g., measured availability becomes lower than 99.98%), the CSN: cloud service broker notifies the failure to meet the SLA to the CSC. Also, according

Table I.9 – A use case for cloud service management in CSB

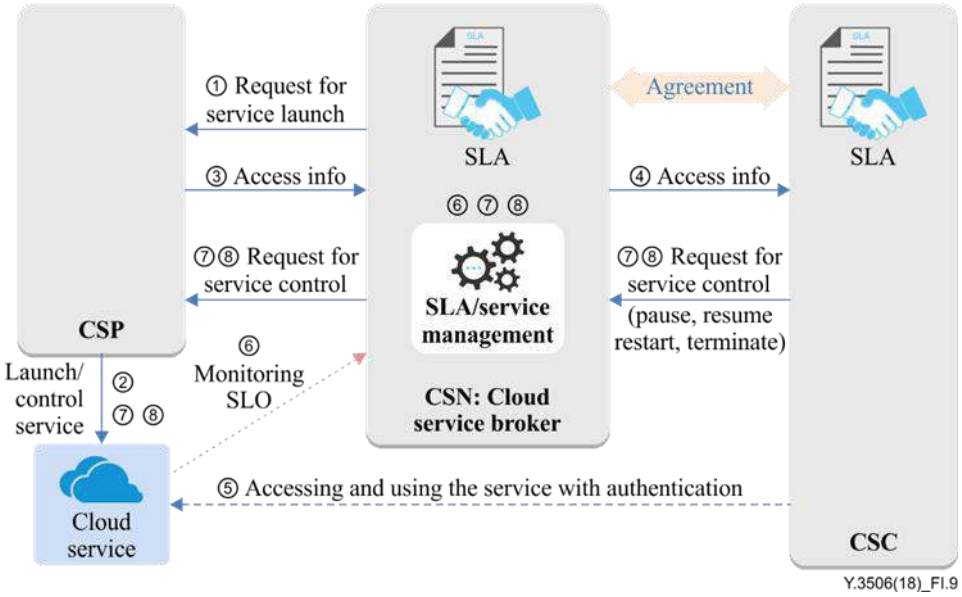
	to the SLA, the CSN: cloud service broker performs remedies (e.g., provides bonus point to the CSC or scales up the service) C. Finally, if the failure to meet the SLA is caused by the CSP who operates the service, the CSN: cloud service broker and the CSP settle the failure. (7) During the service period, the CSC makes a request to the CSN: cloud service broker to control (e.g., pause, resume, or restart) the service. A. The CSN: cloud service broker records the request information from the CSC. B. The CSN: cloud service broker makes a control request (e.g., pause, resume, or restart) to the CSP, who is operating the service. C. The CSP controls the service according to the request from the CSN: cloud service broker and replies with a result of control to the CSN: cloud service broker. D. The CSN: cloud service broker verifies the control request is correctly performed. E. Through the CSB workspace, the CSC is notified that the request has been performed. (8) During the service period, the CSC makes a request to the CSN: cloud service broker to stop and terminate the service. A. The CSN: cloud service broker records the termination request information from the CSC. B. The CSN: cloud service broker makes a termination request to the CSP, who is operating the service. C. The CSP stops and terminates the service according to the request from CSN: cloud service broker and replies with a result of termination to the CSN: cloud service broker. D The CSN: cloud service broker verifies the service is correctly terminated. E Through the CSB workspace, the CSC is notified the termination has been performed and the cost of the service usage.
Roles/sub-roles	CSP, CSN: cloud service broker, CSC
Figure	
Pre-conditions (optional)	The CSP is a member of the CSN: cloud service broker and has an account for accessing CSB workspace. The CSC is a member of the CSN: cloud service broker and has an account for accessing CSB workspace. The CSC selected a cloud service to utilize. The CSN: cloud service broker and the CSC established a SLA.

Table I.9 – A use case for cloud service management in CSB

Post-conditions (optional)	
Derived requirements	– Delivering request of cloud service control (See clause 7.5) – Validation of result for request of cloud service control (See clause 7.5) – History of cloud service control status validation (See clause 7.5) – Cloud service monitoring (See clause 7.5) – Detection of failures to meet the terms of the SLA (See clause 7.5) – Remedies for failures to meet the terms of the SLA (See clause 7.3) – Delivering cloud resource request (See clause 7.4)

Table I.10 – A use case of cloud service control status validation

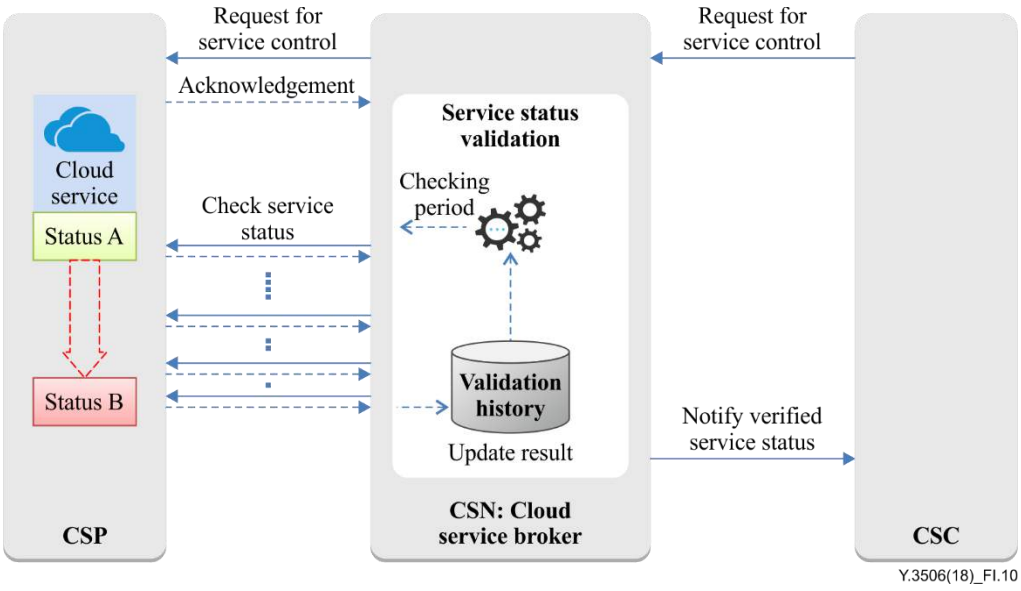
Title	A use case for cloud service control status validation in cloud service brokerage.
Description	This use case describes a validation of legitimate service status after a CSN: cloud service broker made a request for an action (e.g., create, pause, resume, or restart) to change service status on behalf of a CSC. Since a CSP and a CSN: cloud service broker are not tightly coupled, the CSN: cloud service broker does not know the result of the control request instantly. So, a CSN: cloud service broker needs to keep checking status of service by communicating with the CSP until the CSN: cloud service broker verifies whether the control request is correctly performed or not. (1) On behalf of the CSC, the CSN: cloud service broker makes a control request (e.g., create, pause, resume, restart, or terminate) to the CSP who is hosting the service. (2) The requested CSP sends an acknowledgement to the CSN: cloud service broker for the service control request and starts to control a service accordingly. (3) After the CSN: cloud service broker receives the acknowledgement, the CSN: cloud service broker sets a time window to wait and periodically verify the service status. The CSN: cloud service determines an efficient period to repeat a communication with the CSP to get information on the latest service status. (4) The CSN: cloud service broker verifies that the current service status complies with the ideal service status by the request from the CSC. The CSN: cloud service broker keeps communicating with the CSP until the service status becomes ideal status or error status, or a certain deadline is over. (5) Finally, through the workspace, the CSN: cloud service broker notifies the result of service control to the CSC.
Roles/sub-roles	CSP, CSN: cloud service broker, CSC
Figure	
Pre-conditions (optional)	The CSP has an account for accessing CSB workspace. The CSC has an account for accessing CSB workspace. The CSC selected a cloud service to utilize. CSN: cloud service broker and CSC established a SLA.

Table I.10 – A use case of cloud service control status validation

Post-conditions (optional)	
Derived requirements	– Initiation of validation (See clause 7.5) – Validation of result for request of cloud service control (See clause 7.5) – History of cloud service control status validation (See clause 7.5) – Status checking period for validation (See clause 7.5) – Notification of result for request of cloud service control (See clause 7.5)

Table I.11 – A use case for cloud service migration in cloud service brokerage

Title	A use case for cloud service migration in cloud service brokerage.
Description	This use case describes cloud service migration in cloud service brokerage during the service period. The CSC is using a cloud service provided by the CSP(A) under a contract with a CSN: cloud service broker. The CSC determines to change the physical location of the service according to some usage requirements. For instance, the CSC, who operates a business using the cloud service, may determine to move business location to another country. The CSC makes a request to migrate the cloud service to the CSN: cloud service broker. The CSN: cloud service broker searches product catalogue to select a CSP candidate (CSP(B)) who provides an equivalent service with the existing service. The CSN: cloud service broker and the CSC negotiate to determine the most appropriate service for the migration. After the CSN: cloud service broker reaches an agreement, the CSN: cloud service broker notifies the updated service information due to the service migration. On behalf of the CSC, the CSN: cloud service broker requests to create a service to the CSP(B) that can accommodate the service requirements. The requested CSP(B) creates a service according to the service requirements. The CSN: cloud service broker makes a request for service migration to the CSP(A) so that the CSP(A) migrates data and the status of the existing service to the service created by the CSP(B). After the CSN: cloud service broker confirms that the migration of status and data was accomplished, the CSP(B) initiates the created service using the transferred data and status. The CSP(B) informs on a creation of the service and provides information for accessing the service such as service access point, ID and password to the CSN: cloud service broker. Using the access information, the CSC accesses and utilizes the created service. Finally, the CSN: cloud service broker requests termination of the existing service to the CSP(A) and ends their contract.
Roles/sub-roles	CSP, CSN: cloud service broker, CSC

Table I.11 – A use case for cloud service migration in cloud service brokerage

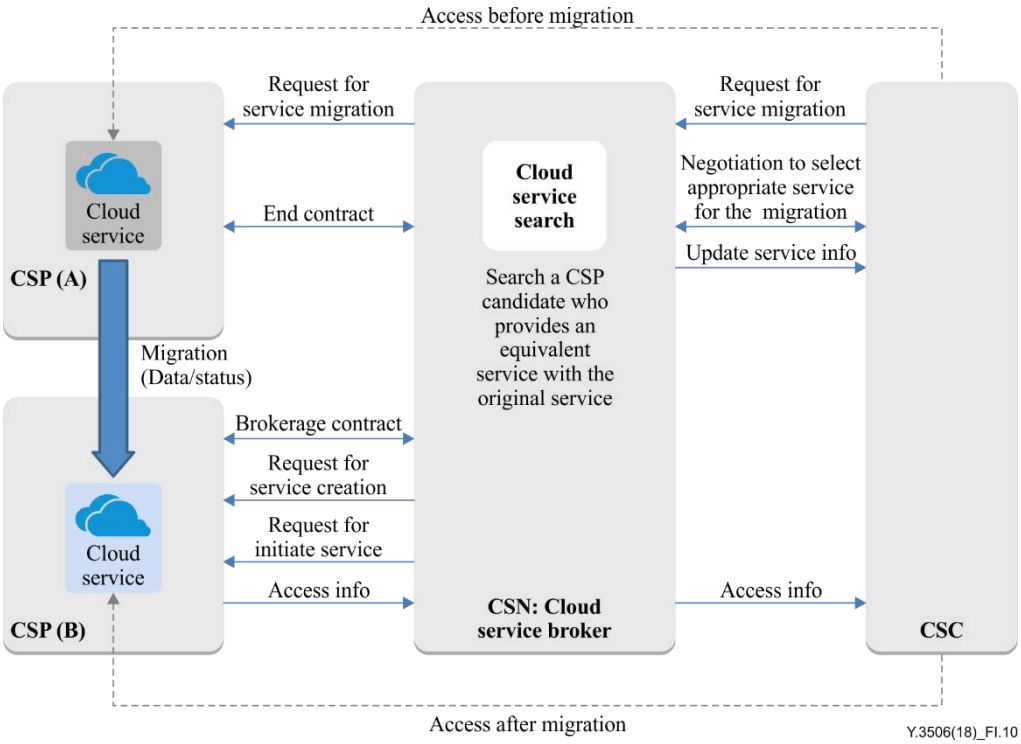
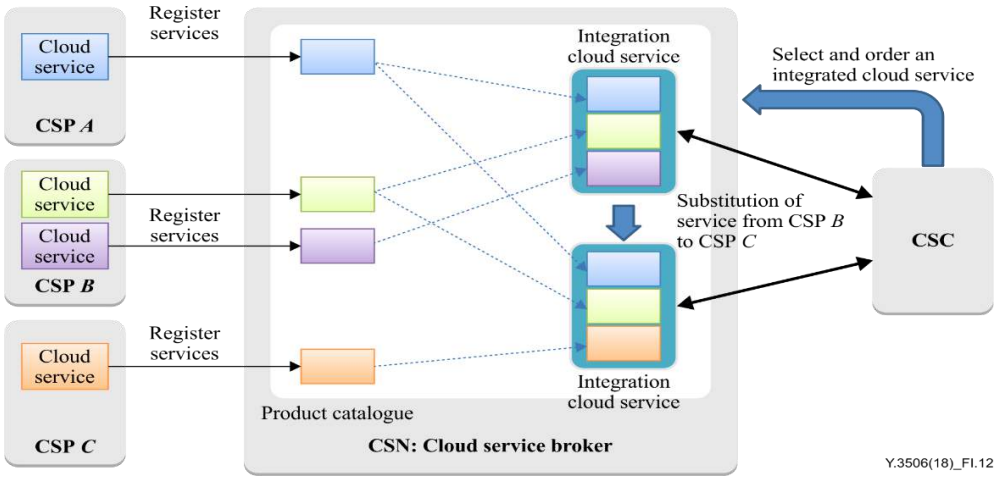
Figure	
Pre-conditions (optional)	The CSP is a member of the CSN: cloud service broker and has an account for accessing CSB workspace. The CSC is a member of the CSN: cloud service broker and has an account for accessing CSB workspace. The CSN: cloud service broker and the CSC established a SLA. The CSC is using a cloud service provided by the CSP(A) though the CSN: cloud service broker.
Post-conditions (optional)	
Derived requirements	– Equivalent cloud service selection (See clause 7.2) – Prevention of service termination during migration (See clause 7.5)

Table I.12 – A use case of cloud service substitution

Title	A use case of cloud service substitution.
Description	This use case describes a substitution of cloud service used as a member of an integrated cloud service in cloud service brokerage to keep the SLA between a CSN: cloud service broker and a CSC. Various CSPs in the market can register their services with the CSN: cloud service broker. Different CSPs can register services, which provide the same functionalities to the CSN: cloud service broker. The CSN: cloud service broker registers a catalogue which describes integrated cloud service based on multiple cloud services from the different CSPs. The registered catalogue is provided as a new integrated cloud service through the CSN: cloud service broker. The CSC selects a cloud service from the CSN: cloud service broker's product catalogue and use that cloud service according to SLA. (1) The CSN: cloud service broker monitors the integrated cloud service in real time to check whether it satisfies the SLA. In addition, real-time monitoring is performed on a

Table I.12 – A use case of cloud service substitution

	member of an integrated cloud service to cope with SLA violation or unavailability situations. (2) If the integrated cloud service does not meet the SLA continuously, the CSN: cloud service broker detects the member cloud service that provides the cause. (3) The CSN: cloud service broker provisions another integrated cloud service which can substitute original one, based on the product catalogue description. At this time, when a large number of candidates for alternative integrated cloud services are searched, priority is evaluated for them and the CSN: cloud service broker makes a final decision for alternative integrated cloud service based on SLA in the aspect of service stability. (4) The CSN: cloud service broker substitutes the provisioned service for the previous one to satisfy the SLA.
Roles/sub-roles	CSP, CSN: cloud service broker, CSC
Figure	
Pre-conditions (optional)	– The CSPs register services to the CSN: cloud service broker. – The CSN: cloud service broker registers an integrated cloud to product catalogue.
Post-conditions (optional)	
Derived requirements	– Cloud service substitution for integrated cloud service (See clause 7.2) – Detection of failures to meet the terms of the SLA (See clause 7.5)

Appendix II

Relationship between the logical components and the activities of cloud service broker for CSB

(This appendix does not form an integral part of this Recommendation.)

Activities of cloud service broker for CSB consist of (1) acquire and assess customers, (2) assess marketplace, (3) set up legal agreement, (4) assist CSC for accessing service and (5) check and control service status.

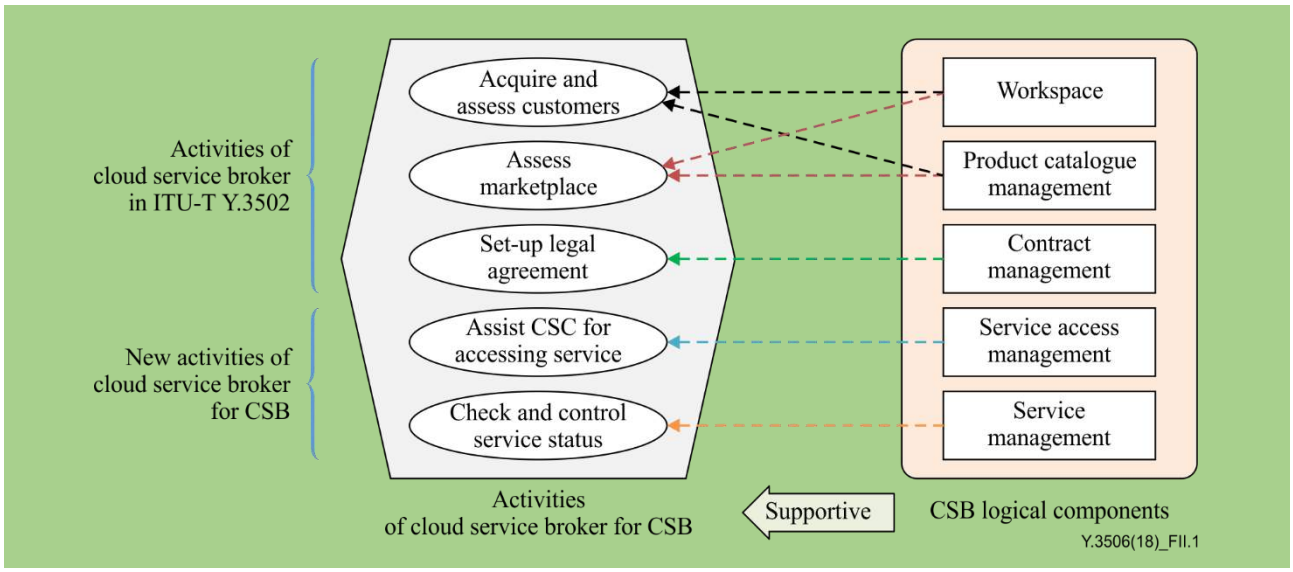


Figure II.1 – Relationship between the logical components and the activities of cloud service broker for CSB

NOTE – Figure II.1 identifies reused activities from [ITU-T Y.3502] as well as new activities needed to support cloud service brokerage.

(1) **Logical components that can cover the acquire and assess customers activity:** The acquire and assess customers activity includes the tasks required to market and sell cloud services up to the point where a cloud service customer agrees a contract to use one or more services, see clause 8.4.2.6 in [ITU-T Y.3502]. The workspace and the product catalogue management logical components cover the acquire and assess customers activity. The workspace logical component (clause 6.4.1) provides a user interface for CSCs to help to present service requirements and to request a cloud service. Also the product catalogue management logical component (clause 6.4.2) provides information to potential CSCs about available services and associated SLAs and contract terms. So, both logical components support the marketing and selling of cloud services up to the point where a cloud service customer agrees a contract to use one or more services.

(2) **Logical components that can cover the assess marketplace activity:** The assess marketplace activity focuses on assessing the current cloud services marketplace to find cloud service(s) that meet the customers' requirements see clause 8.4.2.7 in [ITU-T Y.3502]. The workspace logical component (clause 6.4.1) and the product catalogue management logical component (clause 6.4.2) cover the assess marketplace activity. The workspace logical component provides a user interface for CSPs. In workspace, a CSP can register, modify and remove a service list to be sold through a cloud service broker. Also the product catalogue management logical component gathers cloud services from multiple CSPs through workspace, registers those cloud services and, if needed, cancels the registered cloud services. So, both logical components support assessing the current cloud services marketplace to find cloud service(s) that meet the customers' requirements.

(3) **Logical components that can cover the set up legal agreement activity:** The set up legal agreement activity concerns the service agreement between the cloud service customer and the chosen cloud service provider(s) see clause 8.4.2.8 in [ITU-T Y.3502]. The contract management logical component (clause 6.4.3) manages all contracts in CSB in terms of SLA. So, the contract management logical component fully covers the set up legal agreement activity.

(4) **Logical components that can cover the assist CSC for accessing service activity:** The assist CSC for accessing service activity focuses on acquiring access information for a cloud service from a CSP who provides the cloud service and forwarding of the access information to the CSC who requested the cloud service so that the CSC understands how to access to and use the service. The service access manager logical component (clause 6.4.4) manages access information of cloud services brokered by a cloud service broker by acquiring access information from the CSP. Also, the service access management logical component is capable of forwarding access information to a proper CSC. So, the service access management logical component fully supports the assist CSC for accessing service activity.

(5) **Logical components that can cover the check and control service status activity:** The check and control service status activity focuses on assisting CSCs in cloud service controls such as stopping, resuming and terminating cloud services. Also, this activity involves checking status of running cloud services by monitoring so that a cloud service broker enforces service qualities agreed in a SLA instead of CSCs. Since the service management logical component (clause 6.4.5) is a logical component to manage controls and status of running cloud services brokered by a cloud service broker, the service management logical component fully supports the check and control service status activity.

Bibliography

[b-ISO/IEC 19086-1] ISO/IEC 19086-1:2016, *Information technology – Cloud computing – Service Level Agreement (SLA) framework – Part 1:Overview and concepts*. https://www.iso.org/standard/67545.html

Cloud computing – Functional requirements of physical machine

Recommendation ITU-T Y.3507

(12/2018)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Summary

The physical machine is a type of computing machine to provide physical resources. Since all cloud services have to reside and operate on physical machines, it is important for the cloud service providers as well as for the manufacturers to identify specific functional requirements of the physical machine.

Recommendation ITU-T Y.3507 provides an introduction to the physical machine including the physical machine components, physical machine types, virtualizations in the physical machine as well as the scalability of components in the physical machine.

In addition, this Recommendation provides functional requirements for the physical machine derived from various use cases described in Appendix II. The relationship with other related specifications developed in other Standards Development Organizations (SDOs) has is introduced in Appendix I.

Keywords

Cloud computing, functional requirements, physical machine.

Table of Contents

1 Scope

This Recommendation provides the functional requirements of the physical machine for cloud computing based on cloud computing infrastructure requirements presented in [ITU-T Y.3510]. This Recommendation addresses the following:

– Overview of the physical machine;

– Functional requirements of the physical machine. The functional requirements provided in this Recommendation are derived from use cases.

NOTE 1 – This Recommendation does not advocate, imply, or assume the use of any specific set or sets of technical specifications. Examples of such sets of technical specifications can be found in Appendix I.

NOTE 2 – This Recommendation addresses a set of use cases which are included in Appendix II.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.3100] Recommendation ITU-T Y.3100 (2017), *Terms and definitions for IMT-2020 network.*

[ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary.*

[ITU-T Y.3510] Recommendation ITU-T Y.3510 (2016), *Cloud computing infrastructure requirements.*

[ITU-T Y.3521] Recommendation ITU-T Y.3521/M.3070 (2016), *Overview of end-to-end cloud computing management.*

[ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 cloud computing [ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

3.1.2 cloud service [ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.3 cloud service customer [ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

3.1.4 cloud service provider [ITU-T Y.3500]: Party which makes cloud services available.

3.1.5 physical resource [ITU-T Y.3100]: A physical asset for computation, storage and/or networking.

NOTE – Components, systems and equipment can be regarded as physical resources

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 physical machine: A type of computing machine providing physical resources.

NOTE – A computing machine provides allocation and scheduling of processing resources. Types of computing machine are physical or virtual [ITU-T Y.3510].

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AC	Alternating Current
AI	Artificial intelligence
API	Application Programming Interface
ATA	AT Attachment
CD	Compact Disc
CPU	Central Processing Unit
CSC	Cloud Service Customer
CSP	Cloud Service Provider
DC	Direct Current
DRAM	Dynamic Random Access Memory
ECC	Error Correcting Code
FSC	Fan Speed Control
GPU	Graphics Processing Unit
HDD	Hard Disk Drive
I2C	Inter-Integrated Circuit
IDE	Integrated Development Environment
IaaS	Infrastructure as a Service
IPMI	Intelligent Platform Management Interface
IT	Information Technology
I/O	Input/Output
iSCSI	Internet Small Computer System Interface
NIC	Network Interface Card
NFV	Network Function Virtualization
NGFF	Next Generation Form Factor
mSATA	Mini-Serial AT Attachment
OPEX	Operational Expenditure
OS	Operating System
PCI	Peripheral Component Interconnect
PCI-E	Peripheral Component Interconnect Express
PDU	Power Distribution Unit
PMBus	Power Management Bus
PWM	Pulse Width Modulation
RAID	Redundant Array of Independent Disks
RPM	Revolutions Per Minute
ROM	Read-Only Memory

SAS	Serial Attached SCSI
SATA	Serial AT Attachment
SCSI	Small Computer System Interface
SEL	System Event Log
SoC	System-on-a-Chip
SRAM	Static Random Access Memory
TCP	Transmission Control Protocol
UART	Universal Asynchronous Receiver/Transmitter
USB	Universal Serial Bus
VGA	Video Graphics Array
VM	Virtual Machine

5 Conventions

In this Recommendation:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "is not recommended" indicate a requirement which is not recommended but which is not specifically prohibited. Thus, conformance with this specification can still be claimed even if this requirement is present.

The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Overview of the physical machine

6.1 Introduction to the computing machine

Cloud infrastructure includes processing, storage, networking and other hardware resources, as well as software assets, for more information see clause 6 in [ITU-T Y.3510]. Processing resources are used to provide essential capabilities for cloud services and to support other system capabilities such as resource abstraction and control, management, security and monitoring.

A computing machine provides allocation and scheduling of processing resources. Types of computing machine are physical or virtual [ITU-T Y.3510]. The capability of a computing machine is typically expressed in terms of configuration, availability, scalability, manageability and energy consumption [ITU-T Y.3510].

The requirements of the virtual machine, as one of categories of the computing machine, have been specified in [ITU-T Y.3510]. Those requirements include virtualization technologies that can be applied to resource types such as the central processing unit (CPU), memory, input/output (I/O) and network interfaces. Several requirements regarding virtual machine management have also been identified, e.g., duplication of a virtual machine (VM) dynamic/static migration of aVM and management automation.

For the physical machine, [ITU-T Y.3510] defines three requirements as follows.

– It is recommended to support hardware resource virtualization.

– It is recommended to support horizontal scalability (e.g., adding more computing machines) and vertical scalability (e.g., adding more resources with a computing machine).

– It is recommended to use power optimization solutions to reduce energy consumption.

It is inferred from the requirements that the physical machine supports scalable resources with consideration of energy consumption.

Figure 6-1 shows the conceptual diagram of a computing machine in [ITU-T Y.3510].

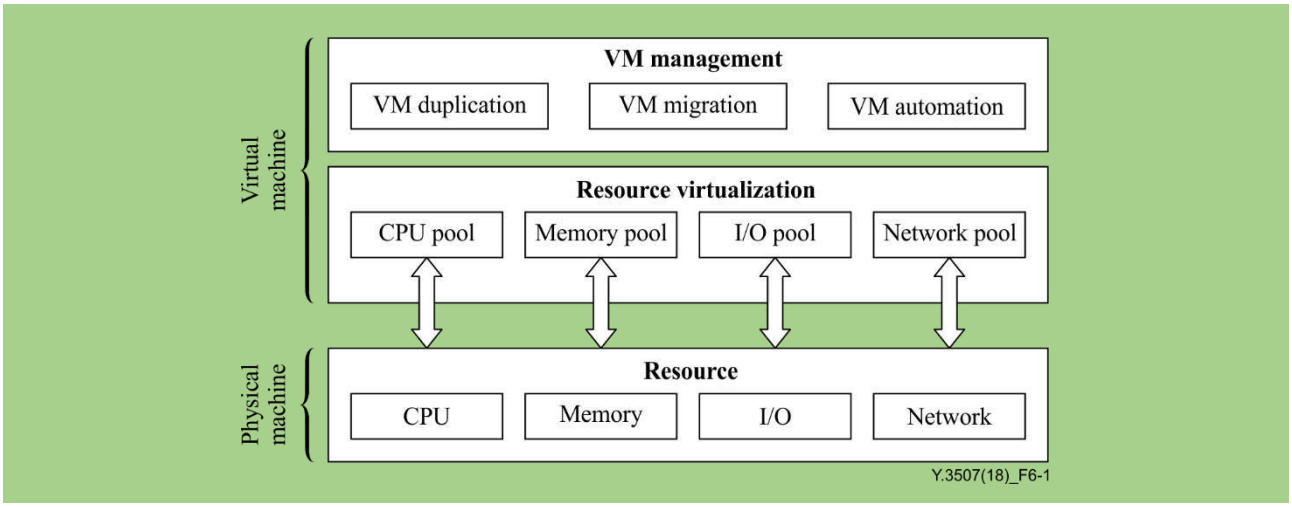


Figure 6-1 – Concept of a computing machine in [ITU-T Y.3510]

A virtual machine provides virtualized resource pools using virtualization technologies specific to physical resource types like CPU, memory, I/O and network from a physical machine. The virtual machine also covers management issues.

Since all cloud services have to reside and operate on physical machines, it is important for the cloud service providers and especially for the infrastructure as a service (IaaS) cloud service provider (CSP) who will build the cloud infrastructure, as well as for the manufacturer who will sell the cloud infrastructure, to identify specific requirements of the physical machine.

6.2 Introduction to the physical machine

The physical machine is a type of computing machine in which the cloud services must reside and operate and that provides physical resources, such as processing, storage, networking, etc.

Figure 6-2 depicts an overview of the physical machine. The scope of this Recommendation focuses on the physical machine.

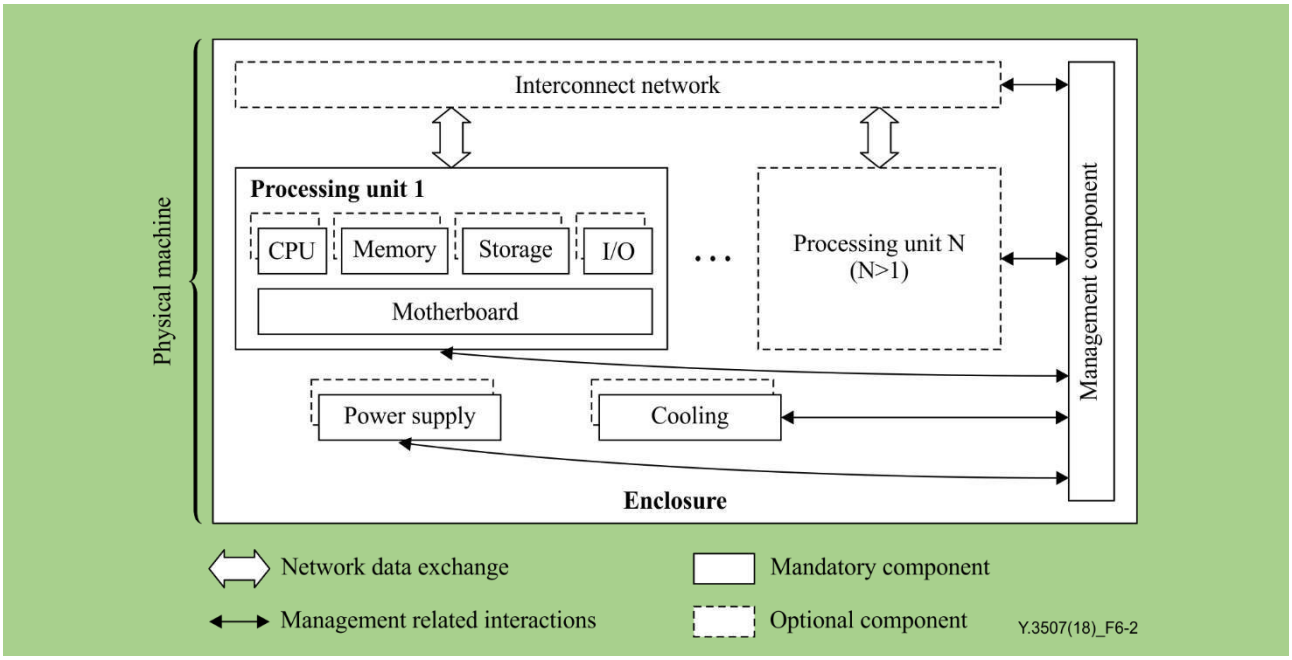


Figure 6-2 – Overview of the physical machine

The physical machine is composed of multiple components, which are described as follows:

– **Processing units**: A processing unit has CPUs, memories, storages and I/O devices. These sub-components in a processing unit are physically implemented on a motherboard. The processing unit is the basic element as a hardware processing resource and normally multiple processing units are involved to provide capacity of resources. Processing units is a mandatory component for the physical machine. A single processing unit type physical machine has only one processing unit, while a multi-processing unit type physical machine has two or more processing units.

– **Interconnect network**: An interconnect network has a role of connecting multiple processing units aiming to be used to share resources in individual processing units through virtualization. In addition, the interconnect network provides a communication interface to other external physical machines. An interconnect network is an optional component only for multi-processing unit type physical machines.

– **Enclosure**: An enclosure includes multiple processing units and other components such as power supply, cooling and interconnect network (in some cases) by providing the form factor with metal apparatus that specifies the physical dimensions of a physical machine. The enclosure also shields the electromagnetic components and helps to dissipate heat of other components. An enclosure is a mandatory component for a physical machine.

– **Power supply**: A power supply provides electrical power to all components in an enclosure. The power supply converts AC power into DC power which all components use to operate and provides redundancy to ensure that the stability and operability of a physical machine is maintained even in the case that a physical machine's power goes out. Power supply is a mandatory component for the physical machine.

– **Cooling**: A cooling system is for maintaining a certain range of temperature in an enclosure by cooling heat generated due to operation of the physical machine. The implementation type can vary depending on cooling materials (e.g., air-cooled or a water-cooled type) and form factors (e.g., air flow or water pipes) of an enclosure. Cooling is a mandatory component for the physical machine.

– **Management component**: A management component monitors and controls all components in a physical machine, by analyzing the gathered status information from the components. A management component is a mandatory component for the physical machine.

NOTE – Standard interfaces (e.g., I2C, PMbus, Ethernet, UART, PWM) are normally used to communicate between the management component and others.

Beside these components, the following are needed to manage and operate the physical machine:

– I/O interface is used for I/O device to communicate with other physical machines or CSC/CSP. The I/O interface has two capabilities (i) capability to provide the channel for data input and output of the physical machine, (ii) capability to provide the channel for CSP/CSC to access the physical machine. The I/O interface follows industrial standards so that the CSP could select and replace the components from multiple vendors. The cloud computing management system communicates with the physical machines without any other development by the standard management interface.

– Physical machine operation reports and maintains its running information, as well as environment condition periodically to the cloud computing management system [ITU-T Y.3521]. In addition, the administrator can operate the physical machine with operation capabilities.

– Scalability of components in the physical machines allows the physical machines to extend their resources elastically in the processing units, power supply and cooling system.

– Security of the physical machine provides access control of the processing units.

– Reliability of the physical machine is to keep physical machine consistently performing as expected. To provide reliability, when some components fail, the physical machine needs to support, detect and locate the faulty components.

6.3 Types of physical machine

6.3.1 Single processing unit type

The single processing unit type of physical machine has one processing unit, a single management component as well as one or more power supplies and cooling components. Since a single processing unit type has only one processing unit, no interconnect network component is involved in this type.

NOTE – An example of single processing unit type is a rack server [b-OCP BS].

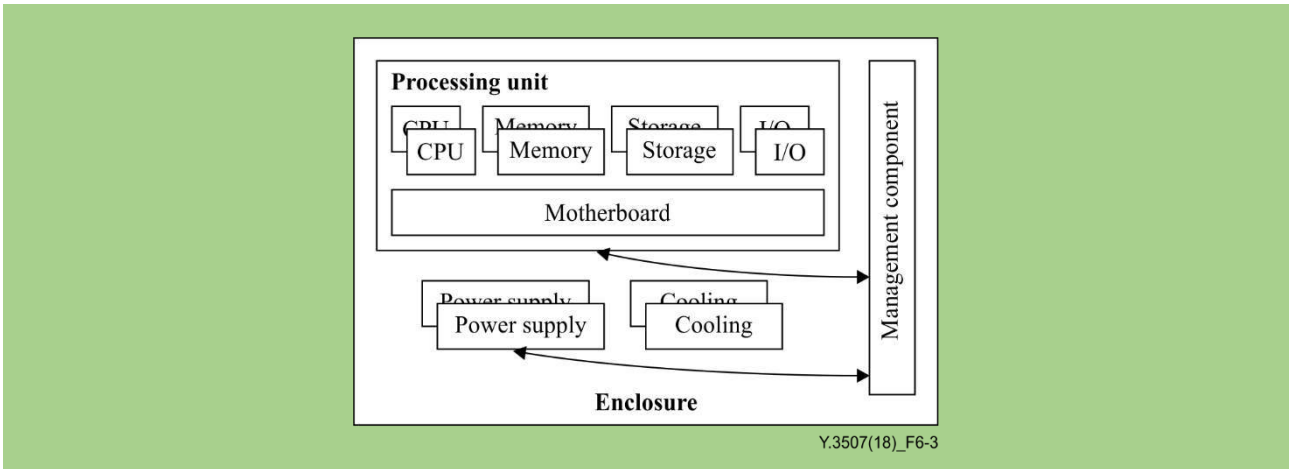


Figure 6-3 – Example of single processing unit type

6.3.2 Multi-processing unit type

The multi-processing unit type has two or more processing units, as well as one or more power supplies, cooling components and a single management component and a single interconnect network.

NOTE – Examples of a multi-processing unit type are blade servers [b-OCP OSR] and rack scale servers [b-OCP OCSC].

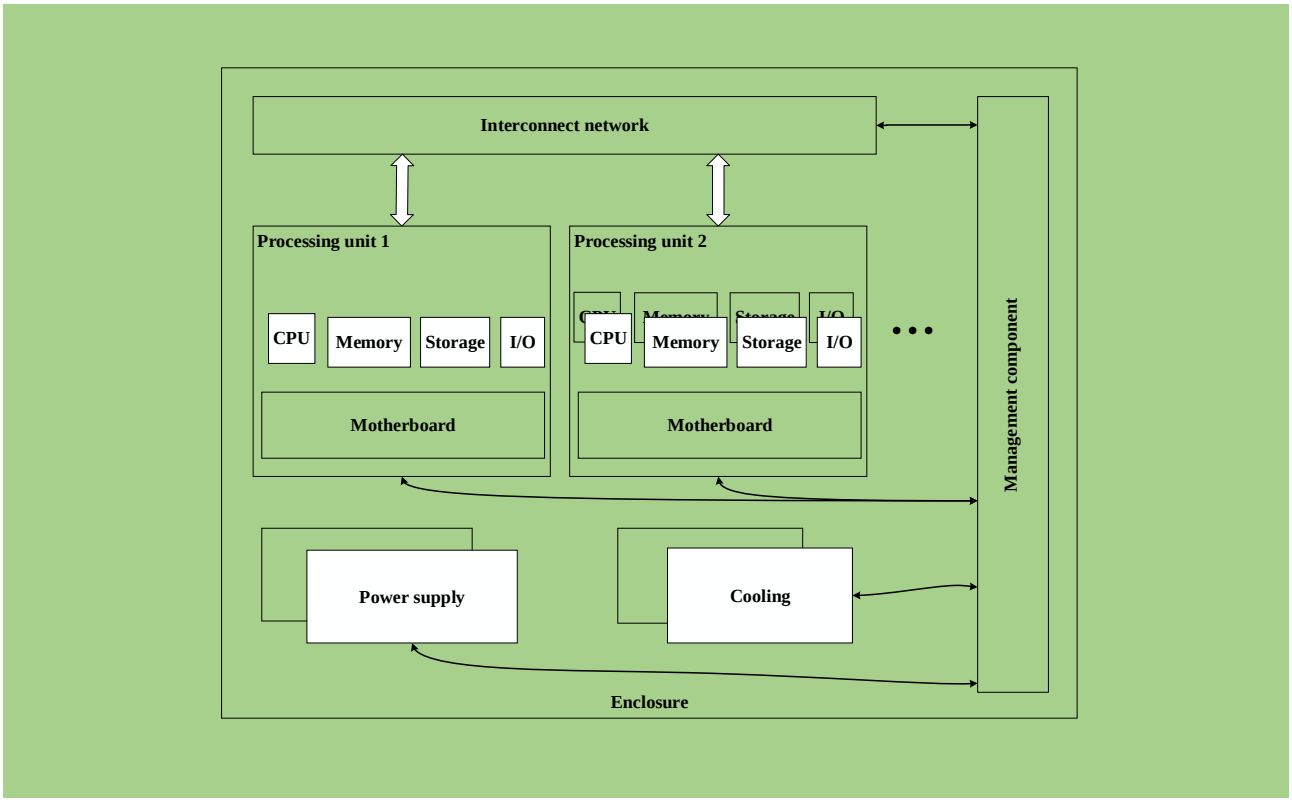


Figure 6-5 – Example of a multi-processing unit type

6.4 Virtualization in physical machines

This clause identifies different types of virtualization of the components in processing units such as CPUs, memory and I/Os. The mode of virtualization in each component can be software based mode or hardware-assisted mode. The requirements in this Recommendation only consider the hardware-assisted mode for virtualization.

6.4.1 CPU virtualization

CPU virtualization technology makes a single CPU act as if it was multiple individual CPUs. There are different ways to implement CPU virtualization. CPU virtualization can be implemented in software-based mode and in hardware-assisted mode:

– In software based mode, the privileged instructions are simulated by software.

– In hardware-assisted mode, the privileged instructions can be directly run by the physical CPU to achieve higher performance. Hardware-assisted mode requires the CPU to support a virtualization instruction set.

NOTE – The difference between the two modes is in the execution of privileged instructions in VM's operating system (OS).

6.4.2 Memory virtualization

Memory virtualization abstracts physical memory to a divided virtual memory for use by a virtual machine. There are two modes of memory virtualization: software-based and hardware-assisted memory virtualization:

– Software-based mode builds a software based memory mapping table.

– In hardware-assisted mode, a memory mapping table is implemented in hardware with better performance.

NOTE – The difference between the two modes is the mapping between virtual memory and physical memory.

6.4.3 I/O virtualization

I/O virtualization refers to dividing a single physical I/O into multiple isolated logical I/Os. There are two modes of I/O virtualization: software based and and hardware-assisted I/O virtualization:

– Software based mode simulates I/O devices based on software.

– The hardware-assisted mode provides better performance by reducing a hypervisor's participation in I/O processing by using hardware.

A network adapter is an I/O device specifically for data transmission. A network adapter provides an isolated logical I/O based on a single physical I/O to receive and send data packets inside and outside of a physical machine as virtual network interfaces in order to improve interface utilization.

6.5 Scalability of components in the physical machine

Scalability of components in a physical machine allows enhancing the processing unit, power supply and cooling components of the physical machine.

6.5.1 Scalability of the processing unit

Scalability of the processing unit allows the processing units of a physical machine to be expanded. Scalability of the processing unit provides more hardware processing resources in order to meet potential growth needs, such as providing more CPU and memory resources to host more VMs with the growth of business needs.

There are several ways to expand processing units as shown hereafter with availability of motherboard interfaces and enclosure:

– Replacing components of a processing unit with other components with higher capability, such as a CPU, memory, storage and I/O devices;

– Adding components to a processing unit, such as a CPU, memory, storage and I/O devices;

– Replacing processing units with other processing units with higher capability;

– Adding processing units to the physical machine.

6.5.2 Scalability of power supply

Scalability of power supply allows the power supply of a physical machine to be expanded. Scalability of power supply provides more power in future for the potential increasing power consumption needs of the physical machine, such as providing more power for additional processing units.

There are several ways to expand power supply as shown hereafter with availability of enclosure:

– Replacing power supplies of a physical machine with other power supplies with higher capability;

– Adding power supplies to the physical machine.

6.5.3 Scalability of cooling

Scalability of cooling allows the cooling capability of a physical machine to be increased. Scalability of cooling provides a higher cooling capability to meet the potential increasing cooling needs of the physical machine.

There are several ways to expand cooling capability as shown hereafter with availability of enclosure:

– Replacing cooling components of a physical machine with other cooling components with higher capability;

– Adding cooling components to the physical machine.

7 Functional requirements for a physical machine

7.1 Component requirements

7.1.1 Processing unit requirements

7.1.1.1 CPU requirements

– **Virtualization instruction set**: It is recommended that a physical machine supports a CPU virtualization instruction set to improve the performance of CPU virtualization.

– **CPU replacement**: It is recommended that a physical machine supports substitution of CPU with other CPUs to allow CPU upgrade or replacement of faulty CPUs.

– **Multiple CPUs**: It is recommended that a physical machine supports multiple CPUs to achieve higher performance.

– **Low power consumption of CPU**: It is recommended that a physical machine supports low power consumption of CPU to reduce the operational expenditure (OPEX).

7.1.1.2 Memory requirements

– **Hardware-assisted memory virtualization**: It is recommended that a physical machine supports hardware-assisted memory virtualization to improve the performance of memory virtualization.

– **Memory replacement**: It is recommended that a physical machine supports substitution of memory with other memories to allow memory upgrade or replacement of faulty memory.

– **Memory reliability**: It is recommended that a physical machine supports memory reliability using memory redundancy and memory error correction technologies.

NOTE 1 – Memory reliability refers to technologies to improve the reliability of the physical machine by preventing permanent loss of data or downtime caused by memory failure. One example is memory mirroring, as one implementation of memory redundancy. Memory mirroring replicates and stores data on a different physical memory within different channels simultaneously. If the primary physical memory failure occurs, subsequent read and write will use the backup memory.

– **Supporting various types of memory**: It is recommended that a physical machine provides various types of memory such as non-volatile and volatile memory depending on the CPU's memory usage.

NOTE 2 – Examples of CPU's memory usage with non-volatile and volatile types are booting up and storing temporary data as main memory, respectively. Non-volatile type includes ROM and volatile type is classified into static random access memory (SRAM) and dynamic random access memory (DRAM).

7.1.1.3 Storage requirements

– **Multiple interfaces for storage**: It is recommended that a physical machine supports interfaces of storage for different media, such as magnetic storage, optical storage and semiconductor storage.

NOTE 1 – Examples of interfaces include integrated development environment (IDE), serial AT attachment (SATA), serial attached SCSI (SAS), small computer system interface (SCSI), AT attachment (ATA), M.2 (formerly known as NGFF), peripheral component interconnect express (PCI-E) and mini-serial AT attachment (mSATA).

– **Storage replacement**: It is recommended that storage in a physical machine supports substitution of storage with other storages to allow external storage upgrade or replacement of faulty external storage.

– **Storage redundancy hardware**: It is recommended that a physical machine supports storage redundancy hardware.

NOTE 2 – An example of storage redundancy hardware is RAID card. RAID card is to support data storage virtualization technology that combines multiple physical disk drive components into one or more logical units for the purposes of data redundancy, performance improvement, or both.

– **Storage hibernation**: It is recommended that a physical machine supports hibernation of storages without I/O for a long time to reduce energy consumption.

NOTE 3 – An example of storage hibernation is hard disk drive (HDD) hibernation. The HDD spins continuously at 5400/7200 revolutions per minute (RPM) consuming lots of power. During HDD hibernation, the HDD stops spinning to reduce power consumption.

7.1.1.4 I/O device requirements

– **Hardware-assisted I/O virtualization**: It is recommended that a physical machine supports hardware-assisted I/O virtualization to improve the performance of I/O virtualization.

– **I/O devices direct accessing**: It is recommended that a physical machine supports I/O devices direct accessing so that a virtual machine can directly access hardware I/O devices.

NOTE 1 – I/O devices direct accessing refers to technologies supporting VM's native accessing of physical I/O devices. One example of I/O devices direct accessing is I/O devices pass-through. I/O devices pass-through is an I/O device assigned directly to a VM. The VM can access the I/O devices without a hypervisor's participation.

– **Workload offload**: It is recommended that a physical machine support offloading workload to I/O devices to reduce the load of the CPU.

NOTE 2 – In offloading workload, hardware I/O devices execute workload instead of software on a CPU in order to relieve the CPU's overhead. An example of offloading workload is checking transmission control protocol (TCP) checksum in a network interface card (NIC) and not in a CPU.

– **Hardware acceleration**: It is recommended that a physical machine supports application-specific hardware acceleration to perform specific applications more efficiently.

NOTE 3 – Application-specific hardware is customized for a particular use, rather than intended for general-purpose use. An example of application-specific hardware is a graphics processing unit (GPU).

7.1.2 Power supply requirements

– **Power supply replacement**: It is recommended that a physical machine supports substitution with other power supplies to allow power supply upgrade or replacement of a faulty power supply.

– **Supporting power redundancy**: It is recommended that a physical machine supports redundant power supply to keep powered on in case of main power supply failure.

NOTE 1 – N+1 redundancy of power supply is widely used (N: number of power supplies based on total power budget).

– **Minimum energy consumption**: It is recommended that a physical machine provides minimum energy consumption.

– **Interface for monitoring power**: It is recommended that a physical machine supports an interface to a management component for monitoring status of the power supply.

NOTE 2 – An example of the interface for monitoring power is a power management bus (PMBus).

7.1.3 Cooling requirements

– **Cooling component replacement**: It is recommended that a physical machine supports substitution with other cooling components to allow substitution of a faulty cooling component.

– **Cooling component redundancy**: It is recommended that a physical machine supports cooling component redundancy to maintain temperature in case of main cooling component failure.

– **Interface for controlling fan speed**: It is recommended that a physical machine supports an interface to a management component to control fan speed.

NOTE – An example of an interface for controlling fan speed is a pulse width modulation (PWM) management component.

7.1.4 Enclosure requirements

– **Monitoring status of the physical machine**: It is recommended that a physical machine provides a status panel to check whether components of the physical machine are installed and working correctly.

– **Visual indications**: It is recommended that a physical machine provides visual indications of working state (e.g., starting, running, stopped, faulty), suitable for administrators of the physical machine to understand.

– **Equipment for mounting and removal**: It is recommended that a physical machine supports safe mounting and easy removal of all components in the enclosure.

– **Circulation of air flow**: It is recommended that a physical machine supports circulation of enough air flow to minimize the heat generated inside the enclosure with cooling components.

7.1.5 Interconnect network requirements

This functional requirement is applied for multi-processing unit types.

– **Interconnect network supports**: It is recommended that a physical machine supports a non-Ethernet based interconnect network as well as an Ethernet based interconnect network among the multiple processing units.

NOTE 1 – For this non-Ethernet based interconnect network, a CSP:cloud operations manager employs a CPU I/O (e.g., PCI Express) of processing units to construct the interconnect network.

– **Sharing process unit component**: It is recommended that a physical machine provides a sharing component in the processing unit in other processing units by an interconnect network.

NOTE 2 – Examples of sharing components are memory, storage and I/O.

– **Network topology**: It is recommended that a physical machine supports various types of network topology (e.g., Ring, Tree, Mesh, Cube, etc.) for multiple processing units.

– **Configuration of multiple processing units**: It is required that a physical machine provides configuration of multiple processing units.

7.1.6 Management component requirements

– **Providing running information**: It is recommended that a physical machine provides running information in all components of the physical machine.

NOTE 1 – Examples of running information are CPU temperature, CPU utilization, memory utilization, storage read/write load, fan speed and the traffic load of interconnect network.

– **Automatically power operation**: It is recommended that a physical machine supports automatically managing for power on, power off and restart operations for automatic scheduling according to the load of the physical machine.

– **Monitoring of environment conditions**: It is recommended that a physical machine provides monitoring of environment conditions, such as air temperature, air humidity, etc.

– **Self-checking mechanism**: It is recommended that a physical machine supports self-checking to ensure the stability of the physical machine after power on.

NOTE 2 – Self-checking is a process to verify CPU and memory, to initialize BIOS and to identity booting devices after a physical machine is powered on.

7.2 I/O interface requirements

– **Provide I/O interface to administrator**: A physical machine can optionally provide an I/O interface to administrators for I/O devices such as a monitor, a mouse and a keyboard.

NOTE 1 – Examples of I/O interface to administrators are a video graphics array (VGA) and a universal serial bus (USB).

– **Provide I/O interface to external storage device**: A physical machine can optionally provide an I/O interface for an external storage device to install the hypervisor, operating system and/or other software applications.

NOTE 2 – Examples of external storage device are CD ROM and USB flash disk.

– **Network interface virtualization**: It is recommended that a physical machine supports network interface virtualization to improve interface utilization.

NOTE 3 – Network interface virtualization is sharing a network interface into multiple virtual network interfaces.

– **Device driver and API supports**: It is required that a physical machine supports device drivers and APIs for I/O interface.

7.3 Operation requirements

– **Processing unit operation**: It is recommended that a physical machine provides operations for processing units, such as power operation, monitoring configuration information of each processing units.

NOTE 1 – The power operation for a processing unit is to control the power status (e.g., power on, power off and restart) of each of the processing units. The monitoring configuration information of processing units is to collect and report the parameters of the processing units (e.g., CPU type, CPU clock speed, memory frequency and storage capacity).

– **Remote management**: It is recommended that a physical machine supports to be managed remotely through network.

NOTE 2 – Examples of remote management of physical machine are power operation, firmware update and log querying for the physical machine remotely.

– **Diagnostic of physical machine**: It is recommended that a physical machine supports diagnostic to analyze before and after a hardware fault as well as firmware and components of physical machine changes.

NOTE 3 – The fault prediction is accomplished by software.

7.4 Scalability requirements

– **Expansion of interconnect network**: It is recommended that a physical machine provides external expansion of the interconnect network among multiple physical machines to meet required computing performance level from a CSU.

– **I/O interface for device extensions**: It is recommended that a physical machine provides an I/O interface for device extensions that can be used to extend high performance network cards, graphics card and so forth.

– **Processing unit replacement**: It is recommended that a physical machine supports substitution with other processing units to allow processing unit upgrade.

– **Adding processing units**: It is recommended that a physical machine supports the addition of more processing units to the physical machine.

– **Adding components of processing units**: It is recommended that a physical machine supports the addition of more components to the processing units, including CPU, memory, storage and I/O device.

– **Adding power supply**: It is recommended that a physical machine supports the addition of more power supply components to the physical machine.

– **Adding cooling component**: It is recommended that a physical machine supports the addition of more cooling components to the physical machine.

7.5 Security requirements

– **No additional ports**: It is recommended that a physical machine does not expose network ports that are not used.

– **Authorized access**: It is recommended that a physical machine supports an authorized access.

7.6 Reliability requirement

– **Support fault location**: It is recommended that a physical machine supports fault location, so that the operator can easily replace the failing components.

– **Hot-plug support**: A physical machine can optionally support hot-plug without damage.

NOTE – Hot-plug is plugging in and out some components of the physical machine while it is running. An example of hot-plug support is hot-plug disk. Hot-plug disk refer to the disks supporting plug in to or plug out from the physical machine without damage while the physical machine is running.

8 Security considerations

Security aspects for consideration within the cloud computing environment are addressed by security challenges for the CSPs as described in [ITU-T X.1601]. In particular, [ITU-T X.1601] analyses security threats and challenges and describes security capabilities that could mitigate these threats and meet the security challenges.

Appendix I

Comparison between functional requirements and other specifications

(This appendix does not form an integral part of this Recommendation.)

I.1 Specifications and other SDOs

I.1.1 Open Compute Project

The Open Compute Project (OCP) is a rapidly growing community of engineers around the world whose mission is to design and enable the delivery of the most efficient server, storage and data centre hardware designs available for scalable computing.

The OCP Server Project provides standardized server system specifications for scale computing. Standardization is key to ensure that the OCP specification pool does not get fragmented by point solutions that plague the industry today. The Server Project collaborates with the other OCP disciplines to ensure broad adoption and achieve optimizations throughout all aspects from validation, to manufacturing, deployments, data centre operations and de-commissioning.

Table I.1 lists OCP related specifications.

Table I.1 – OCP related specifications

Family	Specification	Summary	Published
OpenRack V2	Twin Lakes 1S Server Design Specification V1.00 [b-OCP 1S]	This specification describes the design of the Twin Lakes 1S server based on the Intel Xeon Processor D-2191 System-on-a-Chip (SoC).	2018
	Facebook 2S Server Tioga Pass Specification V1.0 [b-OCP 2S]	This specification describes Facebook dual sockets server Intel Motherboard v4.0 (Project name: Tioga Pass) design and design requirement to integrate Tioga Pass into Open Rack V2.	2018
	Big Basin-JBOG Specification V1.0 [b-OCP JBOG]	This document describes technical specifications for Facebook's Big Basin-JBOG for use in Open Rack V2.	2018
	Inspur Server Project San Jose V1.01 [b-OCP SJ]	This document defines the technical specification for San Jose Motherboard and chassis used in Open Compute Project Open Rack V2.	2017
	Facebook Multi-Node Server Platform: Yosemite V2 Design Specification V1.0 [b-OCP Yose]	This specification describes the design of the Yosemite V2 Platform that hosts four One Socket (1S) servers, or two sets of 1S server/device card pairs.	2017
	Facebook Server Intel Motherboard V4.0 Project Tioga Pass V0.30 [b-OCP TP]	This specification describes Facebook dual sockets server Intel Motherboard v4.0 (Project name: Tioga Pass) design and design requirement to integrate Intel Motherboard v4.0 into Open Rack V2.	2017
	Facebook Server Intel Motherboard V3.1 [b-OCP MB]	This specification describes Intel Motherboard v3.0 design and design requirement to integrate Intel Motherboard v3.0 into Open Rack V11 and Open Rack V2.	2016
	Open Rack- Intel Motherboard Hardware V2.0 [b-OCP IMBH]	This document defines the technical specifications for the Intel motherboard used in Open Compute Project servers.	2016

Table I.1 – OCP related specifications

Family	Specification	Summary	Published
OpenRack v1	Open Rack- AMD Motherboard Hardware V2.0 [b-OCP AMBH]	This document defines the technical specifications for the AMD motherboard used in Open Compute Project servers.	2012
	Facebook server Fan Speed Control Interface Draft V0.1 [b-OCP FSCI]	This document describes Facebook's FSC algorithm and its update methodology. Using the OpenIPMI fan speed control (FSC) is an intelligent method for controlling server fans to provide adequate cooling while managing thermal constraints and power efficiency. This document will help to manage FSC settings and FSC updates by using intelligent platform management interface (IPMI) commands to vary the fan control profile on either local or remote systems.	2017
Olympus	Project Olympus AMD EPYC Processor Motherboard Specification [b-OCP OAPM]	This specification describes the Project Olympus AMD Server Motherboard. This is an implementation specific specification under the Project Olympus Universal Motherboard Specification.	2017
	Project Olympus Cavium ThunderX2 ARMx64 Motherboard Specification [b-OCP OCTAM]	This specification focuses on the Project Olympus Cavium ThunderX2 ARMx64 Motherboard. This is an implementation specific specification under the Project Olympus Universal Motherboard Specification.	2017
	Project Olympus 1U Server Mechanical Specification [b-OCP O1USM]	This specification focuses on the Project Olympus full-width server mechanical assembly. It covers the mechanical features and supported components of the server, as well as the interfaces with the mechanical and power support structure.	2017
	Project Olympus 2U Server Mechanical Specification [b-OCP O2USM]	This specification focuses on the Project Olympus 2U server mechanical assembly. It covers the mechanical features and supported components of the server, as well as the interfaces with the mechanical and power support structure.	2017
	Project Olympus Intel Xeon Scalable Processor BIOS Specification [b-OCP OBIOS]	The System BIOS is an essential platform ingredient which is responsible for platform initialization that must be completed before booting of an operating system. Thus, the BIOS execution phase of the boot process is often referred to as pre-boot phase.	2017
	Project Olympus Intel Xeon Scalable Processor Motherboard Specification [b-OCP OMB]	This specification describes the Project Olympus Intel Server Motherboard. This is an implementation specific specification under the Project Olympus Universal Motherboard Specification.	2017
OCS	Open CloudServer OCS Programmable Server Adapter Mezzanine Programmables V1.0 [b-OCP OCSPSAM]	This document defines physical and interface requirements for the programmable NIC mezzanine card that can be installed on an Open Cloud Server (OCS) server blade. This server adapter is programmable and provides CPU offload for Host-based SDN, virtual switch data path and tunneling protocols.	2016

Table I.1 – OCP related specifications

Family	Specification	Summary	Published
	Open CloudServer OCS Chassis Manager Specification V2.1 [b-OCP OCSCM]	This specification is an addendum to the OCS Open CloudServer Chassis Management v2.0 specification. It defines the requirements for the upgrade to the Chassis Manager v1.0 made necessary by end of production of the CPU.	2016
	Open CloudServer OCS Blade Specification V2.1 [b-OCP OCSB]	This document is intended for designers and engineers who will be building blades for an OCS system.	2016
	Open CloudServer OCS Solid State Drive V2.1 [b-OCP OCSSSD]	This specification, Open CloudServer Solid State Drive, OCS SSD, describes the low-cost, high-performance flash-based storage devices deployed first in the Open CloudServer OCS Blade V2 specification. The OCS Blade V2 supports four PCI-Express riser cards and eight Open CloudServer Solid State Drive M.2 modules. The Table 1 briefly describes the required features.	2015
	Open CloudServer OCS Power Supply V2.0 [b-OCP OCSPS]	This specification, Open CloudServer Chassis Power Supply Version 2.0, describes the power supply family requirements for the Windows Cloud Server system. The mechanical interface and electrical interface is identical between power supply options to enable a common slot, universal, modular foundation power supply system to enable the Microsoft Windows Cloud Server systems.	2015
	Open CloudServer SAS Mezzanine I/O specification V1.0 [b-OCP OCSSAS]	This document outlines specifications for the Open CloudServer Storage Attached SCSI (SAS) mezzanine card.	2015
	Open CloudServer JBOD specification V1.0 [b-OCP OCSJBOD]	This document provides the technical specifications for the design of the 6G half-width JBOD blade for the Open CloudServer system.	2015
	Open CloudServer OCS Tray Mezzanine Specification V2.0 [b-OCP OCSTRAY]	This specification, Open CloudServer OCS Tray Mezzanine Version 2.0, describes the physical and interface requirements for the Open CloudServer (OCS) tray mezzanine card. The mezzanine card will be installed on the tray backplane and will have a Peripheral Component Interconnect Express (PCIe) x16 Gen3 interface. This interface can either be used as one x16, two x8, or four x4 channels.	2015
	Open CloudServer Chassis Specification V2.0 [b-OCP OCSC]	Describes the hardware used in the Version 2.0 (V2.0) OCS system, including the chassis, tray and systems management.	2015
	Open CloudServer OCS NIC Mezzanine Specification V2.0 [b-OCP OCSNIC]	This specification, Open CloudServer NIC Mezzanine Version 2.0, describes the physical and interface requirements for the Open CloudServer (OCS) NIC mezzanine card that to be installed on an OCS blade.	2014

Table I.1 – OCP related specifications

Family	Specification	Summary	Published
OCP Mezzanine	Mezzanine Card 2.0 Design Specification V1.0 [b-OCP MEZZ]	Mezzanine card 2.0 specification is developed based on original OCP Mezzanine card. It extends the card mechanical and electrical interface to enable new uses cases for Facebook and other users in OCP community. The extension takes backward compatibility to existing OCP platforms designed for original OCP Mezzanine card specification V0.5 into consideration and some tradeoffs are made between backward compatibility and new requirements.	2016
	Mezzanine Card for Intel v2.0 Motherboard [b-OCP MEZZMB]	This document describes the mezzanine card design for use with Open Compute Project Intel v2.0 motherboards. The mezzanine card is installed on an Intel v2.0 OCP motherboard to provide extended functionality, such as support for 10GbE PCI-E devices.	2012
19" Server	QCT Big Sur Product Architecture Following Big Sur Specification V1.0 [b-OCP BS]	The QCT Big Suris 4OU/21 "chassis which using IA-64 based dual-socket servers that support the Grantley–EP processors in combination with the Wellsburg PCH to provide a balanced feature set between technology leadership and cost. QCT Grantley platform will be 16DIMMsand supports 8 GPGPU cards and Max. 8x2.5" HDDs.	2017
	Hyve Solutions Ambient Series-E V1.2 [b-OCP HSAS]	This document defines the technical specifications for the Hyve Solutions Ambient Series-E server, including motherboard, chassis and power supply.	2017
	QuantaGrid D51B-1U V1.1 [b-OCP QGD]	The Quanta Grid D51B-1Uwill be IA-64 based dual-socket servers that support the Grantley–EP processors in combination with the Wellsburg PCH (PCH) to provide a balanced feature set between technology leadership and cost.	2015
	Decathlete Server Board Standard V2.1 [b-OCP DSBS]	This standard provides board-specific information detailing the features and functionality of a general purpose 2-socket server board for adoption by the Open Compute Project community. The purpose of this document is to define a dual socket server board that is capable of deployment in scale out data centres as well as traditional data centres with 19” rack enclosures.	2013
SOC Boards	Panther+ Micro-Server Card Hardware V0.8 [b-OCP PMSCH]	This document describes the technical specifications used in the design of an Intel Avoton SoC based Micro-Server card for Open Compute Project, known as the Panther+.	2016
	Micro-Server Card Hardware V1.0 [b-OCP HSCH]	This specification provides a common form factor for emerging micro-server and SOC (System-On-Chip) server designs.	2016

Table I.1 – OCP related specifications

Family	Specification	Summary	Published
Barreleye	Barreleye G2 Specification [b-OCP G2]	This document describes the specifications for: Zaius POWER9 motherboard, Barreleye G2 server – 2OU, Zaius server – 1.5OU	2017
	Barreleye G1 Specification [b-OCP G1]	This document describes the specification of Barreleye, an OpenPOWER-based Open Compute server, with a mechanical and electrical package designed for Open Rack.	2016
	Facebook, Microsoft, M.2 Carrier Card Design Specification V1.0 [b-OCP M2]	This specification provides the requirements for a PCIe Full Height Half Length (FHHL) form factor card that supports up to four M.2 form factor solid-state drives (SSDs). The card shall support 110mm (Type 22110) or 80mm (Type 22080) dual sided M.2 modules.	2018
	Facebook PCIe Retimer Card V1.1 [b-OCP PCIRC]	This specification describes the design and design requirements for a PCIe add-in card that converts an internal PCIe connection to an external PCIe connection.	2017
	Add-on-Card Thermal Interface Spec for Intel Motherboard V3.0 [b-OCP ACTI]	The goal of this document is to define a standard interface for Facebook Intel motherboard V3.0 to poll thermal data from an add-on-card including Mezzanine card.	2017
Debug Card	OCP debug card with LCD spec V1.0 [b-OCP Debug]	The specification defines the OCP Debug Card with LCD for a server system debug.	2018
Mezz Card	25G Dual Port OCP 2.0 NIC Mezzanine Card V1.0 [b-OCP 25GDual]	This document specifies a technical design implementation to define 25G Ethernet card which meets the requirements of OCP Mezzanine card 2.0 type-A design and the heat sink design could let this card to be able to deployment in OCP server or standard server.	2018
	OCP NIC 3.0 Design Specification V0.8 [b-OCP NIC]	The OCP NIC 3.0 specification is a follow-on to the OCP Mezz 2.0 rev 1.00 design specification. The OCP NIC 3.0 specification supports two basic card sizes: Small Card and Large Card. The Small Card allows for up to 16 PCIe lanes on the card edge while the Large Card supports up to 32 PCIe lanes.	2018

I.1.2 DMTF

The Distributed Management Task Force (DMTF) is an industry standards organization working to simplify the manageability of network-accessible technologies through open and collaborative efforts by leading technology companies. DMTF creates and drives the international adoption of interoperable management standards, supporting implementations that enable the management of diverse traditional and emerging technologies including cloud, virtualization, network and infrastructure.

DMTF has developed specifications related to management interface, which are related to the management of physical machines.

Table I.2 – DMTF related specifications

Specification	Summary	Published
Redfish Scalable Platforms Management API Specification [b-DMTF RFAPI]	This specification is to define the protocols, data model and behaviors, as well as other architectural components needed for an interoperable, cross-vendor, remote and out-of-band capable interface that meets the expectations of Cloud and web-based IT professionals for scalable platform management. While large scale systems are the primary focus, the specifications are also capable of being used for more traditional system platform management implementations.	2018-08-23
Redfish Host Interface Specification [b-DMTF RFHI]	This specification defines functional requirements for Redfish Host Interfaces. In the context of this document, the term "Host Interface" refers to interfaces that can be used by software running on a computer system to access the Redfish Service that is used to manage that computer system.	2017-12-11
Redfish Interoperability Profiles [b-DMTF RFP]	The Redfish Interoperability Profile is a JSON document that contains Schema-level, Property-level and Registry-level requirements. At the property level, these requirements can include a variety of conditions under which the requirement applies.	2018-05-15

I.1.3 SNIA

The Storage Networking Industry Association (SNIA) is a non-profit organization made up of member companies spanning information technology. A globally recognized and trusted authority, SNIA's mission is to lead the storage industry in developing and promoting vendor-neutral architectures, standards and educational services that facilitate the efficient management, movement and security of information.

Table I.3 – SNIA related specifications

Specification	Summary	Published
SNIA Swordfish Specification V1.0.6 [b-SNIA SF]	The Swordfish Scalable Storage Management API ("Swordfish") defines a RESTful interface and a standardized data model to provide a scalable, customer-centric interface for managing storage and related data services. It extends the Redfish Scalable Platforms Management API Specification (DSP0266) from the DMTF.	2018-05-25

I.1.4 ETSI

The European Telecommunications Standards Institute (ETSI) is the recognized regional standards body – European Standards Organization (ESO) – dealing with telecommunications, broadcasting and other electronic communications networks and services.

The ETSI NFV EVE Working Group seeks to develop the necessary requirements to enable a common set of hardware elements and physical environments (e.g., data centres) that can be used to support network function virtualization (NFV) services [b-ETSI EVE007].

Table I.4 – ETSI related specifications

Specification	Summary	Published
Hardware Interoperability Requirements Specification [b-ETSI EVE007]	The document develops a set of normative interoperability requirements for the NFV hardware ecosystem and telecommunications physical environment to support NFV deployment.	2017-03

I.2 Relationship with related specifications from other SDOs

Table I.5 analyses the relationship between functional requirement introduced in this Recommendation and the related Specification from other SDOs. The major differences between this Recommendation and other related Specifications are as follows:

– 'Monitoring environment condition' (see clause 7.1.6) and 'No additional ports' (see clause 7.5) are not addressed in the specifications identified in I.1

– This Recommendation introduced the physical machine with functional requirements derived by use cases with general purpose; other deliverables from other SDOs are specific for server implementation or interface in detail.

Table I.5 – Relationship with related specifications from other SDOs

NO.	Requirements in this Recommendation	Relationship with related specifications from other SDOs
1	**Virtualization instruction set**	– [b-OCP 1S] provides virtualization instruction set as 'The Twin Lakes 1S server is designed to use Intel Xeon Processor D-2191 utilizing the performance and advanced Intelligence of Intel Xeon processors packaged into a dense, lowpower SoC' in clause 3. – [b-OCP BS] provides virtualization instruction set as 'Intel Xeon Haswell/Broadwell-EP' in clause 2 table 2-1. – [b-OCP HSAS] provides virtualization instruction set as 'The motherboard is designed to support dual Intel Xeon E5-2600 v3 and v4 series processors and up to 2048GB LRDIMM 3DS/1024GB LRDIMM/ 512GB RDIMM DDR4 memory. Leveraging advanced technology from Intel, the motherboard is capable of offering scalable 32- and 64- bit computing, high-bandwidth memory design and lightning-fast PCI-E bus implementation' in clause 7. – [b- OCP IMBH] provides virtualization instruction set as 'The Efficiency Performance motherboard, built with the Intel Xeon E5-2600 processor, was originally was code-named the Sandy Bridge-EP motherboard' in clause 4. – [b-OCP OAPM] provides virtualization instruction set as 'CPU: AMD EPYC processors' in clause 5. – [b-OCP MB] provides virtualization instruction set as 'Intel Motherboard V3.1 (also referred to "motherboard" or "the motherboard" in this document, unless noted otherwise) is based on Intel Xeon Processor E5-2600 v3 (formerly code-named Haswell-EP processor) product family CPU architecture' in clause 4.1

Table I.5 – Relationship with related specifications from other SDOs

NO.	Requirements in this Recommendation	Relationship with related specifications from other SDOs
2	**CPU replacement**	– [b-OCP 2S] provides CPU replacement as 'The motherboard supports all Intel Xeon Scalable processor family (aka Skylake-SP) processors with TDP up to 165W. The motherboard shall provision the support of all future CPUs in Intel Xeon Scalable processor Family Platform and the Next gen Intel Xeon Scalable processor Family Platform unless noted otherwise' in clause 5.3.1. – [b-OCP HSAS] provides CPU replacement as 'The motherboard is designed to support dual Intel Xeon E5-2600 v3 and v4 series processors and up to 2048GB LRDIMM 3DS/1024GB LRDIMM/ 512GB RDIMM DDR4 memory. Leveraging advanced technology from Intel, the motherboard is capable of offering scalable 32- and 64-bit computing, high-bandwidth memory design and lightning-fast PCI-E bus implementation' in clause 7. – [b-OCP MB] provides CPU replacement as 'The motherboard uses Intel Xeon E5-2600 v3 (LGA2011-3) Product Family processors with TDP up to 145W. The features listed below must be supported by the motherboard: Support two Intel Xeon E5-2600 v3 (LGA2011-3) Product Family processors up to 145W TDP and vendors should engage with Intel to ensure the design ready for future processors; Two full-width Intel QPI links up to 9.6 GT/s/direction; Up to 18 cores per CPU (up to 36 threads with Hyper-Threading Technology). Up to 45MB last level cache; Single Processor mode is supported' in clause 5.3.1.
3	**Multiple CPUs**	– [b-OCP 2S] provides multiple CPUs as 'Support two Intel XeonScalable processor family (aka Skylake-SP) processors up to 165W TDP and vendors should engage with Intel to ensure the design ready for future processors' in clause 5.3.1. – [b- OCP AMBH] provides multiple CPUs as 'The motherboard supports two AMD G34 Magny Cours or Interlagos CPUs with a TDP (thermal design power) of 115W' in clause 4.3. – [b- OCP DSBS] provides multiple CPUs as 'Support up to two processors with a thermal design point (TDP) of up to 135 W' in clause 4. – [b- OCP DSBS] provides multiple CPUs as 'Support up to two processors using LGA2011-3 (socket type R3) and VRD 12.5 and a thermal design point (TDP) of up to 145W' in clause 4. – [b-OCP HSAS] provides multiple CPUs as 'The motherboard is designed to support dual Intel Xeon E5-2600 v3 and v4 series processors and up to 2048GB LRDIMM 3DS/1024GB LRDIMM/ 512GB RDIMM DDR4 memory. Leveraging advanced technology from Intel, the motherboard is capable of offering scalable 32- and 64- bit computing, high-bandwidth memory design and lightning-fast PCI-E bus implementation' in clause 7. – [b-OCP IMBH] provides multiple CPUs as '2 Intel Xeon E5-2600 (LGA2011) series processors up to 115W' in clause 4.3. – [b-OCP OAPM] provides multiple CPUs as 'Sockets: Dual socket operation' in clause 5. – [b-OCP MB] provides multiple CPUs as 'The motherboard uses Intel Xeon E5-2600 v3 (LGA2011-3) Product Family processors with TDP up to 145W. The features listed below must be supported by the motherboard: Support two Intel Xeon E5-2600 v3 (LGA2011-3) Product Family processors up to 145W TDP and vendors should engage with Intel to ensure the design ready for future processors; Two full-width Intel QPI links up to 9.6 GT/s/direction; Up to 18 cores per CPU (up to 36 threads with Hyper-Threading Technology). Up to 45MB last level cache; Single Processor mode is supported' in clause 5.3.1.

Table I.5 – Relationship with related specifications from other SDOs

NO.	Requirements in this Recommendation	Relationship with related specifications from other SDOs
4	**Low power consumption of CPU**	– [b-OCP 2S] provides Low power consumption of CPU as 'Tuning CPU/Chipset settings to reach minimized power consumption and best performance in a data centre environment' in clause 6.3.1. – [b- OCP 2S] provides Low power consumption of CPU as 'The vendor should implement BMC firmware to support platform power monitoring. To enable power limiting for processor, memory and platform, Intel Server Platform Services-NM is required' in clause 9.8. – [b- OCP 2S] provides Low power consumption of CPU as 'CPU VR optimizations shall be implemented to remove cost and increase the efficiency of the power conversion system' in clause 15.3.2. – [b-OCP G1] provides Low power consumption of CPU as 'The motherboard shall be designed to handle a processor with a maximum TDP of 190W CPU' in clause 7.3.1 – [b- OCP DSBS] provides Low power consumption of CPU as 'Support up to two processors with a thermal design point (TDP) of up to 135 W' in clause 4. – [b-OCP AMBH] provides Low power consumption of CPU as 'The CPU VRM is optimized to reduce cost and increase the efficiency of the power conversion system' in clause 9.1.5. – [b- OCP DSBS] provides Low power consumption of CPU as 'Support up to two processors using LGA2011-3 (socket type R3) and VRD 12.5 and a thermal design point (TDP) of up to 145W' in clause 4. – [b-OCP IMBH] provides Low power consumption of CPU as 'The motherboard uses next generation Intel Xeon processor E5-2600 product family CPUs with a TDP (thermal design power) up to 115W' in clause 4.3. – [b-OCP IMBH] provides Low power consumption of CPU as 'Two to monitor temperatures for CPU0 and CPU1, retrieved through the CPU's temperature sensor interface (PECI)' in clause 6.1. – [b-OCP MB] provides Low power consumption of CPU as 'The motherboard uses Intel Xeon E5-2600 v3 (LGA2011-3) Product Family processors with TDP up to 145W. The features listed below must be supported by the motherboard: Support two Intel Xeon E5-2600 v3 (LGA2011-3) Product Family processors up to 145W TDP and vendors should engage with Intel to ensure the design ready for future processors; Two full-width Intel QPI links up to 9.6 GT/s/direction; Up to 18 cores per CPU (up to 36 threads with Hyper-Threading Technology). Up to 45MB last level cache; Single Processor mode is supported' in clause 5.3.1. – [b-OCP MB] provides Low power consumption of CPU as 'The BIOS should be tuned to minimize system power consumption and maximize performance. This includes: Disable any unused devices, such as unused PCI, PCIe ports, USB ports, SATA/SAS ports, clock generator and buffer ports. Tuning CPU/Chipset settings to reach minimized power consumption and best performance in a data centre environment' in clause 6.3.1.

Table I.5 – Relationship with related specifications from other SDOs

NO.	Requirements in this Recommendation	Relationship with related specifications from other SDOs
5	**Hardware-assisted memory virtualization**	– [b-OCP 2S] provides hardware-assisted memory virtualization as 'Setting for the watchdog timer: The default setting for EVT/DVT/PVT is disabled. The default setting for MP is enabled. The timeout value is 15 minutes and reset the system after the timer expires. The watchdog timer is always disabled after POST' in clause 6.3.2. – [b-OCP HSAS] provides hardware-assisted memory virtualization as 'The motherboard is designed to support dual Intel Xeon E5-2600 v3 and v4 series processors and up to 2048GB LRDIMM 3DS/1024GB LRDIMM/ 512GB RDIMM DDR4 memory. Leveraging advanced technology from Intel, the motherboard is capable of offering scalable 32- and 64- bit computing, high-bandwidth memory design and lightning-fast PCI-E bus implementation' in clause 7. – [b-OCP IMBH] provides hardware-assisted memory virtualization as 'The Efficiency Performance motherboard, built with the Intel Xeon E5-2600 processor, was originally was code-named the Sandy Bridge-EP motherboard' in clause 4. – [b-OCP OAPM] provides hardware-assisted memory virtualization as 'AMD EPYC platform' in clause 5. – [b-OCP MB] provides hardware-assisted memory virtualization as 'Intel Motherboard V3.1 (also referred to "motherboard" or "the motherboard" in this document, unless noted otherwise) is based on Intel Xeon Processor E5-2600 v3 (formerly code-named Haswell-EP processor) product family CPU architecture' in clause 4.1.
6	**Memory replacement**	– [b-OCP 2S] provides memory replacement as 'Besides traditional DDR4 DIMM, the motherboard shall support Non-Volatile DIMM (NVDIMM) on all DIMM slots' in clause 5.3.3. – [b-OCP DSBS] provides memory replacement as 'Memory Expansion :16 sockets for un-buffered DDR3 and registered DDR3 DIMMS' and 'Provide 16 sockets for DDR4 DIMMS' in clause 4. – [b-OCP G1] provides memory replacement as '4 DDR3 Memory channels per memory buffer; total 32 DDR3 RDIMMs, 1333 MHz (1DPC), 8/16/32GB' in clause 6.1. – [b-OCP HSAS] provides memory replacement as 'The motherboard is designed to support dual Intel Xeon E5-2600 v3 and v4 series processors and up to 2048GB LRDIMM 3DS/1024GB LRDIMM/ 512GB RDIMM DDR4 memory. Leveraging advanced technology from Intel, the motherboard is capable of offering scalable 32- and 64- bit computing, high-bandwidth memory design and lightning-fast PCI-E bus implementation' in clause 7. – [b-OCP MB] provides memory replacement as 'The motherboard has DIMM subsystem designed as below: DDR4 direct attach memory support on CPU0 and CPU1; 4x channels DDR4 registered memory interface on each CPU; 2x DDR4 slots per channel (total 16 DIMM); Support RDIMM, LRDIMM; Support SR, DR and QR DIMM; Support DDR4 speeds of 1600/1866/2133; Up to maximum 1024 GB with 64GB DIMMs; Follow updated JEDEC DDR4 specification with 288 pin DIMM socket' in clause 5.3.2.

Table I.5 – Relationship with related specifications from other SDOs

NO.	Requirements in this Recommendation	Relationship with related specifications from other SDOs
7	**Memory reliability**	– [b-OCP 2S] provides memory reliability as 'Setting for ECC error threshold: Available settings are 1, 4, 10 and 1000. The default setting is 1 for EVT, DVT and PVT and 1000 for MP. Setting for ECC error event log threshold: Available settings are disabled, 10, 50, 100. The default setting is 10' in clause 6.3.2. – [b-OCP 2S] provides memory reliability as 'Both correctable ECC and uncorrectable ECC errors should be logged into SEL. Each log entry should indicate location of DIMM by CPU socket#, Channel # and slot #. Memory error reporting need to be tested by both XDP injection and reworked ECC DIMM' in clause 9.11.1. – [b-OCP AMBH] provides memory reliability as 'Setting for ECC error threshold, available settings are 1, 4, 10 and 1000' in clause 5.5. – [b-OCP AMBH] provides memory reliability as 'CPU/memory errors: Both correctable ECC and uncorrectable ECC errors should be logged into event log. Error categories include DRAM, HyperTransport Link and L3 Cache' in clause 5.10.1. [b-OCP HSCH] provides memory reliability as 'Memory Correctable ECC: The threshold value is 1000. When the threshold is reached, the BIOS logs the event and includes the physical DIMM location.' in clause 8.5.10. – [b-OCP IMBH] provides memory reliability as 'DDR3 direct attached memory support on cpu0 and cpu1 with: 4 channel DDR3 registered memory interface on processors 0 and 1; 2 DDR3 slots per channel per processor (total of 16 DIMMs on the motherboard); RDIMM/LV-RDIMM (1.5V/1.35V), LRDIMM and ECC UDIMM/LV-UDIMM(1.5V/1.35V); Single, dual and quad rank DIMMs ; DDR3 speeds of 800/1066/1333/1600 MHz; Up to maximum 512 GB memory with 32GB RDIMM DIMMs' in clause 4.3. – [b-OCP IMBH] provides memory reliability as 'CPU/Memory errors: Both correctable ECC and un-correctable ECC errors should be logged into the event log. Error categories include DRAM, Link and L3 cache' in clause 5.9.1. – [b-OCP IMBH] provides memory reliability as 'Memory Correctable ECC: The threshold value is 1000. When the threshold is reached, the BIOS should log the event including DIMM location information and output DIMM location code through the debug card' in clause 5.9.2.
8	**Supporting various types of memory**	– [b-OCP 2S] provides supporting of various types of memory as 'Besides traditional DDR4 DIMM, the motherboard shall support Non-Volatile DIMM (NVDIMM) on all DIMM slots' in clause 5.3.3. – [b-OCP AMBH] provides supporting of various types of memory as 'DDR3 direct attached memory support on cpu0 and cpu1 with: o 4 channels DDR3 registered memory interface on each CPU; 2 DDR3 slots per channel per processor (total of 16 DIMMs on the motherboard); RDIMM/LV-RDIMM (1.35V/1.25V), LRDIMM and UDIMM/LV-UDIMM (1.35V/1.25V); SR, DR and QR DIMMs; DDR3 speeds of 800/1066/1333/1600; Up to maximum 512GB memory with 32GB RDIMMs' in clause 4.3. – [b-OCP HSAS] provides supporting of various types of memory as 'DIMM Type: RDIMM DDR4, LRDIMM 3DS DDR4, LRDIMM DDR4' in clause 8. – [b-OCP IMBH] provides Supporting various types of memory as 'DDR3 direct attached memory support on cpu0 and cpu1 with: 4 channel DDR3 registered memory interface on processors 0 and 1; 2 DDR3 slots per channel per processor (total of 16 DIMMs on the motherboard); RDIMM/LV-RDIMM (1.5V/1.35V), LRDIMM and ECC UDIMM/LV-UDIMM(1.5V/1.35V); Single, dual and quad rank DIMMs ; DDR3 speeds of 800/1066/1333/1600

Table I.5 – Relationship with related specifications from other SDOs

NO.	Requirements in this Recommendation	Relationship with related specifications from other SDOs
		MHz; Up to maximum 512 GB memory with 32GB RDIMM DIMMs' in clause 4.3. – [b-OCP OAPM] provides supporting of various types of memory as 'DIMM Type Double data rate fourth generation (DDR4) Registered DIMM (RDIMM) with Error-Correcting Code (ECC)' in clause 5. – [b-OCP MB] provides supporting of various types of memory as 'The motherboard has DIMM subsystem designed as below: DDR4 direct attach memory support on CPU0 and CPU1; 4x channels DDR4 registered memory interface on each CPU; 2x DDR4 slots per channel (total 16 DIMM); Support RDIMM, LRDIMM; Support SR, DR and QR DIMM; Support DDR4 speeds of 1600/1866/2133; Up to maximum 1024 GB with 64GB DIMMs; Follow updated JEDEC DDR4 specification with 288 pin DIMM socket' in clause 5.3.2.
9	**Multiple interfaces for storage**	– [b-OCP 1S] provides multiple interfaces for storage as 'The Twin Lakes 1S server implements primary and extension x16 PCIe edge connectors as defined in the 1S server specification. The primary x16 PCIe edge connector supports: • PCIe Gen3 ports • A 10GBase-KR • A SATA port • A USB 2.0 port • A Universal Asynchronous Receiver/Transmitter (UART)' in clause 3. – [b-OCP 1S] provides multiple interfaces for storage as 'The Twin Lakes 1S server supports three on-card Solid State Drives (SSDs) in the 2280 or 22110 M.2 form factor' in clause 3. – [b-OCP 1S] provides multiple interfaces for storage as 'The Twin Lakes 1S server supports three M.2 solid-state drives in 2280 or 22110 form factors. Boot M.2 slot is only available in 2280 form factor and it can be configured as either SATA or PCIe interface through BOM options, but not both. A minimum 256GB M.2 SATA or NVMe SSD is required as a boot device and for logging purpose. Two additional SSD drives are designed in to support applications that require high disk performance. These two M.2 slots only support PCIe X4 links but both support SSD drives in 2280 or 22110 form factors' in clause 9.4. – [b-OCP 2S] provides multiple interfaces for storage as 'Following internal connectors should be placed as close as possible to front of the board in order to have easy front access: 1x vertical combo SATA signal and power connector; 1x 14-pin Debug card header; 1X right angle USB3 Type A connector; 1X SMD switch to enable/disable Intel Intel At Scale Debug; 1x M.2 connector with 2280 and 22110 support; 1x RJ45; 1x USB type C; 1X customized VGA connector' in clause 5.2. – [b-OCP 2S] provides multiple interfaces for storage as 'The motherboard uses Intel PCH chipset, which supports following features: 4x USB 3.0/2.0 ports: one type A for front connector; one type C for front connector; one for BMC in-band firmware update; one to X32 riser connector; 1x M.2 connector; 1x individual SATA 6Gps port; 1x miniSAS HD x8 port or 1x miniSAS HD x4 port; 1x PCIe x4 ports to M.2 connector, colayout with SATA port to M.2 connector; SPI interface, mux with BMC to enable BMC the capability to perform BIOS upgrade and recovery; SPI interface for TPM header' in clause 5.4. – [b-OCP 2S] provides multiple interfaces for storage as 'The motherboard has Intel PCH on board. Intel PCH has a SATA controller support 8x SATA3 ports and an sSATA controller support 6x SATA3 ports' in clause 11.6. – [b-OCP AMBH] provides multiple interfaces for storage as 'PCI-E x16 Slot/Riser Card; PCI-E Mezzanine Card; PCI-E External Connector; SATA' in clauses 10.1,10.2,10.3, 10.7.

Table I.5 – Relationship with related specifications from other SDOs

NO.	Requirements in this Recommendation	Relationship with related specifications from other SDOs
		– [b-OCP BS] provides multiple interfaces for storage as 'PCIe Expansion Slot; SATA hot-plug drives' in clause 2, Table 2-1. – [b-OCP DSBS] provides multiple interfaces for storage as 'Storage: Two single port AHCI SATA connectors capable of supporting up to 6 Gb/sec; Two SCU 4-port mini-SAS connectors capable of supporting up to 3 Gb/sec SATA/SAS; Two 4-port mini HD connectors capable of supporting up to 6 Gb/sec SATA' and 'Support for PCI Express* 225W/300W High Power Card Electromechanical Specification 1.0' in clause 4, Tables 1 and 2. – [b-OCP G1] provides multiple interfaces for storage as '15x 12Gb/s SAS or 6Gb/s SATA 2.5' drive slots, up to 15mm thickness, connected via SEB, to an onboard HBA. One M.2 SATA slot, also on board.' and '1 x 16 Gen3 FH/FL, 2 x8 Gen3 LP/HL, 1 x8 OCP Mez with front Panel access, 1 x8 PCIe OCP Mez in a non-front-accessible internal slot to support SAS HBA or Raid-on-Chip with SuperCap' in clause 6.1. – [b-OCP HSAS] provides multiple interfaces for storage as '▪ Intel C612 Controller;▪ (2) discrete SATA 7pin for SATA4 and SATA5;▪ (2) MiniSAS SFF-8087 for SATA0~SATA3, sSATA0~sSATA3;▪ 6.0Gb/s speed;▪ SATA SGPIO supported;▪ RAID 0/1/10/5 (Intel RST);▪ (4) Internal MiniSASHD SFF-8643 connectors (Optional)' in clause 8. – [b- OCP HSCH] provides multiple interfaces for storage as 'The SATA connections are a minimum of SATA2.0 (3Gb/s) and may be SATA3.0 (6Gb/s).The PCIe connection is a minimum of PCIe 2.0 and may be PCIe 3.0' in clauses 6.4 and 6.5. – [b-OCP OAPM] provides multiple interfaces for storage as 'SATA, and PCI-Express Expansion' in clause 5. – [b-OCP MB] provides multiple interfaces for storage as 'The motherboard uses Intel C610 series chipset, which supports following features: 3x USB 3.0/2.0 ports: one for front connector; one for optional vertical on board connector; one for BMC in-band firmware update; 1x mSATA connector from SATA port 4 co-layout with M.2 connector; 1x individual SATA 6Gps ports from SATA port 5; 1x miniSAS port from SATA port 0/1/2/3, 1x miniSAS port from sSATA0/1/2/3; 1x PCIe x4 ports to M.2 connector; SPI interface, connect to BMC to enable BMC the capability to perform BIOS upgrade and recovery; SMBUS interface (master and slave); Intel Server Platform Services (SPS) 3.0 Firmware with Intel Node Manager' in clause 5.4.
10	**Storage replacement**	– [b-OCP 1S] provides storage replacement as 'The carrier assembly includes 2x ejectors which are used for card injection/ejection into the PCIe connectors' in clause 5.1. – [b-OCP 1S] provides storage replacement as 'The Twin Lakes 1S server supports three M.2 solid-state drives in 2280 or 22110 form factors. Boot M.2 slot is only available in 2280 form factor and it can be configured as either SATA or PCIe interface through BOM options, but not both. A minimum 256GB M.2 SATA or NVMe SSD is required as a boot device and for logging purpose. Two additional SSD drives are designed in to support applications that require high disk performance. These two M.2 slots only support PCIe X4 links but both support SSD drives in 2280 or 22110 form factors' in clause 9.4. – [b-OCP 2S] provides storage replacement as 'The motherboard uses Intel PCH chipset, which supports following features: 4x USB 3.0/2.0 ports: one type A for front connector; one type C for front connector; one for BMC in-band firmware update; one to X32 riser connector; 1x M.2 connector; 1x individual SATA 6Gps port; 1x miniSAS HD x8 port or 1x miniSAS HD x4 port;

Table I.5 – Relationship with related specifications from other SDOs

NO.	Requirements in this Recommendation	Relationship with related specifications from other SDOs
		1x PCIe x4 ports to M.2 connector, colayout with SATA port to M.2 connector; SPI interface, mux with BMC to enable BMC the capability to perform BIOS upgrade and recovery; SPI interface for TPM header' in clause 5.4. – [b-OCP AMBH] provides storage replacement as 'PCI-E x16 Slot/Riser Card; PCI-E Mezzanine Card; PCI-E External Connector; SATA' in clauses 10.1,10.2,10.3 and 10.7. – [b-OCP BS] provides storage replacement as 'PCIe Expansion Slot; SATA hot-plug drives' in clause 2, Table 2-1. – [b-OCP DSBS] provides storage replacement as 'Storage: Two single port AHCI SATA connectors capable of supporting up to 6 Gb/sec; Two SCU 4-port mini-SAS connectors capable of supporting up to 3 Gb/sec SATA/SAS; Two 4-port mini HD connectors capable of supporting up to 6 Gb/sec SATA' and 'Support for PCI Express* 225W/300W High Power Card Electromechanical Specification 1.0' in clause 4, Tables 1 and 2. – [b-OCP HSAS] provides storage replacement as '▪ Intel C612 Controller;▪ (2) discrete SATA 7pin for SATA4 and SATA5;▪ (2) MiniSAS SFF-8087 for SATA0~SATA3, sSATA0~sSATA3;▪ 6.0Gb/s speed;▪ SATA SGPIO supported;▪ RAID 0/1/10/5 (Intel RST);▪ (4) Internal MiniSASHD SFF-8643 connectors (Optional)' in clause 8. – [b-OCP HSCH] provides storage replacement as 'The BIOS is tuned to minimize card power consumption. It has the following features: • Unused devices are disabled including PCIe* lanes, USB ports, SATA/SAS ports, etc;• BIOS setup menu;• SOC settings are provided to allow tuning to achieve the optimal combination of performance and power consumption' in clause 8.5.2. – [b-OCP MB] provides storage replacement as 'The motherboard uses Intel C610 series chipset, which supports following features: 3x USB 3.0/2.0 ports: one for front connector; one for optional vertical onboard connector; one for BMC in-band firmware update; 1x mSATA connector from SATA port 4 co-layout with M.2 connector; 1x individual SATA 6Gps ports from SATA port 5; 1x miniSAS port from SATA port 0/1/2/3, 1x miniSAS port from sSATA0/1/2/3; 1x PCIe x4 ports to M.2 connector; SPI interface, connect to BMC to enable BMC the capability to perform BIOS upgrade and recovery; SMBUS interface (master and slave); Intel Server Platform Services (SPS) 3.0 Firmware with Intel Node Manager' in clause 5.4.
11	**Storage redundancy hardware**	– [b-OCP HSAS] provides storage redundancy hardware as 'Storage: RAID 0/1/10/5 (Intel RST)' in clause 8. – [b-OCP SJ] provides Storage redundancy hardware as 'SATA RAID KEY: 1x4' in clause 6.12.
12	**Storage hibernation**	– [b-OCP 2S] provides storage hibernation as 'Disable any unused devices, such as unused PCI, PCIe ports, USB ports, SATA/SAS ports, clock generator and buffer ports' in clause 6.3.1. – [b-OCP HSCH] provides storage hibernation as 'The BIOS is tuned to minimize card power consumption. It has the following features: • Unused devices are disabled including PCIe* lanes, USB ports, SATA/SAS ports, etc.; • BIOS setup menu; • SOC settings are provided to allow tuning to achieve the optimal combination of performance and power consumption' in clause 8.5.2.

Table I.5 – Relationship with related specifications from other SDOs

NO.	Requirements in this Recommendation	Relationship with related specifications from other SDOs
		– [b-OCP MB] provides storage hibernation as 'The BIOS should be tuned to minimize system power consumption and maximize performance. This includes: Disable any unused devices, such as unused PCI, PCIe ports, USB ports, SATA/SAS ports, clock generator and buffer ports. Tuning CPU/Chipset settings to reach minimized power consumption and best performance in a data centre environment' in clause 6.3.1.
13	**Hardware-assisted I/O virtualization**	– [b-OCP OBIOS] describes how Intel Virtualization Technology (Intel VT) must be supported via platform BIOS policy variable, in clause 4.8.
14	**I/O devices direct accessing**	– [b-OCP 25GDual] describes how QL41202 shall support single root I/O virtualization (SR-IOV), in clause 12.
15	**Workload offload**	– [b-OCP 25GDual] describes how QL41202 shall support offload traffic types RDMA over Converged Ethernet (RoCE) on each of the ports and also support Internet wide area RDMA protocol (iWARP), in clause 12.
16	**Hardware acceleration**	– [b-OCP OBIOS] describes key features for WCS Intel Xeon Scalable Platform, support 2 GP-GPU+1 PCIe card in 2U, in clause 2.2. – [b-OCP BS] describes QCT Grantley platform will be 16 DIMMs and support 8 GPGPU cards and Max. 8x 2.5"HDDs' in clause 1.
17	**Power supply replacement**	– [b-OCP OCSSSD] describes how OCS v2.0 servers shall support drives with volatile write caches by leveraging the server backup power supply in clause 11.3 Power-Loss Protection. – [b-OCP OCTAM] Indicates that when PSU ALERT# signal occurs, the Olympus PSU has transitioned its power source from AC to battery backup, in clause 7.4.
18	**Supporting power redundancy**	– [b-ETSI EVE007] provide power redundancy as 'Power supply redundancy may be achieved by installing more than one power supply unit' in clause 5.3.3.2. – [b-OCP 1S] require platform designers to provide adequate power and cooling to properly handle the SoC's power and thermal requirements, in clause 3 overview. – [b-OCP 1S] require Twin Lakes 1S Server to provide a standby 3.3V_AUX power rail on the card to power the Bridge IC at all power states, in clause 8.1.2. – [b-OCP HSAS] describe that the Hyve Solutions Ambient Series-E servers support single or redundant power supply, in clause 11.
19	**Minimum energy consumption**	– [b-ETSI EVE007] provides minimum energy consumption as 'different forms of processors would be utilized for different types of services to improve power efficiency' in clause 5.2. – [b-OCP 1S] describes that the Twin Lakes 1S server recommend a power-capping implementation to reduce the server's power consumption (cut off power in certain time) in clause 8.4. – [b-OCP OAPM] describe that the motherboard supports Emergency Power Reduction mechanism (PWRBRK#) for the x16 PCIe slots in clause 7.5. – [b-OCP OCTAM] describes how the motherboard supports Emergency Power Reduction mechanism (PWRBRK#) for the x16 and x32 PCIe slots in clause 7.5. – [b-OCP OMB] describes how the motherboard supports Emergency Power Reduction mechanism (PWRBRK#) for the x16 PCIe slots in clause 6.5, the main purpose is to provide a power reduction mechanism for GPGPU cards as part of the throttle and power capping strategy.

Table I.5 – Relationship with related specifications from other SDOs

NO.	Requirements in this Recommendation	Relationship with related specifications from other SDOs
		– [b-OCP HSCH] describes how the BIOS is tuned to minimize card power consumption. It has the following features: • Unused devices are disabled including PCIe* lanes, USB ports, SATA/SAS ports, etc.; • BIOS setup menu; • SOC settings are provided to allow tuning to achieve the optimal combination of performance and power consumption' in clause 8.5.2. – [b-OCP HSCH] describes how each card must provide temperature sensors for the SOC, the SO-DIMM(s) (if they are used) and one ambient temperature sensor. All temperature readings for each sensor must be readable via the management sideband interface to the baseboard. Additionally, over-temperature thresholds are configurable and an alert mechanism is provided to enable thermal shutdown and/or an increase in airflow. The sensors are accurate to +/−3C' in clause 5.4.
20	**Interface for monitoring power**	– [b-ETSI EVE007] provides interface for monitoring power as 'Each power supply unit should be capable of measuring and remotely reporting the following operational parameters' in clause 5.3.4.2. – [b-OCP 1S] describes how the Twin Lakes 1S server shall uses power sensor to measure Card and SoC power consumption. The power data can be used by the platform for power management purposes. The Twin Lakes 1S server supports an Advanced Configuration Power Interface (ACPI)-compliant power button and reset signals from the platform, in clause 3 overview and clause 6.5. – [b-OCP AMBH] describes how to use BMC to monitor power in clause 7.2 and use PMBUS interface to enable the BMC to report server input power in clause 8.6. – [b-OCP DSBS] describes how Decathlete Server Board shall support power supply redundancy monitoring and support in clause 8.1.2. – [b-OCP TP] requires vendors to implement BMC firmware to support remote system power on/off/cycle and warm reboot through In-Band or Out-of-Band IPMI commands in clause 8.4 and support platform power monitoring in clause 8.8.
21	**Cooling component replacement**	– [b-OCP 2S] describes that if and only if one rotor in server fan fails, the negative or positive DC pressurization can be considered in the thermal solution in the hot aisle or in cold aisle respectively in clause 10.2.4.
22	**Cooling component redundancy**	– [b-OCP 2S] provides a description of fan redundancy which is one implementation of cooling redundancy – as 'the server fans at N+1 redundancy should be sufficient for cooling server components to temperatures below their maximum spec to prevent server shut down or to prevent either CPU or memory throttling' in clause 10.2.5. – [b-OCP O1USM] requires fans to be N+2 redundant to optimize fan efficiency and server availability while eliminating the need for hot swap capability in clause 4.4. – [b-OCP O2USM] requires fans to be N+2 redundant to optimize fan efficiency and server availability while eliminating the need for hot swap capability in clause 4.4. – [b-OCP TP] describe how server fans should be N+1 redundancy to be sufficient for cooling server components to temperatures below their maximum spec to prevent server shut down or to prevent either CPU or memory throttling in clause 9.2.5. [b-ETSI EVE007] provides Cooling component redundancy as 'Redundancy within the rack cooling system shall provide appropriate levels of cooling to all the rack equipment while the rack cooling system is serviced' in clause 5.5.3.

Table I.5 – Relationship with related specifications from other SDOs

NO.	Requirements in this Recommendation	Relationship with related specifications from other SDOs
23	**Interface for controlling fan speed**	– [b-OCP 2S] requires vendors to enable fan speed control (FSC) on BMC. The FSC algorithm processes sensor data and drives two PWM outputs to optimized speed, in clause 9.12. – [b-OCP AMBH] requires ODM to provide system access interface to retrieve hardware sensor readings and control fan speed, in clause 6. – [b-OCP DSBS] describes how Decathlete Server Board shall support ACPI to control power and fan speed in clause 8.2. – [b-OCP SFCI] describes how server management controller like BMC use standard IPMI commands to manage SFC in whole document. – [b-OCP OCSPS] describes that the PSU shall adjust internal fan speed based upon internal temperature sensor(s) in clause 4.3. – [b-OCP TP] requires vendors to enable FSC on the BMC in clause 8.12.
24	**Monitoring status of physical machine**	– [b-OCP 1S] provides monitoring status set as 'There is also a blinking amber heartbeat LED on the Twin Lakes 1S server to indicate that the Bridge IC is in operating mode' in clause 9.8. – [b-OCP 2S] provides system state monitor set as 'There are 4 states of Power/system identification LED depending on system power state and chassis identify status' in clause 9.6. – [b-OCP Yose] provides monitor status set as 'On the Adapter Card of a Yosemite V2 sled, there is a power button, a reset button, an OCP debug card and a USB port attached to the current selected 1S server. There are four blue LEDs placed on the baseboard in the same order as 1S server slots to indicate server status' in clause 9.4. – [b-OCP O1USM] provides visual indication set as 'A 3D mechanical drawing of the Front Panel is shown in Figure 2. The Front Panel supports the following mechanical features. Status LEDs o UID, Attention, Power Status' in clause 4.1.
25	**Visual indications**	– [b-OCP JBOG] provides system event log (SEL) set as 'The BMC needs to support SEL capabilities. The following items are to be logged in the SEL' in clause 7.1. – [b-OCP SJ] provides silk screen colour set as 'The colour of silk screen is white and the labels for the components are listed as below' in clause 13.4. – [b-OCP Yose] provides visual feedback set as 'The LED associated with the active 1S server blinks as visual feedback to the user. When a BMC is selected, all four LEDs blink as visual feedback to the user' in clause 9.4.1. – [b-OCP OAPM] provides visual indication set as 'The motherboard supports a blue UID (unit ID) LED used to help visually locate a specific server within a data centre' in clause 6.11.1.
26	**Equipment for mounting and removal**	– [b-OCP 1S] provides easy to remove set as 'The air baffle must be easy to service with the goal of requiring no tooling to remove' in clause 6.6. – [b-OCP 2S] provides removal set as 'It is installed on a sheet metal panel with tool-less install and removal' in clause 12.2.5. – [b-OCP IMBH] provides mounting and removal set as 'In order to remove and install one board without affecting the other board, the following internal connectors are placed as close as possible to front of the board in order to have easy frontal access' in clause 4.2 and "The PCIe* x4 connector can be hot inserted and removed" in clause 10.2.

Table I.5 – Relationship with related specifications from other SDOs

NO.	Requirements in this Recommendation	Relationship with related specifications from other SDOs
27	**Circulation of air flow**	– [b-OCP 1S] provides air flow set as 'The card level air baffle must be designed to help maintain temperatures of all major components on the server card by reducing bypass air and increasing airflow through key components' in clause 6.6. – [b-OCP 2S] provides airflow set as 'The unit of airflow (or volumetric flow) used for this spec is CFM (cubic feet per minute).The maximum allowable airflow per watt in the system must be 0.107' in clause 10.2.26. – [b-OCP JBOG] provides system airflow set as 'The unit of airflow (or volumetric flow) used for this spec is CFM (cubic feet per minute). The maximum allowable airflow per watt in the system must be 0.14 at sea level' in clause 8.2.3. – [b-OCP SJ] provides cooling set as 'To meet thermal reliability requirement, the thermal and cooling solution should dissipate heat from the components when system operating at its maximum thermal power' in clause 11. – [b-OCP Yose] provides airflow set as 'The unit of airflow (or volumetric flow) used for this spec is cubic feet per minute (CFM)' in clause 8.2.5.
28	**Interconnect network supports**	– [b-ETSI EVE007] provide interconnect network supports as 'support links of types other than Ethernet' in clause 5.4.2. – [b-OCP 1S] provides interconnect set as 'When the SoC's integrated network controller is used as a shared NIC, its SMBus is routed to Connector A as the sideband interface' in clause 7.9.1. – [b-OCP 2S] provides interconnect set as 'High speed mid-plane is mid-plane with power delivery, plus high speed interconnect on mid-plane' in clause 12.3. – [b-OCP JBOG] provides interconnect set as 'For JBOG with 8x GPUs in SXM2 form factor, it shall support NVLINK interconnection shown below' in clause 4.3.
29	**Sharing process unit component**	– [b-OCP 2S] provides share SPI bus set as 'A secondary identical BIOS chip is designed in sharing the same SPI bus with multiplexedCS pin' in clause 6.1. – [b-OCP OBIOS] provides share io set as 'ATA controllers running in native mode use their PCI interrupt for both channels and can share this interrupt with other devices in the system, like any other PCI device' in clause 7.3.1.2.
30	**Network topology**	– [b-OCP OCSB] provides topology set as 'CPU-to-tray backplane mezzanine PCIe link topology' in clause 7.1.
31	**Configuration of multiple processing units**	– [b-OCP 1S] provides configuration set as 'Set Bridge IC configuration' in clause 9.7.10, Table 6. – [b-OCP 2S] provides configuration set as 'Vendor should provide utility under CentOS to perform VR configuration change. Configuration change should take effect without AC cycling node' in clause 15.3.4. – [b-OCP OBIOS] provides multi process configuration set as 'The Intel Xeon Scalable processor is implemented with 1 or more cores with each core capable of supporting Intel HT Technology. The result is multiple logical processors in a physical package' in clause 4.13.

Table I.5 – Relationship with related specifications from other SDOs

NO.	Requirements in this Recommendation	Relationship with related specifications from other SDOs
32	**Providing running information**	– [b-OCP 1S] provides temperature and power sensors set as 'Each card must provide following sensors: Temperature sensors for SOC, DIMM, voltage regulators and other critical chips' in clause 6.5. – [b-OCP 2S] provides running monitor set as 'The vendor should implement BMC FW to support thermal monitoring, including processor, memory, chipset, VRs, PCIe card, Mezzanine cards, Inlet/outlet air temperature and airflow sensor' in clause 9.8. – [b-OCP AMBH] provides memory reliability as 'Hardware health monitoring display' in clause 5.5. – [b-OCP JBOG] provides monitor set as 'The BMC implemented is to have access to all analog sensors placed in the system and ensure that they are displayed in a sensor data record repository' in clause 7.9.1.1. – [b-OCP Yose] provides monitor set as 'During the entire hot-service process, the BMC shall monitor the thermal condition closely' in clause 5.2. – [b-OCP AMBH] provides monitor set as 'The BMC can be used to monitor hardware and control fan speed' in clause 6. – [b-OCP OBIOS] provides multi process configuration set as 'BIOS requirements for Intel NM enabled firmware NM5 BIOS should implement processor utilization notifications support in ACPI tables' in clause 9.2.2.
33	**Automatically power operation**	– [b-OCP 1S] provides power operation set as 'The Twin Lakes 1S server can throttle itself down to lowest possible power state as quickly as possible when the platform asserts the FAST_THROTTLE_N signal or it receives request from BMC, or over power event reported by on-card power monitor' in clause 8.4， and 'The BMC controls power on, off and reset directly via the signals defined in the pin-out' in clause 9.7.13. – [b-OCP 2S] provides auto power on set as 'Motherboard should be set to restore last power state during AC on/off. This means that, when AC does on/off cycle, motherboard should power on automatically without requiring power button' in clause 15.9. – [b-OCP JBOG] provides power operation set as 'Support power on policy to be last-state, always-on and always-off upon recovery from an AC power loss event. T' in clause 7.7. – [b-OCP Yose] provides auto power set as 'Now the user can replace the failed unit with a new one, BMC would automatically resume power and boot the new card' in clause 5.2. – [b-OCP OBIOS] provides power controller set as 'The following actions are available on expiration of the Watchdog Timer: • System Reset• System Power Off• System Power Cycle• Pre-timeout Interrupt (OPTIONAL)' in clause 9.2.2.
34	**Monitoring environment condition**	
35	**Self-checking mechanism**	– [b-OCP 2S] provides get selftest result set as 'Get Selftest Results (0x04) in clause 9.13. – [b-OCP TP] provides selftest set as 'During system boot-up, POST (Power-On-SelfTest) codes will be send to port 80 and decoded by the BMC to drive the LED display as described in section 8.5. P' in clause 8.2. – [b-OCP OBIOS] provides selftest set as 'Built-In Self-Test (BIST) The BIST_ENABLE can be controlled by a BMC, GPO, strap or other mechanism. BIOS shall implement a platform policy to control BIST execution' in clause 4.12.

Table I.5 – Relationship with related specifications from other SDOs

NO.	Requirements in this Recommendation	Relationship with related specifications from other SDOs
36	**Provide I/O interface to administrator**	– [b-OCP 1S] provides 'The primary x16 PCIe edge connector supports: USB 2.0 port' in clause 3. – [b-OCP 2S] provides 'support of GUI and KVM on hardware level to accommodate the OCP customers whose environment requires using of VGA and KVM' in clause 9.3. – [b-OCP SJ] provides 'USB and VGA' in clause 4.2. – [b-OCP Yose] provides 'supports a VGA interface' in clause 9.5. – [b-OCP 1S] provides keyboard interface as 'Bridge IC provides ways to transfer messages between them via KCS interfaces. For in-band management, the Bridge IC can forward the SoC's Keyboard Controller Style (KCS) request to the BMC' in clause 9.7.3. – [b-OCP AMBH] provides USB interface as 'The motherboard has two external USB ports located in the front of the motherboard. The BIOS supports the following USB devices: Keyboard and mouse' in clause 10.6. – [b-OCP TP] provides USB interface as 'The motherboard has one external Type-A, right angle USB 2.0/3.0 port and one USB 3.0. Type-C port located in front of the motherboard. The BIOS should support the following USB devices: USB keyboard and mouse' in clause 10.5. – [b-OCP Yose] provides VGA support as 'The Yosemite V2 Platform supports a VGA interface. The original SATA interface on 1S server interface has been repurposed to be a x1 PCIe link' in clause 9.5. – [b-OCP DSBS] provides USB support as 'The server board SHALL provide two external USB ports and the BIOS SHALL support the following USB devices: Keyboard and mouse ,Bootable USB flash drive, Bootable USB hard disk, Bootable USB optical disk' in clause 6.2.
37	**Provide I/O interface to external storage device**	– [b-OCP 1S] provides interface to external storage as 'Boot M.2 slot is only available in 2280 form factor and it can be configured as either SATA or PCIe interface through BOM options' in clause 9.4. – [b-OCP AMBH] provides SATA port as 'The motherboard has SP5100 interfaces on board, which support up to six SATA ports' in clause 10.7. – [b-OCP TP] provides SATA port as 'SATA port 0~7 can be connected to one vertical mini-SAS HD 8 ports connector. sSATA ports 2~5 can be connected to one mini-SAS HD 4 ports connector' in clause 10.6. – [b-OCP O2USM] provides SATA port as 'Supports up to 12 SATA devices' in clause 4. – [b-OCP DSBS] provides SATA port as 'The server board SHALL have support up to six SATA ports' in clause 6.3.
38	**Network interface virtualization**	– [b-OCP 25GDual] provides network virtualization as 'Support receive side scaling (RSS), single root I/O virtualization (SR-IOV), VLAN tagging, Layer 2 priority encoding, link aggregation and full-duplex flow control 802.3 functions in the MAC' in Table 1.
39	**Device driver and API supports**	– [b-ETSI EVE007] provide device driver and API supports as 'the network interface should be configurable to service either a management or production network' in clause 5.6.2. – [b-OCP 1S] provides device driver support as 'The Twin Lakes 1S server supports three M.2 solid-state drives in 2280 or 22110 form factors' in clause 3.

Table I.5 – Relationship with related specifications from other SDOs

NO.	Requirements in this Recommendation	Relationship with related specifications from other SDOs
		– [b-OCP 2S] provides device driver support as 'All data network and management network should have this capability. This includes, but not limit to: DHCP and static IP setting, PXE booting capability, NIC and BMC firmware support, OS driver and utility in both IPv4 and IPv6' in clause 11.4.3. – [b-OCP AMBH] provides device driver support as 'The x4 connector can be hot inserted and removed. A PCI-E re-driver is used for PCI-E external links and supports a miniSAS cable up to 2 meters long' in clause 10.3. – [b-OCP TP] provides device driver support as 'It is recommended that PCB is planned with three vendors at EVT. EVT and DVT build plan should cover all possible combinations of key components of DC-DC VR including output inductor, MOSFETs and driver' in clause 18.9.
40	**Processing unit operation**	– [b-OCP 1S] provides power operation as 'server shall have the power monitoring capability to read power consumption reliably and accurately and can report a one-second average power reading with 3% accuracy' in clause 8.4. – [b-OCP 2S] provides monitoring information as 'BMC should implement thermal monitoring feature for PCIe card on riser and Mezzanine card. BMC reads the temperature of key components of PCIe and Mezzanine cards through its SMBus ports in the format as TMP421 temperature sensor. BMC' in clause 9.18. – [b-OCP AMBH] provides monitoring information as 'The ODM needs to provide a system access interface and application to retrieve hardware monitoring sensor readings, including at minimum, lm_sensors, a Linux application for the CentOS operating system and its driver' in clause 6. – [b-OCP AMBH] provides power operation as 'The motherboard includes a power switch, reset switch, power LED, HDD activity LED and beep error LED' in clause 10.9. – [b-OCP Yose] provides monitoring information as 'The BMC firmware shall support platform power monitoring. The BMC firmware shall support thermal monitoring' in clause 6.13. – [b-OCP DSBS] provides monitoring information as 'The management controller SHALL support the following IPMI features: Sensor device and sensor scanning/monitoring' in clause 8.11. – [b-OCP NIC] provides monitoring information as 'When the temperature sensor reporting function is implemented, the OCP NIC 3.0 card shall support PLDM for Platform Monitoring and Control (DSP0248 1.1 compliant) for temperature reporting' in Table 49: Temperature Reporting Requirements.
41	**Remote management**	– [b-ETSI EVE007] provide Remote management as 'The BMC/service processor shall be accessible remotely via Ethernet network' in clause 5.6.2. – [b-OCP 1S] provides remote BIOS update as 'The BIOS can be updated remotely under these scenarios' in clause 9.6.8. – [b-OCP 2S] provides remote BIOS update as 'Vendors should provide tool(s) to implement remote BIOS update function' in clause 6.3.6. – [b-OCP AMBH] provides remote BIOS firmware update as 'The motherboard has SP5100 interfaces on board, which support up to six SATA ports' in clause 7.6. – [b-OCP AMBH] provides remote power control as 'The BMC supports remote system power on/off and reboot through LAN or IPMB' in clause 7.4.

Table I.5 – Relationship with related specifications from other SDOs

NO.	Requirements in this Recommendation	Relationship with related specifications from other SDOs
		– [b-OCP Yose] provides remote BMC firmware update as 'Vendors should provide tool(s) to implement a remote BMC firmware update, which will not require any physical input' in clause 6.17. – [b-OCP DSBS] provides remote machine management as 'A Revision 1.0 Decathlete server board SHALL implement the requirements of the OCP Open Hardware Management Specification for Remote Machine Management (Version 0.93)' in clause 10.
42	**Diagnostic of physical machine**	– [b-ETSI EVE007] provide diagnostic of physical machine as 'the rack power subsystem should provide a means to report power system fault events' in clause 5.3.2.3. – [b-OCP 2S] provides error log as 'Error to be logged' in clause 9.11.1. – [b-OCP AMBH] provides system log as 'The BIOS logs system events through the baseboard management controller (BMC)' in clause 5.10. – [b-OCP Yose] provides event log as 'The vendor should implement the BMC to support storing events/logs from each 1S server baseboard, device carrier card and mezzanine card' in clause 6.15. – [b-OCP DSBS] provides log as 'The Decathlete server board standard will define a minimal set of error handling and alerts. These features may become a section of this standard, or may be a standalone specification authored by the OCP Hardware Management project' in clause 9.
43	**Expansion of interconnect network**	– [b-OCP Yose] provides network connectivity as 'The network controller vendors offer Network Interface Cards (NICs) that support multi-host functions. These multi-host NICs provide network connectivity to multiple servers through a PCIe interface' in clause 5.7.6. – [b-OCP DSBS] provides network connectors as 'The server board SHALL have one LAN device to support the RJ-45 network interface connectors' in clause 6.1. – [b-OCP NIC] provides network interconnect as 'NC-SI over RBT capable OCP NIC 3.0 cards shall use a unique Package ID per ASIC when multiple ASICs share the single NC-SI physical interconnect to ensure there are no addressing conflicts' in clause 4.8.1.
44	**I/O interface for device extensions**	– [b-OCP OCSB] provides I/O interface for device extensions as 'High-Speed Interface Topologies' in clause 7. – [b-OCP 2S] provides I/O interface for device extensions as 'PCIe x32 Slot/Riser Card' in clause 11.1. – [b-OCP JBOG] provides I/O interface for device extensions as '8 x16 PCIE Gen3 slots for GPU' in clause 4.1. – [b-OCP HSAS] provides I/O interface for device extensions as 'PCIe Port Assignments' in clause 8. – [b-OCP QGD] provides I/O interface for device extensions as 'PCIe expansion slot' in clause 2. – [b-OCP DSBS] provides I/O interface for device extensions as 'The server board SHALL provide support for one riser card and MAY provide support for two riser cards. The riser card slots can be configured to meet any range of usage models' in clause 6.4.

Table I.5 – Relationship with related specifications from other SDOs

NO.	Requirements in this Recommendation	Relationship with related specifications from other SDOs
45	**Processing unit replacement**	– [b-OCP Yose] provides processing unit replacement as 'The USB connections from all 1S servers are connected to the BMC's virtual hub port through a USB multiplexer so that a user could upgrade the BMC firmware via a USB interface from a 1S server. This method is much faster than going through the OOB' in clause 5.2. – [b-OCP NIC] provides processing unit replacement as 'A multi-host capable OCP NIC 3.0 card shall gracefully handle concurrent in-band queries from multiple hosts and out-of-band access from the BMC for firmware component versions, device model and device ID information' in clause 4.7.3. – [b-OCP OCSB] provide processing unit replacement as 'Tray Backplane Interface' in clause 9.1. – [b-OCP OCSTRAY] provide Processing unit replacement as 'The connector interfaces between the tray mezzanine card and the tray backplane use the Samtec SEARAY solution' in clause 2.
46	**Adding processing units**	– [b-OCP OCSC] provide adding processing units as 'support trays that house up to 24 individual OCS blades' as clause 2. – [b-OCP Yose] provide adding processing units as 'support multi-host functions' in clause 5.7.6.
47	**Adding sub-components of processing units**	– [b-OCP 2S] provide adding memory of processing units as '2x DDR4 slots per channel 'In clause 5.3.2. – [b-OCP IMBH] provide adding sub-components of processing units as 'two PCIe* x4 external connectors on the motherboard' in clause 10.2. – [b-OCP AMBH] provide adding sub-components of processing units as 'motherboard's I/O features' in clause 10.
48	**Adding power supply**	– [b-OCP OCSC] provide adding power supply as 'PDU placement' in clause 3.1.3. – [b-OCP AMBH] provide adding sub-components of processing units as 'The motherboard includes a full server management solution and supports interfaces to an integrated or a set of rear-access 12V Power Supply Units (PSUs)' in clause 3.
49	**Adding cooling component**	– [b-OCP OCSC] provide adding cooling component as 'Fan tray (includes six 140 x 140 mm fans in parallel)' in clause 4.2. – [b-OCP O2USM] provide adding cooling component as 'A maximum of six 40mm fans may be used to cool the components in a single U, with a maximum of twelve 40mm fans* in a 2U server configuration.' in clause 4.4.
50	**No additional ports**	
51	**Authorized access**	– [b-DMTF RedfishAPI] provide authorized access as support both 'Basic Authentication' and 'Redfish Session Login Authentication' in clause 9.2. – [b-DMTF RedfishHI] provide authorized access as 'Opening a Redfish session on the Host Interface may be accomplished by use of any authorized Redfish credentials' in clause 9. – [b-SNIA Swordfish] provide authorized access as 'Implement TLS version 1.2 or greater' in clause 8.1.

Table I.5 – Relationship with related specifications from other SDOs

NO.	Requirements in this Recommendation	Relationship with related specifications from other SDOs
52	**Support fault location**	– [b-ETSI EVE007] provide fault location support as 'hardware with fast failure detection' in clause 5.11. – [b-OCP 1S] provide fault location as 'these errors must include the date, time and location information so that failing components can be easily identified' in clause 9.6.10. – [b-OCP 2S] provide fault location as 'A power failure detection circuit needs to be implemented to initiate 3x actions related to data transferring' in clause 5.3.3. – [b-OCP 2S] provide fault location as 'All POST errors, which are detected by BIOS during POST, should be logged into Event Log' in clause 9.11.1. – [b-OCP Yose] provide fault location as 'Fan failure errors should be logged if the fan speed reading is outside expected ranges between the lower and upper critical thresholds. The Error log should also identify which fan fails' in clause 6.15.1.7.
53	**Hot-plug support**	– [b-ETSI EVE007] provide hot-plug support as 'Supporting hot-plug for vulnerable components, including hard drive and optical modules' in clause 5.11. – [b-OCP OCSPS] provide hot-plug support as 'The power supply shall be hot pluggable' in clause 1. – [b-OCP OCSB] provide hot-plug support as 'The blade contains a NIC mezzanine card to provide small form-factor pluggable (SFP+) and Quad SFP (QSFP+) cable connectivity' in clause 7.2. – [b-OCP 2S] provide hot-plug support as 'the x32 PCIe in riser slot shall support Standard PCIe signal hot swap' in clause 5.5.2. – [b-OCP TP] provide hot-plug support as 'PCIe Hot Plug' in clause 5.5.1.

Appendix II

Use cases of the physical machine for cloud computing

(This appendix does not form an integral part of this Recommendation.)

This appendix describes physical machine related use cases.

Table II.1 – Providing IaaS service with processing resource – use case

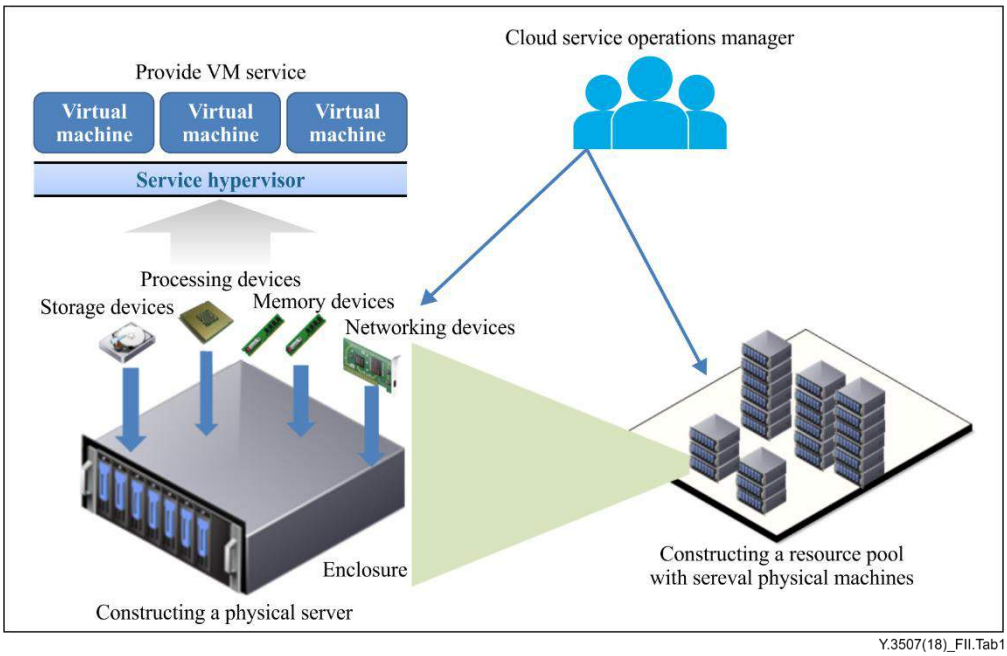
Title	Providing IaaS service with processing resource use case
Description	Infrastructure capabilities type, especially for providing VM, which is resided on a physical machine. The virtual machine provides a virtualized and isolated computing environment for each guest operating system (OS) with processing, storage, networking and other hardware resources. Usually a physical machine would carry more than one virtual machine and needs to provide more virtual CPU than physical CPU, so as the memory and I/O devices. Furthermore, the physical machine usually provides a management function for the CSP to manage and monitor the physical machines. The loading information would help the CSP to select which host to deploy the VMs and the fault location information could help the CSP easily replace the failure component. As more applications run in one physical machine, the reliability is required so that it could continue to run and bear the services without migrating when there are few failures. As some applications may require some other hardware components with special features, the physical machine would have to reserve one or more extended interfaces for adding cloud resources. To improve the VM's performance, the physical machines usually use CPUs with virtualization instruction set support. For situations with a lot of network traffic processing, physical machines can offload traffic processing to I/O devices to improve performance and reduce the load of CPUs.
Roles/sub-roles	CSP: cloud service operations manager
Figure	 Y.3507(18)_FII.Tab1
Pre-conditions (optional)	The virtual machine resides on the physical machine.
Post-conditions (optional)	CSP: cloud service operations manager wants to build or expand a resource pool to provide VM service.

Table II.1 – Providing IaaS service with processing resource – use case

Derived requirements	– Virtualization instruction set (see clause 7.1.1.1) – Hardware-assisted I/O virtualization (see clause 7.1.1.4) – Hardware-assisted memory virtualization (see clause 7.1.1.2) – Supporting various types of memory (see clause 7.1.1.2) – Network interface virtualization (see clause 7.2) – Provide I/O interface to administrator (see clause 7.2) – Provide I/O interface to external storage device (see clause 7.2) – I/O devices direct accessing (see clause 7.1.1.4) – Monitoring status of physical machine (see clause 7.1.4) – Automatically power operation (see clause 7.1.6) – Processing unit operation (see clause 7.3) – Remote management (see clause 7.3) – Support fault location (see clause 7.6) – Hot-plug support (see clause 7.6) – Workload offload (see clause 7.1.1.4) – Hardware acceleration (see clause 7.1.1.4) – Interface for monitoring power (see clause 7.1.2)

Table II.2 – Preparing a physical machine – use case

Title	Preparing a physical machine
Description	A cloud service operations manager installs multiple processing units on the backplane of an enclosure to increase the computing resources of a physical machine. He or she also installs more than one storage device per CPU in a processing unit through standard storage interfaces. To connect all multiple processing units together, a cloud service operations manager mounts a switch device which is responsible for system interconnects and network topology to the backplane of the enclosure. In addition, the enclosure is equipped with a power supply to provide power to an entire physical machine and a cooling device to reduce heating. A cloud service operations manager should be able to check whether each device is installed in a physical machine correctly through a console panel on the enclosure. System software and operating systems are installed on corresponding devices or rebooted and consequently a physical machine completes to set up its operations. Based on the above steps to construct a physical machine, several physical machines are connected with each other by their external interfaces and can be installed in a standard rack.
Roles/sub-roles	CSP: cloud service operations manager.

Table II.2 – Preparing a physical machine – use case

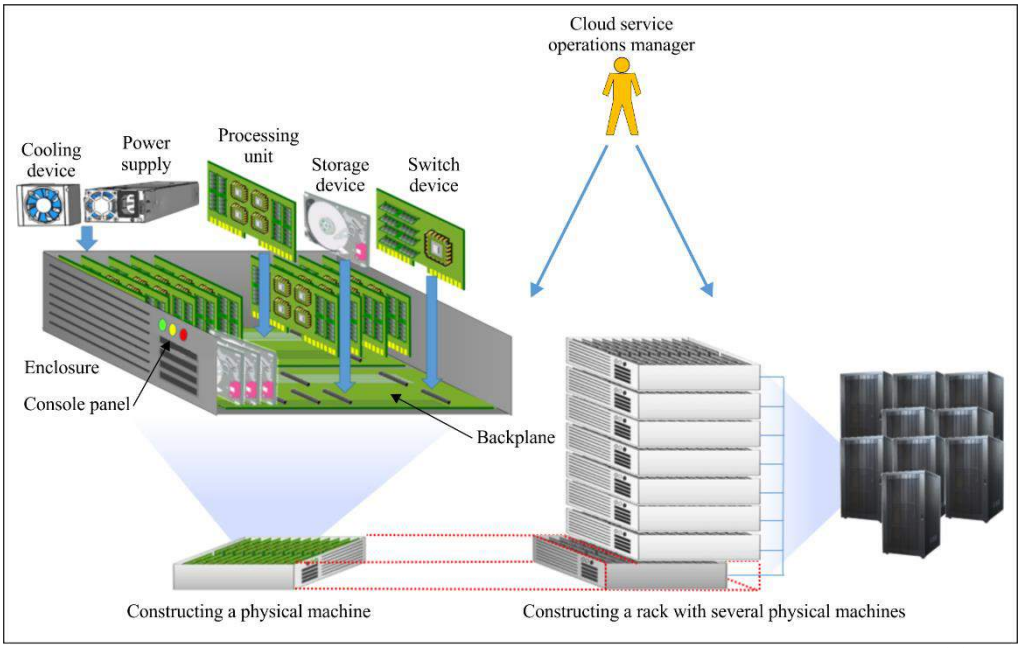
Figure	
Pre-conditions (optional)	CSP: cloud service operations manager wants to modify or expand the resources in a physical machine.
Post-conditions (optional)	A physical machine provides a cloud service.
Derived requirements	– Hot-plug support (see clause 7.6) – Configuration of multiple processing units (see clause 7.1.5) – Monitoring status of physical machine (see clause 7.1.4)

Table II.3 – Cold data storage resource – use case

Title	Cold data storage resource use case
Description	Cold data means data that is stored but almost never read again. The cloud storage service for cold data provides almost no limit storage capacity at a very low cost and the physical machine for cold data storage requires the highest capacity and the lowest cost. The typical use case is a series of sequential writes, but random reads. As the physical machine is recommended to provide as much storage capacity as possible, it would have many large-capacity disks. To provide a highly durable storage service, the physical machine is recommended to provide management function for the CSP to manage and monitor the physical machine cluster and then the CSP can rebuild the data in time when some failures happen, also the hot plug function is needed. Physical machines usually support storage of different media to balance between cost and performance for different situations.
Roles/sub-roles	CSP: cloud service operations manager

Table II.3 – Cold data storage resource – use case

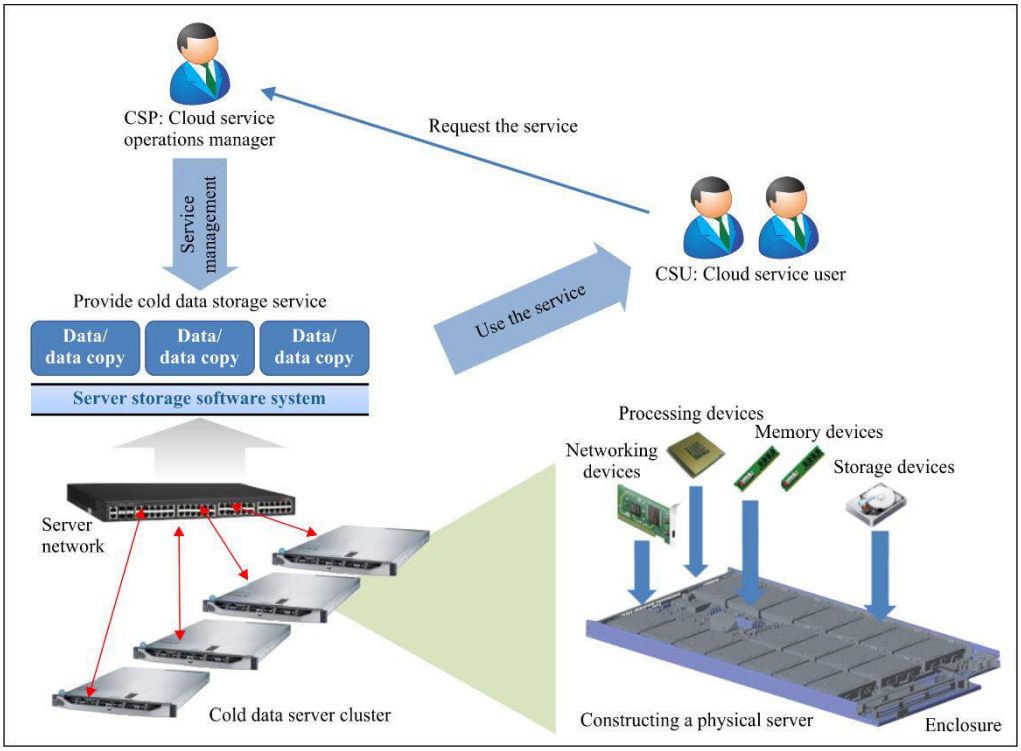
Figure	
Pre-conditions (optional)	The cloud storage service resides on the physical machine.
Post-conditions (optional)	CSP: cloud service operations manager wants to build or expand a resource pool to provide cloud storage service for cold data.
Derived requirements	– Hot-plug support (see clause 7.6) – Low power consumption of CPU (see clause 7.1.1.1) – Supporting various types of memory (see clause 7.1.1.2) – Provide I/O interface to administrator (see clause 7.2) – Provide I/O interface to external storage device (see clause 7.2) – Storage hibernation (see clause 7.1.1.3) – Remote management (see clause 7.3) – Diagnostic of physical machine (see clause 7.3) – Multiple interfaces for storage (see clause 7.1.1.3) – I/O interface for device extensions

Table II.4 – Using an interconnect network for high-performance service – use case

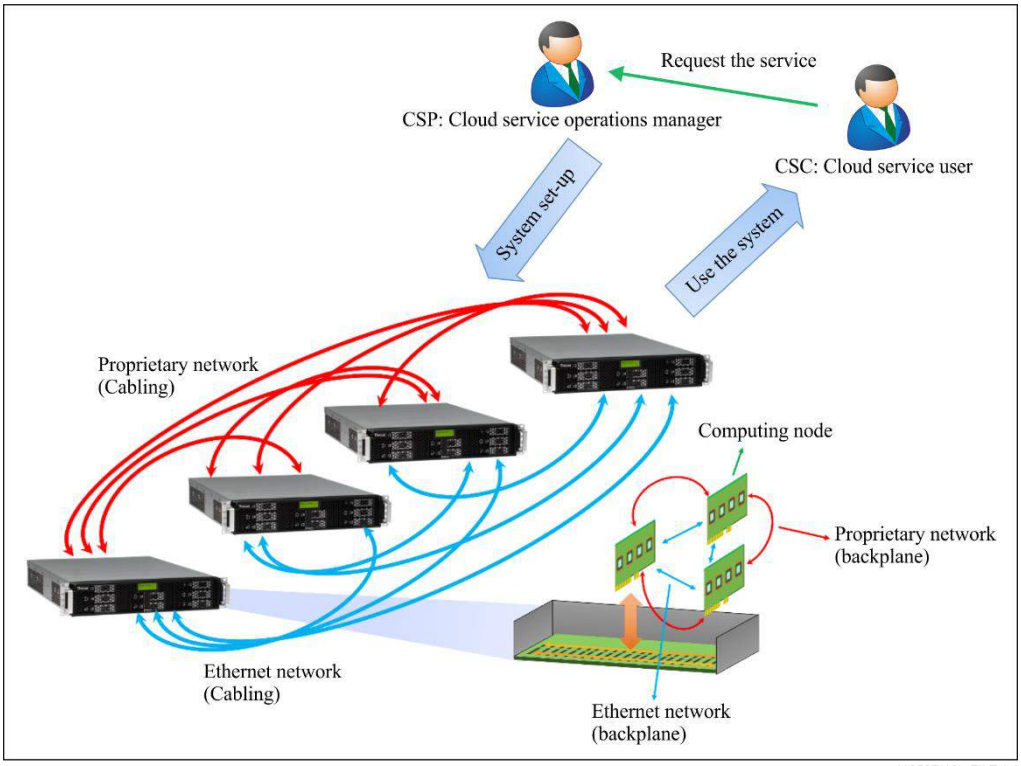
Title	Using interconnect network for high-performance service
Description	When a cloud service user requests a high performance computing service (e.g., parallel processing, Big data processing, etc.), a cloud service operations manager is responsible for setting up an interconnection network among processing units, because multiple computing resources are required to perform such a service. Ethernet is a widely used protocol for the interconnection network but the cloud service operations manager may provide other protocols. Therefore, depending on the protocols, the performance of the interconnect network is determined and the cloud service operations manager can select and provide the appropriate interconnect network to the cloud service user. For utilizing this interconnect network system, a cloud service user can employ socket based applications in the case of using Ethernet protocol. For other networks, a cloud service user is provided with applications per application program interfaces (API) from a cloud service operations manager. This is due to the fact that, a cloud operations manager also has a responsibility to provide a device driver and API for utilizing the propriety network. Occasionally, a cloud service user may request multiple physical machines for such a service. In this case, a cloud operations manager has a responsibility to support multiple shared resources through the network. Since the physical machines are independent of network devices, this network would be arranged as cabling in an interconnect network. When a cloud service operations manager makes this cabled network, it is constructed to support various topologies (e.g., ring, mesh, tree) to meet the different performance levels of the service requested from a cloud service user.
Roles/sub-roles	CSC: Cloud service user and CSP: Cloud service operations manager
Figure	 Y.3507(18)_FII.Tab4
Pre-conditions (optional)	CSC: Cloud service user wants to use a high performance computing application.
Post-conditions (optional)	Physical machines can run a high performance computing application through a system interconnect network and cabled network.

Table II.4 – Using an interconnect network for high-performance service – use case

Derived requirements	– Sharing process unit component (see clause 7.1.5) – Interconnect network supports (see clause 7.1.5) – Device driver and API supports (see clause 7.2) – Expansion of interconnect network (see clause 7.4) – Network topology (see clause 7.1.5)

Table II.5 – Physical machine for hyper-scale deployment – use case

Title	Physical machine for hyper-scale deployment
Description	This use case covers the situation where very large numbers of physical machines will be employed in multiple data centres around a region or around the world. In this case, a single physical machine will typically be implemented as a server blade that fits into a specially built rack. The rack will typically also include storage, management and networking equipment, which might or might not be implemented using similar blades.
Roles/sub-roles	CSP: cloud service operations manager.
Figure	 In this type of deployment, physical machines are constructed for deployment in high-density racks specifically designed for the purpose. Each rack provides all the infrastructure required to support the machines, including power, network connectivity and ventilation/cooling. Individual physical machines are automatically initialised and provisioned with necessary software when plugged into an active rack. Once running, each machine is made available for the deployment of VMs or other functions requested by CSCs or CSP administrators. Fault tolerance is often provided by software across multiple machines, so an individual machine can fail without adverse effect on the overall system.
Pre-conditions (optional)	CSP: The CSP wishes to deploy many physical machines in two or more locations, using minimal staffing.
Post-conditions (optional)	A physical machine is plugged into a rack, configures itself to the local network and is automatically provisioned with all necessary software including the host operating system, network stacks and hypervisor. The data centre management system is then able to deploy workloads to the machine. In the event of failure, the machine can be removed from the rack and a replacement plugged in with minimal impact on deployed cloud services. A data centre can be left unmanned for several days or weeks at a time. When visited, the failed machines can be quickly removed and replaced by new or refurbished machines, which configure and provision themselves automatically.

Table II.5 – Physical machine for hyper-scale deployment – use case

Derived requirements	– Minimum energy consumption (see clause 7.1.2) – No additional ports (see clause 7.5) – Authorized access (see clause 7.5) – Hot-plug support (see clause 7.6) – Visual indications (see clause 7.1.4)

Table II.6 – Physical machine for unmanned deployment – use case

Title	Physical machine for unmanned deployment
Description	This use case covers the situation where physical machines will be in places where physical access is extremely difficult or only available at infrequent intervals. In this case, a single physical machine will typically be implemented as a server blade that fits into a specially built rack. The rack will typically also include storage, management and networking equipment, which might or might not be implemented using similar blades.
Roles/sub-roles	CSP: cloud service operations manager.
Figure	 In this type of deployment, physical machines are constructed for deployment in locations where physical access is very tightly constrained. These will typically be inside some form of self-contained "capsule" rather than a normal building. Examples are systems deployed in underwater containers for positioning close to coastal urban centres.
Pre-conditions (optional)	CSP: The CSP wishes to deploy physical machines in locations where human access will not be possible for the majority or operational time.
Post-conditions (optional)	The physical machines are left running without human access for periods of six months or more. The data centre management system can deploy workloads to the machine. In the event of failure, the machine can be taken off line, remote diagnostics can be run and the machine either returned to service or taken permanently offline.
Derived requirements	– Minimum energy consumption (see clause 7.1.2) – Cooling component replacement (see clause 7.1.3) – Cooling component redundancy (see clause 7.1.3) – Interface for controlling fan speed (see clause 7.1.3) – Self-checking mechanism (see clause 7.1.6) – Remote management (see clause 7.3) – Diagnostic of physical machine (see clause 7.3)

Table II.7 – Physical machine for network edge – use case

Title	Physical machine for network edge
Description	This use case covers the situation where physical machines will be in network edge locations such as at 5G cell towers, telephone exchanges and cable TV head-end multiplexers. This is one use of the term "micro data centre". The primary reason for this is to minimise network latency between end users and the cloud services running at the network edge, or to concentrate network traffic at the edge to manage load on core network servers (e.g., for massive IoT telemetry applications).
Roles/sub-roles	CSP: cloud service operations manager.
Figure	 In this type of deployment, physical machines are constructed for deployment at the edge of the network, usually co-located with access network transmission and/or multiplexing equipment. Examples of such locations include: • Local telephone exchanges • Street multiplexers (e.g., FTTC) • Cellular towers • Cable TV head-ends • Airliner WiFi/Cellular network equipment.
Pre-conditions (optional)	CSP: The CSP wishes to deploy physical machines to support cloud services running at the edge of their (or a partner's) physical network.
Post-conditions (optional)	The physical machine(s) run co-located with other network equipment at the edge of the network. The CSP can deploy cloud services or service components to these network edge micro data centres. CSUs can access the cloud service within minimal network latency. The CSP can process large amounts of data from CSUs, without imposing heavy loads on the backhaul network or the core network cloud services.
Derived requirements	– Supporting power redundancy (see clause 7.1.2) – Adding power supply (see clause 7.4) – Adding cooling component (see clause 7.4) – Authorized access (see clause 7.5) – Hot-plug support (see clause 7.6) – Visual indications (see clause 7.1.4) – Monitoring environment condition (see clause 7.1.6)

Table II.8 – Configurations of clustering processing units – use case

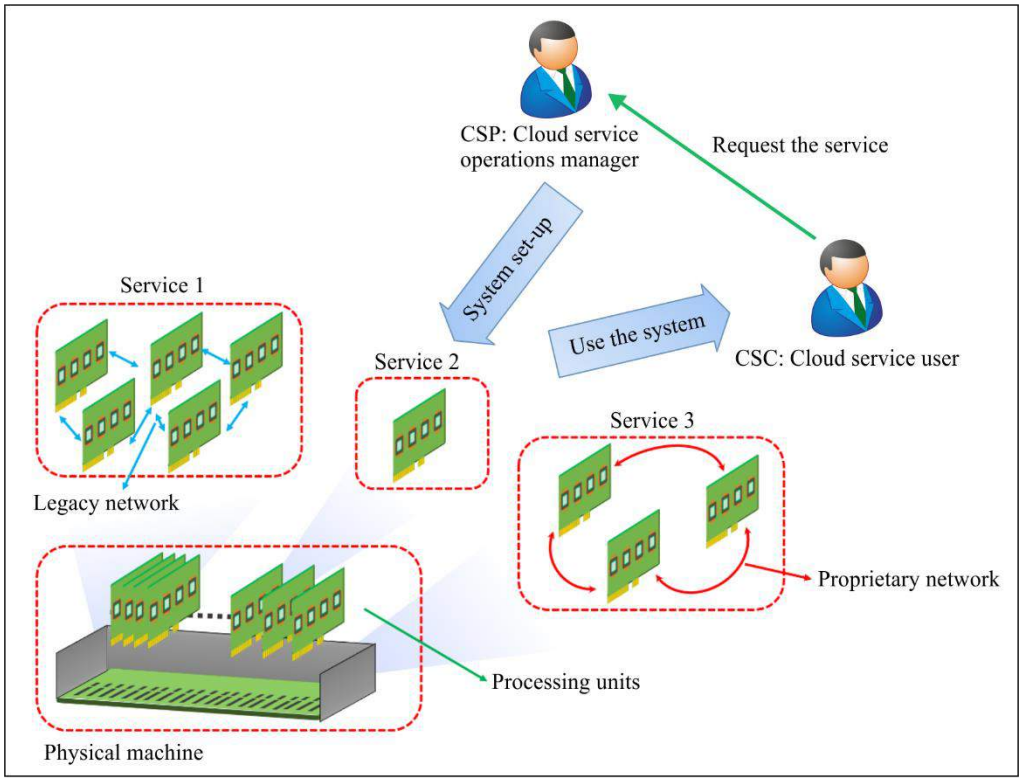
Title	A use case of configurations of clustering processing units
Description	When a CSC: cloud service user requests a cloud service, a CSP: cloud service operations manager is responsible for providing computing resources, which can run the cloud service. In this case, based on the multiple processing units in the physical machine, it is possible for the CSP: cloud operations manager to configure a clustering system which can distribute the computational loads among the multiple processing resources. Therefore, in order to utilize highly integrated computing resources efficiently, the CSP: cloud operations manager has a responsibility to configure the clustered processing units. The configuration can be changed dynamically and elastically according to the cloud service's requirements from the CSC: cloud service user. In other words, according to the required cloud service's characteristics (e.g., network usage ratio, computing capability, the proportion of memory intensive computation, an efficiency of distributed computing), the configuration of the cluster system can vary. In case of a cloud service based on distributed processing clustering configuration is suitable because data analysis work load can be divided into several processing units. On the other hand, when a CSC: cloud service user requests a cloud service, where data communications occur intensively among processing units, minimum numbers of processing units are recommended as a clustered resources. In addition, the networking between each processing unit for clustering can be basically based on a legacy network such as Ethernet. For a cloud service that is clustering-favourable but has high proportion of network usage among processing units, a proprietary network for clustering environment can be provided to eliminate the overhead of network communications.
Roles/sub-roles	CSP: cloud service operations manager, CSC: cloud service user
Figure	 Y.3507(18)_FII.Tab8
Pre-conditions (optional)	CSC: cloud service user wants to use a cloud service.

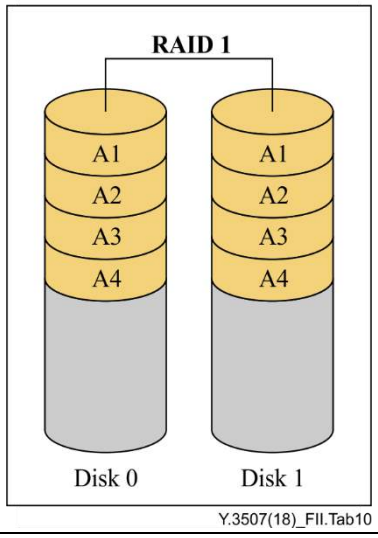
Table II.8 – Configurations of clustering processing units – use case

Post-conditions (optional)	Physical machines can run a cloud service efficiently and elastically according to the desired performance.
Derived requirements	– Configuration of multiple processing units (see clause 7.1.5) – Multiple CPUs (see clause 7.1.1.1) – Adding processing units (see clause 7.4) – Adding sub-components of processing units (see clause 7.4) – Network topology (see clause 7.1.5) – Interconnect network supports (see clause 7.1.5) – Device driver and API supports (see clause 7.2)

Table II.9 – Replacing components of a physical machine – use case

Title	A use case of replacing components of physical machine
Description	This use case covers the situation where components of physical machine be replaced. After deployment and operation, a component of physical machine may need to be replaced with another new one due to component failure. In addition, a component could be replaced with component of other model to upgrade the performance. Typically, physical machine should support replacement of the main components, including CPU, memory, storage, power supply and cooling component.
Roles/sub-roles	CSP: cloud service operations manager
Figure	  To support replacement, the components are not coupled to the physical machine so that the components can be installed or uninstalled dynamically. Typically, the components are designed to follow certain specifications to ensure compatible interface and shape.
Pre-conditions (optional)	CSP wishes to replace some components of physical machines to fix components failure or upgrade components.
Post-conditions (optional)	Physical machine can runs normally with the new components.
Derived requirements	– CPU replacement (see clause 7.1.1.1) – Memory replacement (see clause 7.1.1.2) – Storage replacement (see clause 7.1.1.3) – Processing unit replacement (see clause 7.4) – Equipment for mounting and removal (see clause 7.1.4) – Power supply replacement (see clause 7.1.2) – Cooling component replacement (see clause 7.1.3)

Table II.10 – High reliability deployment – use case

Title	A use case for high reliability deployment
Description	This use case covers the situation where physical machine will be deployed with high reliability. To achieve high reliability, physical machine needs to be deployed with redundant main components, such as CPU, power supply and cooling component. In addition, physical machine needs to support technology to reduce data errors and data loss at work, such as memory error correction and RAID. Trough RAID technology, data of physical machine is distributed across multiple drives in different ways, referred to as RAID levels, depending on the required level of redundancy and performance. Take RAID1 as an example, as shown in below figure, RAID 1 consists of an exact copy (or mirror) of a set of data on two or more disks. The data of physical machine will not loss so long as at least one member drive is operational.
Roles/sub-roles	CSP: cloud service operations manager
Figure	
Pre-conditions (optional)	CSP wishes to deploy physical machines with high reliability.
Post-conditions (optional)	Physical machines can still work when some components fail. The physical machine can reduce data errors and losses due to memory and storage failures.
Derived requirements	– Multiple CPUs (see clause 7.1.1.1) – Memory reliability (see clause 7.1.1.2) – Storage redundancy hardware (see clause 7.1.1.3) – Supporting power redundancy (see clause 7.1.2) – Cooling component redundancy(see clause 7.1.3)

Bibliography

[b-DMTF RFAPI] *Redfish Scalable Platforms Management API Specification*.

[b-DMTF RFHI] *Redfish Host Interface Specification*.

[b-DMTF RFP] *Redfish Interoperability Profiles*.

[b-ETSI EVE007] *Hardware Interoperability Requirements Specification*.

[b-OCP 1S] *Twin Lakes 1S Server Design Specification V1.00*.

[b-OCP 25GDual] *25G Dual Port OCP 2.0 NIC Mezzanine Card V1.0*.

[b-OCP 2S] *Facebook 2S Server Tioga Pass Specification V1.0*.

[b-OCP ACTI] *Add-on-Card Thermal Interface Spec for Intel Motherboard V3.0*.

[b-OCP AMBH] *Open Rack- AMD Motherboard Hardware V2.0*.

[b-OCP BS] *QCT Big Sur Product Architecture Following Big Sur Specification V1.0*.

[b-OCP Debug] *OCP debug card with LCD spec V1.0*.

[b-OCP DSBS] *Decathlete Server Board Standard V2.1*.

[b-OCP FSCI] *Facebook server Fan Speed Control Interface Draft V0.1*.

[b-OCP G1] *Barreleye G1 Specification*.

[b-OCP G2] *Barreleye G2 Specification*.

[b-OCP HSAS] *Hyve Solutions Ambient Series-E V1.2*.

[b-OCP HSCH] *Micro-Server Card Hardware V1.0*.

[b-OCP IMBH] *Open Rack- Intel Motherboard Hardware V2.0*.

[b-OCP JBOG] *Big Basin-JBOG Specification V1.0*.

[b-OCP M2] *Facebook, Microsoft, M.2 Carrier Card Design Specification V1.0*.

[b-OCP MB] *Facebook Server Intel Motherboard V3.1*.

[b-OCP MEZZ] *Mezzanine Card 2.0 Design Specification V1.0*.

[b-OCP MEZZMB] *Mezzanine Card for Intel v2.0 Motherboard*.

[b-OCP NIC] *OCP NIC 3.0 Design Specification V0.8*.

[b-OCP O1USM] *Project Olympus 1U Server Mechanical Specification*.

[b-OCP O2USM] *Project Olympus 2U Server Mechanical Specification*.

[b-OCP OAPM] *Project Olympus AMD EPYC Processor Motherboard Specification*.

[b-OCP OBIOS] *Project Olympus Intel Xeon Scalable Processor BIOS Specification*.

[b-OCP OCSB] *Open CloudServer OCS Blade Specification V2.1*.

[b-OCP OCSC] *Open CloudServer Chassis Specification V2.0*.

[b-OCP OCSCM] *Open CloudServer OCS Chassis Manager Specification V2.1*.

[b-OCP OCSJBOD] *Open CloudServer JBOD specification V1.0*.

[b-OCP OCSNIC] *Open CloudServer OCS NIC Mezzanine Specification V2.0*.

[b-OCP OCSPS] *Open CloudServer OCS Power Supply V2.0*.

[b-OCP OCSPSAM] *Open CloudServer OCS Programmable Server Adapter Mezzanine Programmables V1.0*.

[b-OCP OCSSAS] *Open CloudServer SAS Mezzanine I/O specification V1.0*.

[b-OCP OCSSSD] *Open CloudServer OCS Solid State Drive V2.1*.

[b-OCP OCSTRAY] *Open CloudServer OCS Tray Mezzanine Specification V2.0*.

[b-OCP OCTAM] *Project Olympus Cavium ThunderX2 ARMx64 Motherboard Specification*.

[b-OCP OMB] *Project Olympus Intel Xeon Scalable Processor Motherboard Specification*.

[b-OCP OSR] *Project Olympus Server Rack Specification*.

[b-OCP PCIRC] *Facebook PCIe Retimer Card V1.1*.

[b-OCP PMSCH] *Panther+ Micro-Server Card Hardware V0.8*.

[b-OCP QGD] *QuantaGrid D51B-1U V1.1*.

[b-OCP SJ] *Inspur Server Project San Jose V1.01*.

[b-OCP TP] *Facebook Server Intel Motherboard V4.0 Project Tioga Pass V0.30*.

[b-OCP Yose] *Facebook Multi-Node Server Platform: Yosemite V2 Design Specification V1.0*.

[b-SNIA SF] *SNIA Swordfish Specification V1.0.6*.

CLOUD STORAGE

CLOUD COMPUTING

Cloud computing – Overview and high-level requirements of distributed cloud

Recommendation ITU-T Y.3508

(08/2019)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Summary

Recommendation ITU-T Y.3508 provides an overview and high-level requirements for distributed cloud. This Recommendation introduces the concept of the distributed cloud and identifies the characteristics of distributed cloud. Based on concept and characteristics, configuration models are illustrated. Deployment considerations of distributed cloud are provided in perspective of infrastructure, network, service, management and security. From use cases, high-level requirements of the distributed cloud are derived.

Keywords

Cloud computing, distributed cloud, high-level requirement.

Table of Contents

1 Scope

This Recommendation provides an overview and high-level requirements of the distributed cloud. It addresses the following subjects:

– definition of distributed cloud;
– concept of distributed cloud;
– characteristics of distributed cloud;
– configuration models of distributed cloud;
– deployment considerations of distributed cloud; and
– high-level requirements of distributed cloud.

Use cases of distributed cloud are provided in Appendices I and II. Also, a comparison between distributed cloud and other technologies is described in Appendix III.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014), *Information technology – Cloud computing – Overview and vocabulary*.

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), *Information technology – Cloud computing – Reference architecture*.

[ITU-T Y.3511] Recommendation ITU-T Y.3511 (2014), *Framework of inter-cloud computing*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 cloud capabilities type [IUT-T Y.3500]: Classification of the functionality provided by a cloud service to the cloud service customer, based on resources used.

NOTE – The cloud capabilities types are application capabilities type, infrastructure capabilities type and platform capabilities type.

3.1.2 cloud computing [IUT-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications and storage equipment.

3.1.3 cloud service [ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.4 cloud service customer [ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

NOTE – A business relationship does not necessarily imply financial agreements.

3.1.5 cloud service provider [ITU-T Y.3500]: Party which makes cloud services available.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 cloud service image: An executable code with state information of virtual machine or container.

NOTE 1 – State information includes execution states, disk states and memory states of system, such as program counter, registry, disk volume number, disk volume size, memory stack and information of allocated memory.

NOTE 2 – Cloud service image includes operating system, libraries, data files, applications, etc.

3.2.2 core cloud: A cloud computing, which manages resource pools including resources in the edge of the network and enables cloud service.

NOTE – Enabled cloud service on the core cloud is provided by a cloud service provider (CSP).

3.2.3 distributed cloud: Distribution of cloud capabilities types to the edge of the network for enabling cloud services with low latency and real time processing on limited bandwidth by interworking among pools of physical or virtual resources.

3.2.3 edge cloud: A cloud computing deployed to the edge of the network accessed by cloud service customers (CSCs) with small capacity resources enabling cloud service.

NOTE 1 – Enabled cloud service on the edge cloud is lightweight cloud service provided by a cloud service provider (CSP) depending on cloud service category.

NOTE 2 – Lightweight cloud service refers to a portion of cloud service to reconfigure the functionality of cloud service to fit on edge cloud such as base station and gateway with small capacity resource.

3.2.5 regional cloud: A cloud computing hosted from core cloud to particular geographical regions.

NOTE – Enabled cloud service on the regional cloud is entire or partial cloud service of core cloud provided by a cloud service provider (CSP).

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AR	Augmented Reality
CC	Core Cloud
CSC	Cloud Service Customer
CSP	Cloud Service Provider
EC	Edge Cloud
IoT	Internet of Things
MEC	Multi-access Edge Computing
ML	Machine Learning
QoS	Quality of Service
RC	Regional Cloud
SLA	Service Level Agreement
VR	Virtual Reality

5 Conventions

In this Recommendation:

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

6 Overview of distributed cloud

6.1 Concept of distributed cloud

Cloud computing is a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand [ITU-T Y.3500]. Services in Internet of things (IoT), augmented reality (AR)/virtual reality (VR), artificial intelligence (AI) and 5G application domains requiring cloud infrastructure are gradually increasing and real-time services in the above domains are also demanding especially for safety and surveillance applications.

Cloud computing has challenges to support the real-time services due to (i) the network latency between cloud service provider (CSP) and cloud service customer (CSC), and (ii) the load congestion on the data centre. For these challenges, what is needed is the delivery of cloud services to nearby CSCs in order to meet real-time service delivery. Also, the distribution of cloud capabilities types to the edge of the network accessed by CSCs are needed for load congestion.

This Recommendation introduces the distributed cloud, which is distribution of cloud capabilities types to the edge of the network for enabling cloud service with low latency and real-time processing on limited bandwidth by interworking among a pool of physical or virtual resources.

Figure 6-1 shows a concept of distributed cloud. The distributed cloud includes core, regional and edge clouds, which meet the cloud capabilities types described in [ITU-T Y.3500]. Cloud services are deployed to the core, regional and edge clouds, interwork with one another, and provide a single system view to the CSCs for location transparency. Thus, the distributed cloud provides low latency and fast response to access cloud services by CSCs to satisfy their need for real-time services in various areas.

Global management manipulates both distributed cloud resources and cloud service distribution appropriately for CSC's demands. The distributed cloud resource is the aggregated infrastructure from core, regional and edge clouds, such as physical or virtual resources of compute, storage and network.

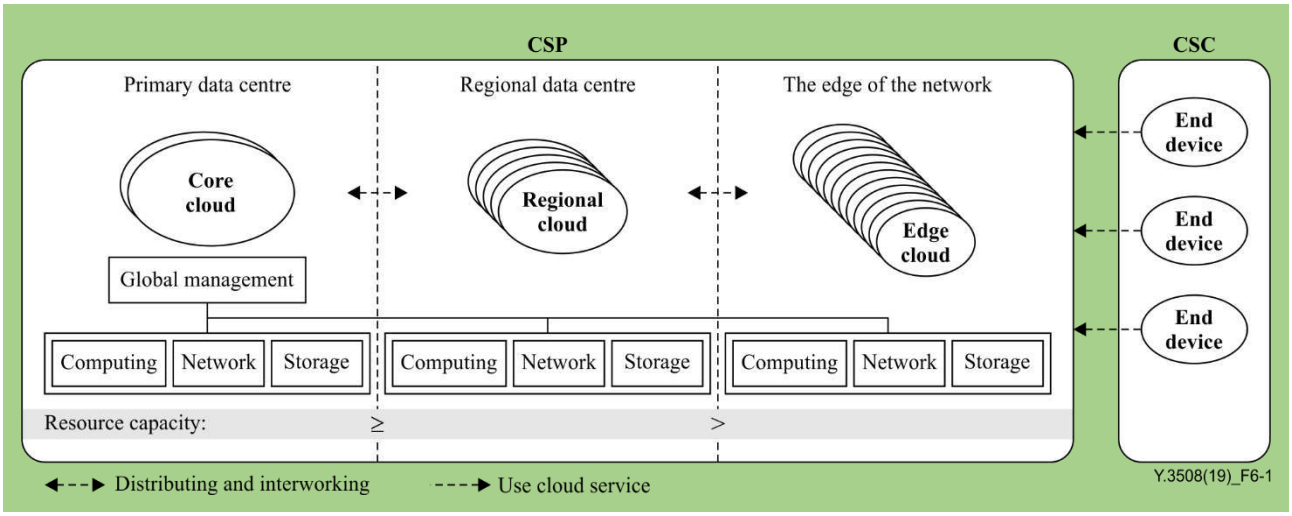


Figure 6-1 – Concept of distributed cloud

– **Core cloud (CC)**: The CC has large resource capacity and global management point to control cloud resources in the distributed cloud. The core cloud supports cloud services with high computing intensive and geographic independence;

– **Regional cloud (RC)**: The RC is optionally deployed in particular regions from the core cloud for load sharing and service quality enhancement. The regional cloud handles cloud service requests from the region controlled by global management of the core cloud;

NOTE 1 – The regional cloud supports lower latency than the core cloud by executing customized cloud services for CSCs in a particular region. It is assumed that the network latency from the CSC to the regional cloud is lower than from the CSC to the core cloud and that the difference of cloud service execution time between the core and regional cloud is negligible.

NOTE 2 – The regional cloud performs buffering load of cloud service and caching data from the core cloud and provides them to CSCs in the region.

– **Edge cloud**: The edge cloud is deployed at the edge of the network accessed by CSCs and has a small resource capacity. The edge cloud requires specialized hardware resources on purpose; i.e., the resources in the edge cloud are constrained due to limitations of space or power. The edge cloud may have different configurations of resources and cloud capabilities types with physical and virtual resources depending on a CSC's requirements of cloud services and conditions in the deployment environment.

Figure 6-2 shows an example of providing real-time service on distributed cloud for the case of a machine learning (ML) service. The example has four phases.

– **Phase 1 – collecting**: End device 1 transfers sensor data to an endpoint of ML training service in the core cloud to train the data;

– **Phase 2 – training**: ML training service trains the data and gets a trained rule at the core cloud;

– **Phase 3 – caching**: The trained rule is cached from core cloud to regional cloud; the trained rule is then cached to edge clouds 1 and 2;

– **Phase 4 – forecasting**: End devices 1 and 2 transfer sensor data to edge clouds 1 and 2, and then edge clouds 1 and 2 perform ML forecasting in real-time processing. The forecasting result is quickly delivered to end devices 1 and 2.

If the ML forecasting service is also processed at the core cloud without the edge cloud, then the end device of the CSC will receive the forecasting results from the core cloud with high latency. The example in Figure 6-2 highlights how the distributed cloud provides benefit to the cloud service in the edge cloud by providing low latency and real-time processing.

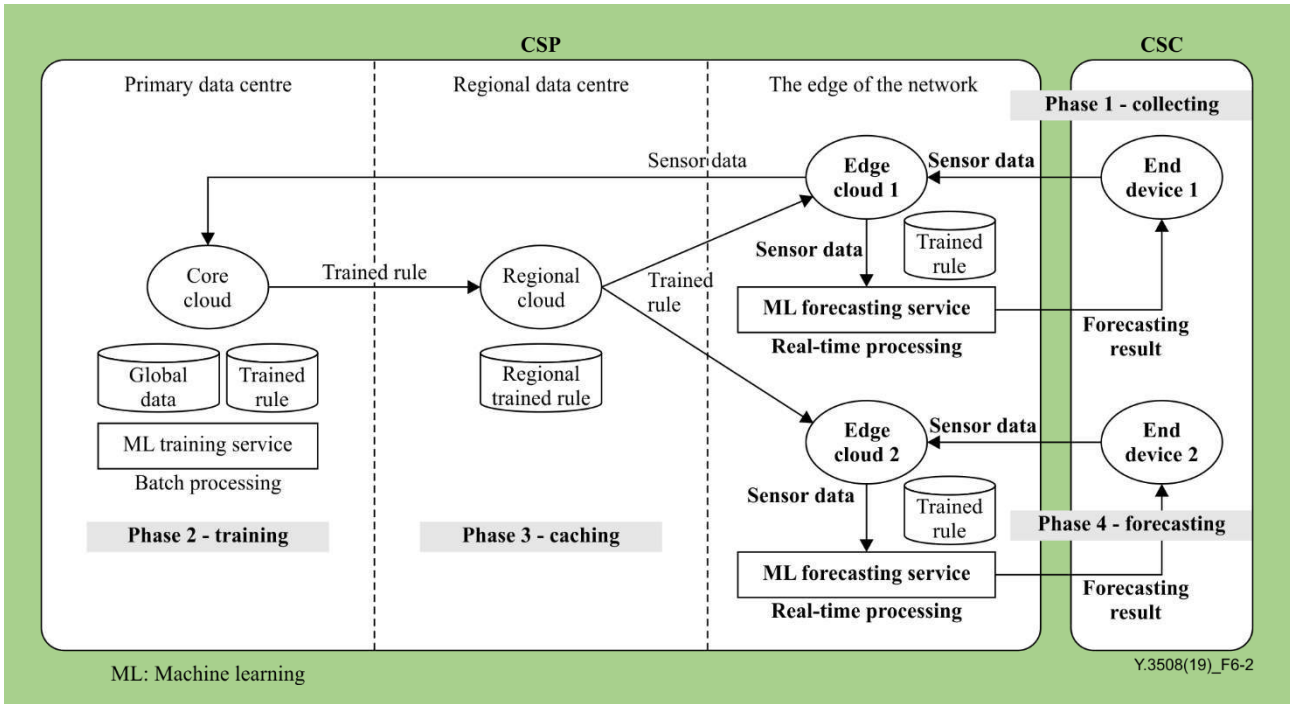


Figure 6-2 – Example of providing real-time service on distributed cloud for the case of a machine learning service

NOTE 3 – In this example, it is assumed that the network latency from the end devices to the edge cloud is much lower than from the end devices to the core cloud, and that the execution time of the ML forecasting service is faster than the ML training service.

6.2 Characteristics of distributed cloud

The characteristics of cloud computing [ITU-T Y.3500] are inherited to distributed cloud as:

– broad network access;
– measured service;
– multi-tenancy;
– on-demand self-service;
– rapid elasticity and scalability;
– resource pooling.

The distributed cloud also has the following additional characteristics:

– **distributed cloud resource**: The resources of distributed cloud are geographically distributed at various types of data centres, base stations and IoT gateways. The distributed cloud resources are pooled on demand to meet CSC requirements by using different physical and virtual resources dynamically;
– **heterogeneous infrastructure**: The distributed cloud has different scale infrastructures with large resource capacity in core/regional cloud and small resource capacity in edge cloud. The distributed cloud needs to utilize heterogeneous infrastructure as a single system to provide various services to CSCs;
– **context awareness network**: The distributed cloud has on-demand network control according to context information for CSCs. Through context awareness network, mirrored cloud service to edge cloud is provided directly to CSCs;

  NOTE – Context information includes cloud service context information and network service context information. Examples of cloud service context information are capacity of cloud, resource usage, service ID/name, service location, status of neighbour. Examples of network service context information are latency, bandwidth, quality of service (QoS), routing path.

– **agile service**: Cloud services can be deployed to the distributed cloud resource quickly and can be easily developed. The developed cloud services can be rapidly and dynamically provided on-demand across various types of distributed cloud resources;
– **autonomous management**: The distributed cloud has global management in core cloud for the management of distributed cloud resources and cloud service with autonomous resource management for edge cloud. Edge cloud can manage its own resources and services when the global management system of distributed cloud is not applicable.

6.3 Configuration models of distributed cloud

The cloud computing needs to be distributed to nearby CSCs to support characteristics of distributed cloud. Depending on a CSC's requirements and characteristics of distributed cloud, cloud services are deployed to one or more cloud among edge, regional and core clouds with network functions. For each cloud service with the CSC's requirements, network resources are allocated by network slicing which allows multiple logical networks to run on top of a shared physical network infrastructure.

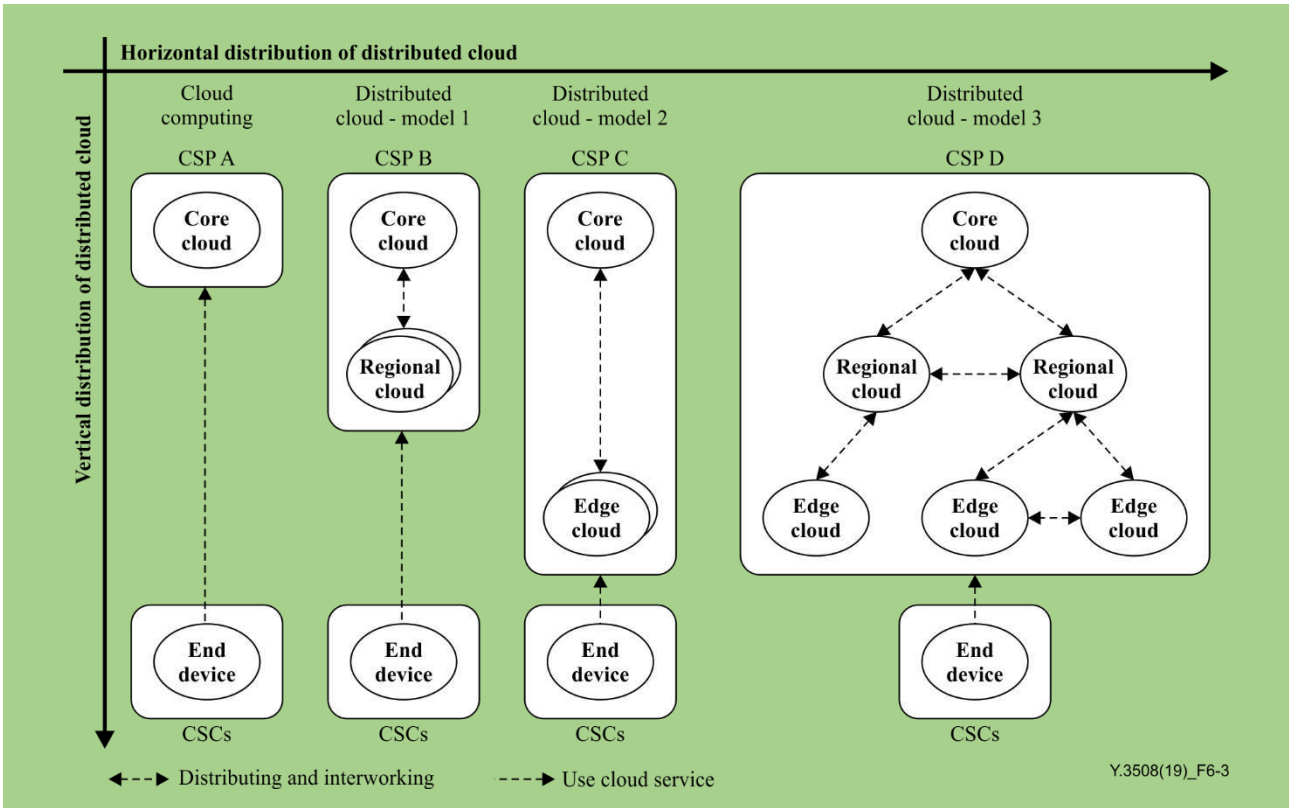


Figure 6-3 – Edge, regional, core cloud configuration in distributed cloud

Table 6-1 describes the generic model of distributed cloud by composing two or more clouds among core, regional and edge cloud. The end device in the figure represents CSCs' devices such as mobile phones, personal computers (PCs), laptops, etc.

Table 6-1 – Distributed cloud configuration model

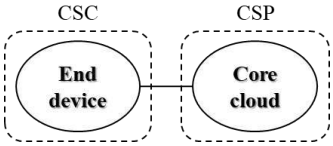
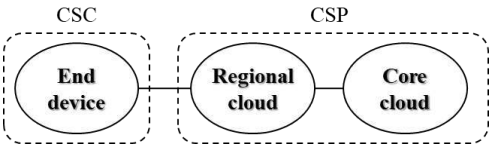
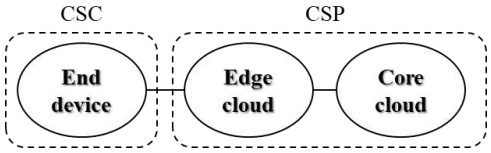
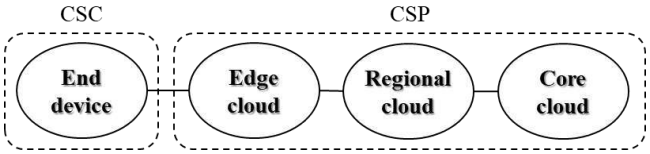
Model	Description
Model 0	 Model 0 is a shape of cloud computing.
Model 1 (Regional – Core)	 Model 1 is a shape of a distributed cloud in which the core cloud and the regional cloud are configured together. Cloud services are provided from one or more clouds among the regional cloud and the core cloud. The regional cloud is hosted for a cloud service from the core cloud to a particular region to support localization of cloud services. The regional cloud assists the core cloud by mitigating traffic of cloud service.

Table 6-1 – Distributed cloud configuration model

Model	Description
Model 2 (Edge – Core)	 Model 2 is a shape of a distributed cloud in which the edge cloud and the core cloud are configured together. A cloud service is functionally reconfigured and is executed on both edge and core clouds by interworking. The edge cloud is configured for real-time service delivery. The edge cloud assists end devices by offloading cloud services or caching the data of cloud services.
Model 3 (Edge – Regional – Core)	 Model 3 is a shape of a distributed cloud in which edge, regional and core clouds are configured together. A cloud service is reconfigured and deployed to edge, regional and core clouds and is executed by interworking. This model is a combination of model 1 and model 2. This model provides cloud services efficiently by mitigating the traffic of the cloud service, caching data of the cloud service and by offloading cloud services for the CSC's end devices.

6.4 Deployment considerations of distributed cloud

This clause provides consideration aspects for the deployment of cloud services on a distributed cloud. These consideration aspects include:

– infrastructure considerations of distributed cloud;
– network considerations of distributed cloud;
– service considerations of distributed cloud;
– management considerations of distributed cloud; and
– security considerations of distributed cloud.

6.4.1 Infrastructure considerations of distributed cloud

Infrastructure in a distributed cloud is heterogeneous and geographically distributed. Thus, consideration aspects are as follows:

– variety of physical resources, which have different hardware structure and instruction, for pooling the resources and deploying cloud services execution efficiently;
– energy efficient resources and power consumption control for edge cloud with small resource capacity; and
– infrastructure automatic provision, configuration and updating, as well as monitoring functionalities for providing a single system view to CSCs.

6.4.2 Network considerations of distributed cloud

The network in a distributed cloud supports connecting distributed cloud resources in broad areas among core, regional and edge clouds and is aware of cloud service. Thus, network considerations are as follows:

– broad network connectivity of distributed cloud resources among edge, regional and core clouds for managing resources and providing cloud service efficiently; and
– deployment of virtual network functions to edge cloud for controlling network on-demand and being aware context of cloud service.

6.4.3 Service considerations of distributed cloud

Services in a distributed cloud have various types based on the resource capacity of core, regional and edge clouds and on the CSC's demands. Thus, service considerations are as follows:

– the scale of a cloud service for deploying cloud services in different-scale edge, regional and core clouds; and

– automatic cloud service delivery for supporting the mobility of CSC's rapidly.

6.4.4 Management considerations of distributed cloud

Management in a distributed cloud has a global view and a local view of operations, and administration for distributed cloud resources and services. Thus, management considerations are as follows:

– global management of both distributed cloud resources and cloud services for interworking among core, regional and edge clouds; and

– provisioning, operation and administration of distributed cloud resources and cloud services.

6.4.5 Security considerations of distributed cloud

Security in a distributed cloud has adaptive security control for core, regional and edge clouds. Thus, security considerations are as follows:

– identification and authentication of CSCs using multiple distributed cloud infrastructures at any distributed cloud;

– different scales of security functions, such as availability and data integrity, based on the resource capacity of core, regional and edge clouds; and

– different security suites for confidentiality, policy and key management appropriate to heterogeneous distributed cloud resources.

7 High-level requirements for distributed cloud

7.1 Infrastructure requirements for distributed cloud

– **high scalability**: It is required that a distributed cloud provide distributed cloud resources with scale-out to edge, regional and core clouds to satisfy a large number of demands for cloud services;

– **high reliability**: It is required that a distributed cloud provide redundant deployment of cloud services among edge, regional and core clouds against catastrophic events;

– **low power consumption**: It is required that a distributed cloud provide energy-efficient distributed cloud resources for low power consumption at an edge cloud in order to save power of the edge cloud;

– **adaptive resource composition**: It is recommended that a distributed cloud provide adaptive resource composition of the distributed cloud among edge, regional and core clouds;

NOTE 1 – Adaptive resource composition refers to preparation of distributed cloud resources appropriately to support changes of a CSC's condition, such as environmental changes by the CSC's mobility.

– **automatic infrastructure provision**: It is recommended that a distributed cloud provide automatic setup of infrastructure, including hardware initiation, network configuration and software installation;

– **heterogeneous devices access**: It is recommended that a distributed cloud provide heterogeneous access mechanisms for end devices to enrich cloud services.

NOTE 2 – Examples of heterogeneous access mechanisms are Wi-Fi, Bluetooth, wireless sensor network (WSN) and radio access network (RAN).

7.2 Network requirements for distributed cloud

– **low latency**: It is required that a distributed cloud provide network resources to support low latency for cloud services in edge clouds;

NOTE 1 – Examples of network resources are access point, switch, router and gateway.

– **on-demand network traffic control**: It is required that a distributed cloud provide on-demand network traffic control to mitigate congested network links among core, regional and edge clouds by reallocating routing paths and allocating bandwidth;

NOTE 2 – The network bandwidth utilization inside a distributed cloud is substantially reduced with on-demand network traffic control.

– **service routing**: It is required that a distributed cloud support service routing for provisioning cloud service flowing to CSCs;

NOTE 3 – Service routing is a unified service supporting platforms built on the distributed service networking (DSN). It supplies the service registration, publication, discovery, triggering and access mechanisms, and enhanced capabilities to optimize the service. [b-ITU-T Y.2085]

– **context awareness**: It is required that a distributed cloud provide discovery of context information for deploying and delivering cloud service requests to the best location among core, regional and edge clouds;

NOTE 4 – Discovery of context information is enabled by network functions.

– **high-speed network connectivity**: It is recommended that a distributed cloud provide high-speed network connectivity to satisfy significantly higher data rates and data transportation among core, regional and edge clouds;

– **reliable network connectivity**: It is recommended that a distributed cloud provide reliable network connectivity for seamless network links with low error rates and fast connection recovery from failures among core, regional and edge clouds;

– **network virtualization**: It is recommended that a distributed cloud support network virtualization for dynamic network deployment;

NOTE 5 – Network virtualization is a technology that enables the creation of logically isolated network partitions over shared physical networks so that heterogeneous collections of multiple virtual networks can simultaneously coexist over the shared networks. This includes the aggregation of multiple resources in a provider and appearing as a single resource. [b-ITU-T Y.3011]

– **network services delivery**: It is recommended that a distributed cloud provide network services delivery wherever CSC's use cloud services.

NOTE 6 – Network service delivery includes virtualized network functions of switching, tunnelling, traffic analysis, and security such as load balancer, firewall and intrusion detection.

7.3 Service requirements for distributed cloud

– **service mobility**: It is required that a distributed cloud provide service mobility for supporting service level agreements (SLAs);

NOTE 1 – For service mobility, the CSCs' location detection and delivery of corresponding cloud services to the suitable distributed cloud resource automatically are needed for fast response time.

– **lightweight service**: It is required that a distributed cloud provide lightweight cloud services for low power consumption resources at edge clouds;

– **context information update**: It is required a distributed cloud support the updating of the associated context information periodically or aperiodically;

NOTE 2 – See clause 6.2 for context information.

– **caching of cloud service image**: It is required that a distributed cloud provide caching of cloud service images;

NOTE 3 – Frequently used cloud service images need to be cached in a regional cloud to deploy cloud service quickly to an edge cloud.

– **service migration**: It is required that a distributed cloud provide service migration from one distributed cloud resource to another one;

NOTE 4 – Service migration refers to running cloud services reallocated to another distributed cloud resource by taking a snapshot.

– **agile service**: It is recommended that a distributed cloud provide rapid development and delivery of cloud services to distributed cloud resources to support various CSC's requests;

– **automatic service displacement**: It is recommended that a distributed cloud provide cloud service displacement to deploy, maintain and upgrade automatically based on SLAs;

– **autonomous cloud service provisioning**: It is required a distributed cloud provide autonomous cloud service provisioning to initially launch the cloud service by using context information for fast provisioning of distributed cloud resources;

NOTE 5 – Autonomous cloud service provisioning refers to deploying and providing cloud services on edge clouds without intervention of global management in the core cloud by using context information in edge or regional clouds.

– **massive data handling on edge cloud**: It is recommended that a distributed cloud provide massive data handling on edge clouds to reduce the interaction between core/regional clouds and edge clouds.

NOTE 6 – Data handling on edge clouds includes filtering and delivery process to prevent noise from multiple end devices, and batched data delivery to core or regional clouds, respectively.

7.4 Management requirements for distributed cloud

– **global management**: It is required that a distributed cloud provide global management of distributed cloud resources collected from core, regional and edge clouds;

NOTE 1 – Core cloud aggregates information of distributed cloud resources, has global knowledge and provides cloud services appropriately to meet CSC's requirements.

– **real-time service management**: It is required that a distributed cloud provide management for real-time cloud services by finding feasible distributed cloud resources, predicting cloud service latency and scheduling cloud services;

– **heterogeneous resource management**: It is required that a distributed cloud provide management of heterogeneous distributed cloud resources to accommodate and utilize distributed cloud resources easily and efficiently;

NOTE 2 – Examples of heterogeneous distributed cloud resources includes different capacity servers, different types (block, object, file) of storages and different speeds of network devices.

– **end-device connectivity management**: It is required that a distributed cloud provide management of network connectivity to end devices supporting various access protocols to control network latency and bandwidth;

– **context information management**: It is required that a distributed cloud provide management of context information to support service routing and context awareness of the distributed cloud;

– **synchronization management**: It is required that a distributed cloud provide synchronization management for the status of cloud services and distributed cloud resources to perform global management accurately.

7.5 Security requirements for distributed cloud

– **resource isolation and protection**: It is recommended that a distributed cloud provide isolation and protection of distributed cloud resources and cloud services for tenants to guarantee security;

– **adaptive security function control**: It is recommended that a distributed cloud provide adaptive security functions to meet a CSC's requirements with different resource capacity among core, regional and edge clouds;

NOTE 1 – Examples of security function include encryption, decryption, key management, authentication and policy management.

– **adaptive security suites control**: It is recommended that a distributed cloud provide adaptive security suites to apply the suites on different resource capacities among core, regional and edge clouds.

NOTE 2 – Examples of security suites in case of encryption include data encryption standard (DES), advanced encryption standard (AES), international data encryption algorithm (IDEA) and Rivest, Shamir, Adleman (RSA).

8 Security considerations related to ITU-T Recommendations

It is recommended that the security framework for cloud computing described in [b-ITU-T X.1601] be considered for the distributed cloud. [b-ITU-T X.1601] analyses security threats and challenges in the cloud computing environment and describes security capabilities that could mitigate these threats and meet security challenges.

It is recommended that the guidelines for the operational security of cloud computing described in [b-ITU-T X.1642] be considered for the distributed cloud. [b-ITU-T X.1642] clarifies the security responsibilities between CSPs and CSCs, and analyses the requirements and categories of security metrics of operational security for cloud computing.

It is recommended that the security framework for the IoT based on the gateway model described in [b-ITU-T X.1361] be considered for edge clouds in the distributed cloud. In particular, [b-ITU-T X.1361] analyses security threats to the IoT gateway and to the network and describes security capabilities for gateways and the network that address and mitigate these security threats and challenges.

Appendix I

General use cases for distributed cloud

(This appendix does not form an integral part of this Recommendation.)

This appendix identifies use cases of distributed cloud. The table below shows the template used for the description of the use cases.

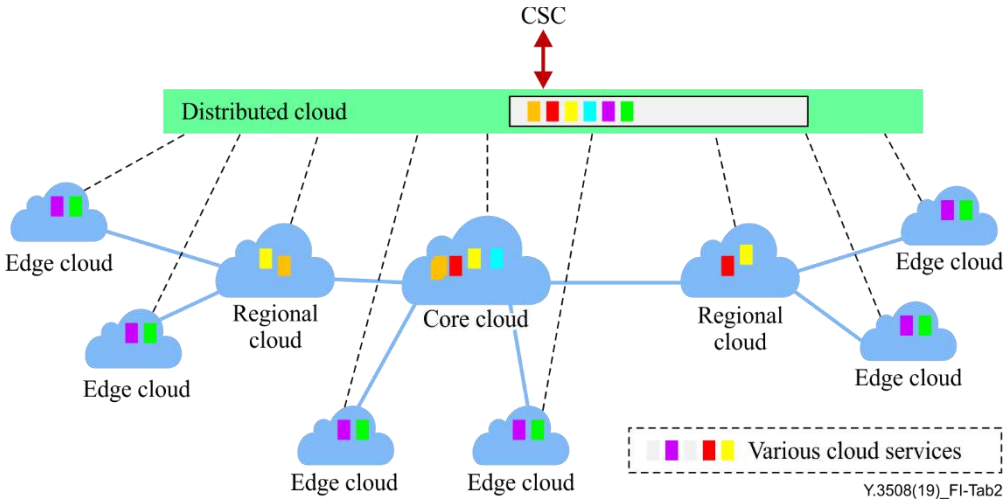
I.1 Use case template

Table I.1 – Template for the description of a use case

Use case	
Name	Title of use case.
Abstract	Overview and features of use case.
Figure	Figure to present the use case. (A unified modeling language (UML)-like diagram is suggested for clarifying relations between roles).
Pre-conditions (optional)	Pre-conditions represent the necessary conditions or use cases that should be achieved before starting the described use case. (Note)
Post-conditions (optional)	As the same for pre-condition, the post-condition describes conditions or use cases that will be carried out after the termination of a currently described use case.
Requirements	The title of requirements derived from the use case. For example: – Large-scale migration.
NOTE – As dependency may exist among different use cases, pre-conditions and post-conditions are introduced to help understand the relationships among use cases.	

I.2 General use case

Table I.2 – General use case of distributed cloud

Use case	
Name	General use case of distributed cloud.
Description	The use case describes the scenarios for the CSC to use a published cloud service. The cloud service has already been published by a CSP and can be browsed through the product catalogue provided by the CSP. The CSC subscribes the cloud service with various requirements, for example, different requirements for service capacity and network latency. The distributed cloud realizes service provisioning to provide cloud service on appropriate core, regional, or edge cloud, according to the CSC's subscription.
Figure	
Pre-conditions (optional)	
Post-conditions (optional)	– The used service should be kept available during the whole invocation. – The SLA should be met for CSC.
Requirements	– High scalability (See clause 7.1) – High reliability (See clause 7.1) – Low power consumption (See clause 7.1) – Low latency (See clause 7.2) – On-demand network traffic control (See clause 7.2)

Appendix II

Use cases for configuration of distributed cloud

(This appendix does not form an integral part of this Recommendation.)

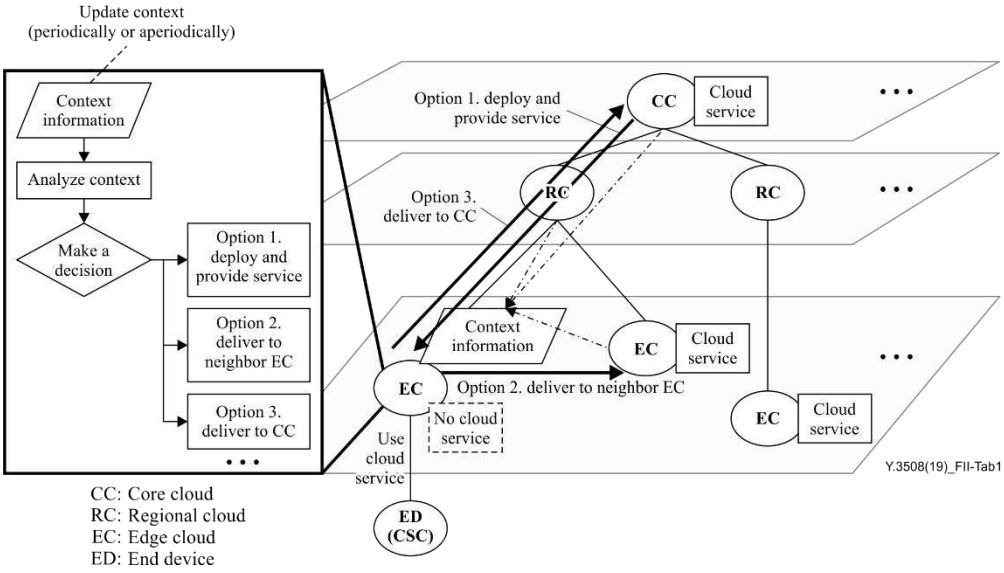
This appendix identifies use cases for configuration of distributed cloud.

II.1 Autonomous cloud service provisioning on distributed cloud

Table II.1 – Autonomous cloud service provisioning on distributed cloud

Use case	
Name	Autonomous cloud service provisioning on distributed cloud.
Abstract	This use case describes the autonomous feature for provisioning a cloud service on distributed cloud. The distributed cloud supports dynamic service provisioning by utilizing core cloud (CC), regional cloud (RC) and edge cloud (EC). EC mainly supports low latency to provide a cloud service. For EC, it is sometimes hard to provide the cloud service due to various reasons (e.g., limited capacity of EC, initially requested service, energy saving). In the case where EC is not ready to provide the corresponding cloud service, EC is required to make a decision to provide the service to the CSC as rapidly as possible. For fast decisions required by time sensitive services in EC, a request to a centralized point (e.g., core cloud and regional cloud) is not appropriate due to network traversal time; the request should be handled in the EC itself. To support autonomous cloud service provisioning on EC, associated context information is required. Associated context information is necessary to be updated on EC periodically and aperiodically. To avoid synchronization burden, associated context information is summarized and updated (e.g., calculating average, grouping value, choosing representative value). To avoid frequent transfer data to the core/regional cloud by edge cloud, the edge cloud filters and deliver to prevent noise from multiple end devices and deliver batched data to core or regional cloud. In conclusion, autonomous provisioning is a main feature that differentiates conventional cloud and distributed cloud. Through the feature, CC, RC and EC on distributed cloud are loosely coupled. The feature also supports fast cloud service provisioning on the distributed cloud. Autonomous provisioning is done by associated context information updated periodically and aperiodically. NOTE – Examples of decision: 1) Deploying the cloud service and provide the cloud service on the EC, 2) Delivering the request to neighbour EC, 3) Delivering the request to the CC, etc.

Table II.1 – Autonomous cloud service provisioning on distributed cloud

Use case	
Figure	
Pre-conditions (optional)	Associated context information is updated periodically or aperiodically.
Post-conditions (optional)	
Requirements	– Adaptive resource composition (See clause 7.1) – Context information update (See clause 7.3) – Autonomous cloud service provisioning (See clause 7.3) – Massive data handling on edge cloud (See clause 7.3) – Context information management (See clause 7.4)

II.2 Customer-oriented cloud service provisioning on distributed cloud

Table II.2 – Customer-oriented cloud service provisioning on distributed cloud

Use case	
Name	Customer-oriented cloud service provisioning on distributed cloud.
Abstract	This use case describes customer-oriented service deployment on distributed cloud. A main benefit of distributed cloud is provisioning of a cloud service in close proximity to CSC. For the provisioning, methods to support customer-oriented cloud service provisioning on distributed cloud are needed and is called service routing. The service routing includes packet routing, service awareness, etc. By service awareness on distributed cloud, a cloud service is deployed on a cloud in close proximity to the CSC or the request of a cloud service is delivered to another cloud. Accordingly, the service routing on distributed cloud enables: – scaling or migrating a cloud service for supporting mobility as shown in figure <An example of scaling or migrating a cloud service for supporting mobility>; – deploying and providing a cloud service for low response time as shown in figure < An example of deploying and providing a cloud service for low response time>; and

Table II.2 – Customer-oriented cloud service provisioning on distributed cloud

Use case	
	– delivering request of a cloud service to neighbour edge cloud as shown in figure <An example of delivering a cloud service to neighbour edge cloud>. Finally, customer-oriented service provisioning (i.e., service routing) method is highly required on distributed cloud in order to improve cloud service QoS (e.g., response time, network bandwidth, mobility). NOTE – Provisioning of a cloud service in close proximity to cloud service customer depends on condition of CSC (e.g., location, QoS level) and condition of surrounding CSC (e.g., availability of edge cloud, capacity of edge cloud, network congestion).

Table II.2 – Customer-oriented cloud service provisioning on distributed cloud

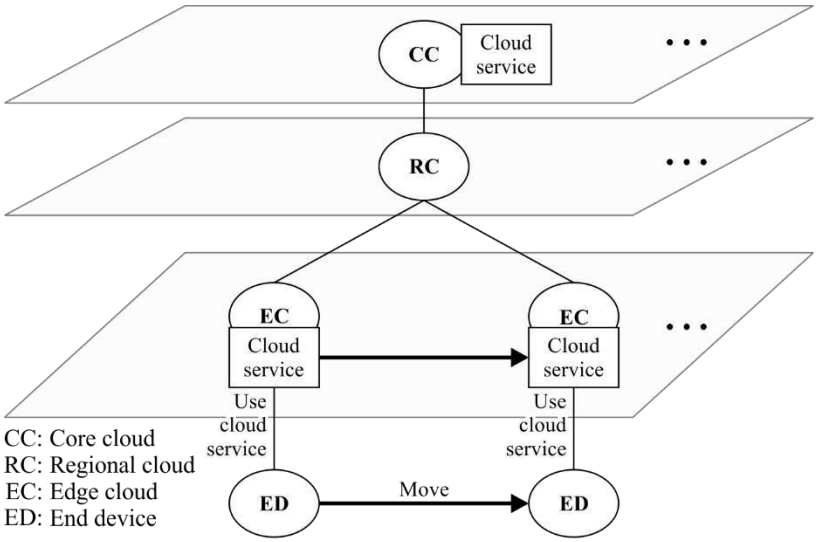
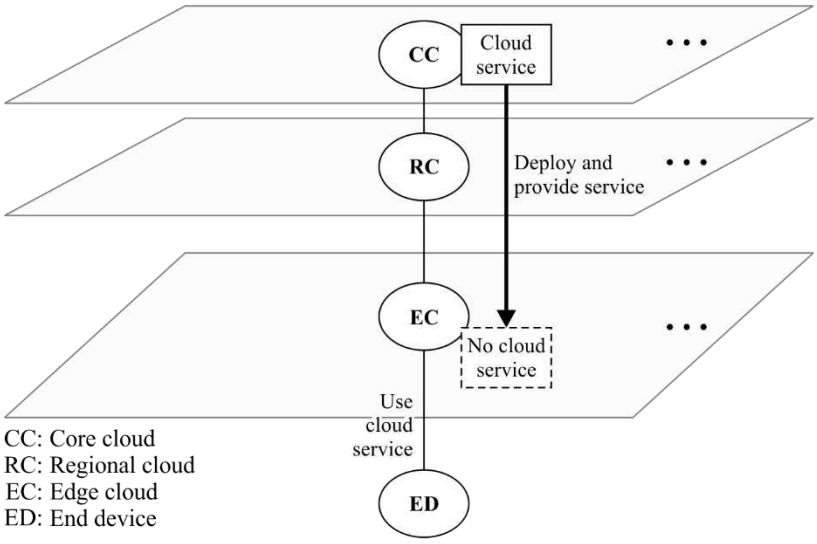
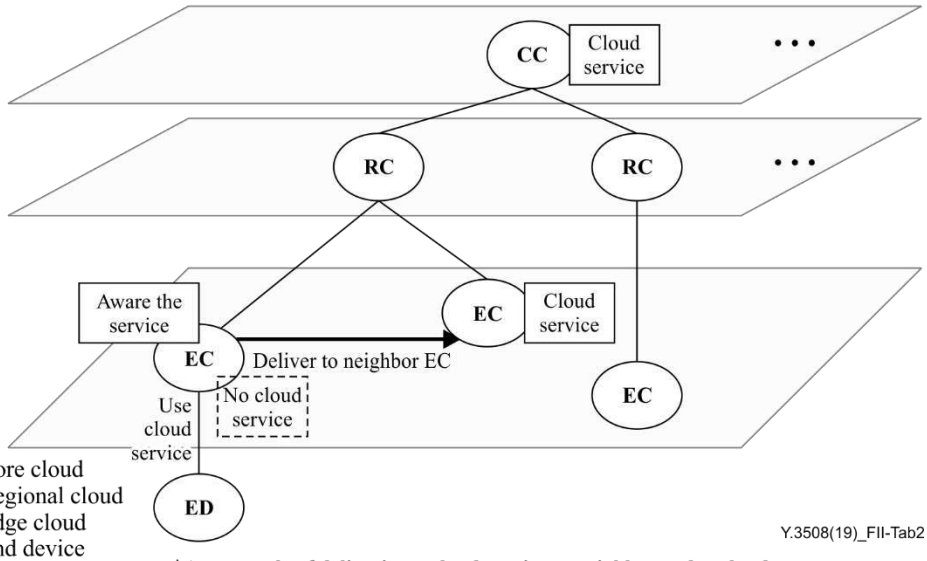
Use case	
Figure	 **An example of scaling or migrating a cloud service for supporting mobility**  **An example of deploying or providing a cloud service for low response time**  **An example of delivering a cloud service to neighbour edge cloud**

Table II.2 – Customer-oriented cloud service provisioning on distributed cloud

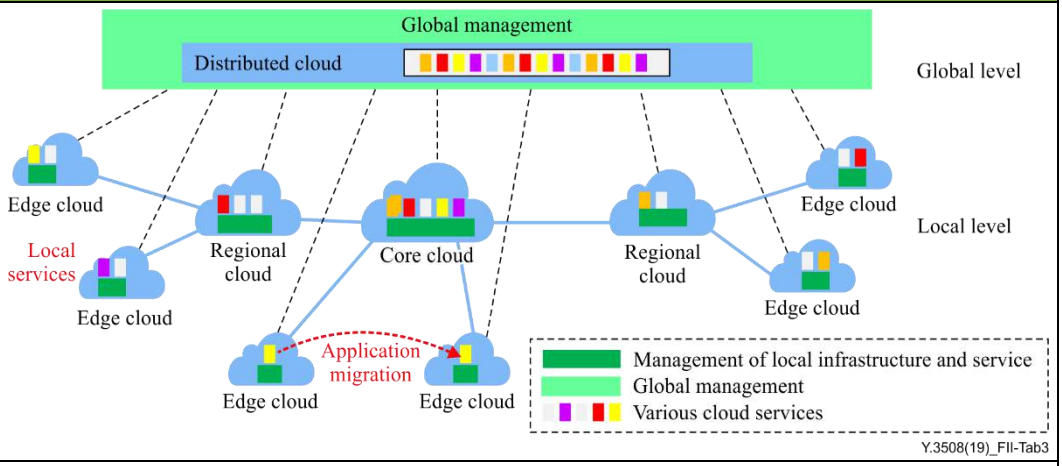
Use case	
Pre-conditions (optional)	
Post-conditions (optional)	
Requirements	– Adaptive resource composition (See clause 7.1) – Service routing (See clause 7.2) – Network services delivery (See clause 7.2) – Context awareness (See clause 7.2) – Context information management (See clause 7.4)

II.3 Distributed cloud infrastructure and service management

Table II.3 – Distributed cloud infrastructure and service management

Use case	
Name	Distributed cloud infrastructure and service management
Description	This use case describes the distributed cloud infrastructure and service management. Distributed cloud infrastructure includes processing, storage, networking and other hardware resources as well as software assets. Distributed cloud infrastructure management is the management of hardware resources and software assets of distributed cloud. Distributed cloud includes core, regional and edge clouds, which are different in size, hardware types and software. For example, a distributed cloud resource may use a graphics processing unit (GPU) or field-programmable gate array (FPGA) hardware for AR/VR scenarios and microprocessor-based server instead of x86 server for some specified application. These resources are distributed across various environments. Thus, resources need to be isolated and protected in secure manner. Distributed cloud provides flexible and agility network connectivity for core, regional and edge clouds. The network connection can be changed on demand or based on policy, such as active-standby policy. The ultimate objective of distributed cloud is to provide distributed cloud services for the customers. The distributed cloud encapsulates the capabilities of distributed cloud infrastructure into various cloud services for the end customers. Distributed cloud is a hierarchical system, in which each core cloud, regional cloud and edge cloud could manage its local infrastructure and service, and the infrastructure and service of the whole distributed cloud could be unified managed and coordinated by the distributed cloud management.

Table II.3 – Distributed cloud infrastructure and service management

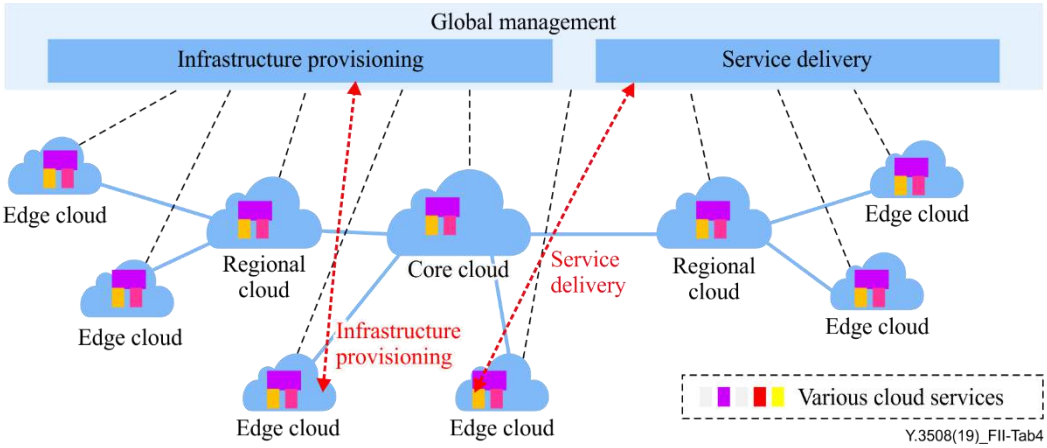
Use case	
Figure	
Pre-conditions (optional)	
Post-conditions (optional)	
Requirements	– Heterogeneous device access (See clause 7.1) – Global management (See clause 7.4) – Heterogeneous resource management (See clause 7.4) – End device connectivity management (See clause 7.4) – Resource isolation and protection (See clause 7.5)

II.4 Distributed cloud infrastructure and service provisioning

Table II.4 – Distributed cloud infrastructure and service provisioning

Use case	
Name	Distributed cloud infrastructure and service provisioning.
Description	This use case describes the distributed cloud infrastructure and service provisioning. Distributed cloud can provision infrastructure and deliver service among core, regional and edge cloud. The distributed cloud infrastructure contains various hardware and software, including servers, storage, network devices and software. The edge cloud especially is resource-constrained due to space and power. The infrastructure provision process includes hardware initiation, network configuration and software installation. After provisioning, the services including security functions and suites can be provided based on the infrastructure. Also, if a cloud service needs to use an edge cloud resource, it is reconfigured or developed to run on the edge cloud with small capacity and heterogeneous resources. The distributed cloud infrastructure can be maintained and upgraded by distributed cloud management. The provisioning is a policy-based process so it can be done automatically on distributed cloud resources. Once the distributed cloud infrastructure has been provisioned, the cloud service should be deployed and delivered rapidly to the suitable distributed cloud resource by high-speed and reliable network connectivity based on service's SLA, such as required resources, maximum latency, required or useful services, etc. The deployed service can be maintained and upgraded based on global management. For accurate global management, status information of cloud service and distributed cloud resource are synchronized from edge/regional cloud to core cloud.

Table II.4 – Distributed cloud infrastructure and service provisioning

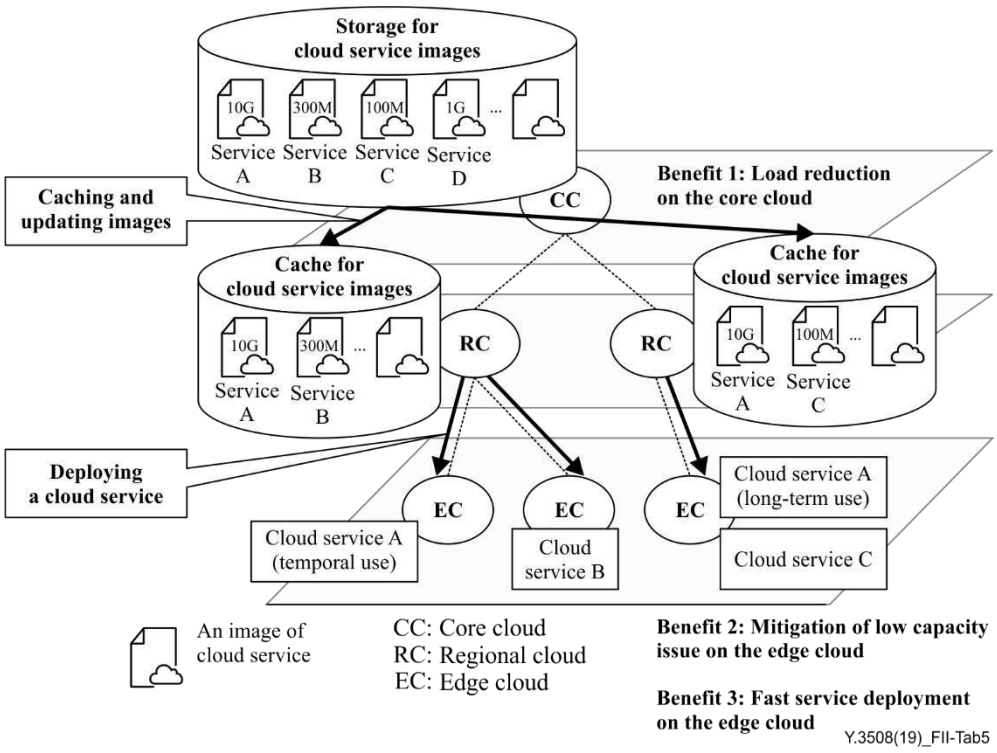
Use case	
Figure	
Pre-conditions (optional)	
Post-conditions (optional)	
Requirements	– Automatic infrastructure provision (See clause 7.1) – High speed network connectivity (See clause 7.2) – Reliable network connectivity (See clause 7.2) – Network virtualization (See clause 7.2) – Network services delivery (See clause 7.2) – Agile service (See clause 7.3) – Lightweight service (See clause 7.3) – Automatic service displacement (See clause 7.3) – Synchronization management (See clause 7.4) – Adaptive security function control (See clause 7.5) – Adaptive security suites control (See clause 7.5)

II.5 Hierarchical caching of cloud service images

Table II.5 – Hierarchical caching of cloud service images

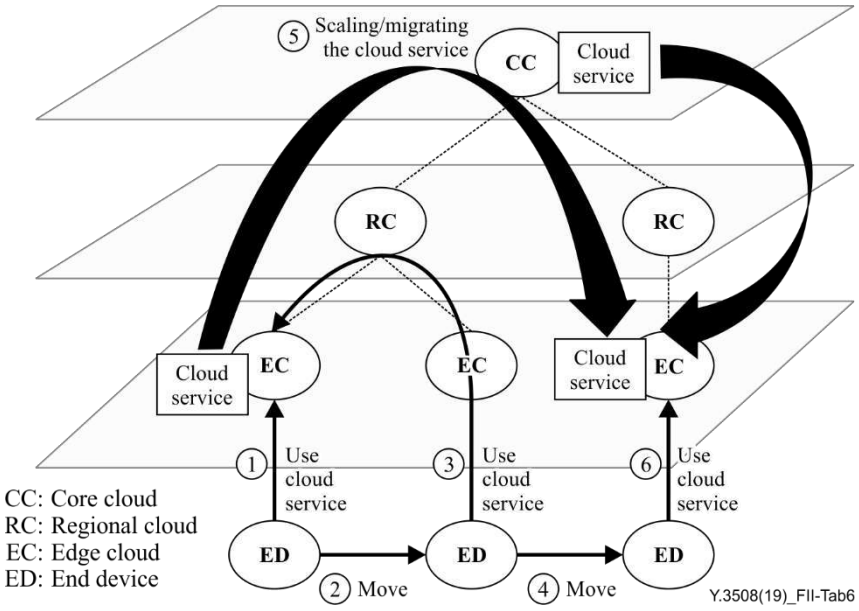
Use case	
Name	Hierarchical caching of cloud service images.
Abstract	This use case shows an example of hierarchical caching of cloud service images. The core cloud mainly manages cloud service images; the size of a cloud service image varies from tens of megabytes to hundreds of gigabytes. A cloud service image is needed to run a cloud service. For example, when a cloud service is run on the edge cloud, the image is copied from the core cloud by request. Thus, depending on the number of requests, the core cloud can be overloaded. In addition, copying a cloud service image from the core cloud to the edge cloud is inefficient. Also, the edge cloud has relatively lower storage capacity than the core cloud or the regional cloud. It is inefficient for the edge cloud to maintain all cloud service images.

Table II.5 – Hierarchical caching of cloud service images

Use case	
	Therefore, hierarchical caching is needed. Cloud service images are cached on the regional cloud according to the initial request or frequency. It is helpful to reduce the load on the core cloud because multiple regional clouds handle the requests respectively. It also mitigates the capacity issue on the edge cloud, and it provides fast service deployment to support real-time performance by reducing latency than from the core cloud.
Figure	
Pre-conditions (optional)	
Post-conditions (optional)	
Requirements	– High speed network connectivity (See clause 7.2) – Caching of cloud service image (See clause 7.3) – Real-time service management (See clause 7.4)

II.6 High mobility support on distributed cloud

Table II.6 – High mobility support on distributed cloud

Use case	
Name	High mobility support on distributed cloud.
Abstract	This use case illustrates an example of high mobility support on distributed cloud. A typical mobility support environment follows a method of modifying the packet routing path while the location of the service is fixed. On the distributed cloud, the location of the service is different from the conventional cloud and is located near the user. Accordingly, the distributed cloud needs high mobility. As an example, the below figure shows two ways of mobility while an end device moves with different type of access. One way is that the regional cloud routes the packet to the previous edge cloud as shown in step 3 in the figure below. (It is also possible to route the cloud service to the current edge cloud.) Another way is that the core cloud routes the cloud service to the edge cloud near the end device by scaling or migrating the cloud service with high-speed and reliable network connectivity as shown in step 5 and 6. The cloud service is from the previous edge cloud or the core cloud. Therefore, to efficiently support high mobility on the distributed cloud, both ways are selected based on service level agreement (SLA) for the cloud service. SLA includes latency, quality of service, etc.
Figure	
Pre-conditions (optional)	
Post-conditions (optional)	
Requirements	– Heterogeneous device access (See clause 7.1) – High speed network connectivity (See clause 7.2) – Reliable network connectivity (See clause 7.2) – Context awareness (See clause 7.2) – Service mobility (See clause 7.3) – Service migration (See clause 7.3) – Context information management (See clause 7.4)

Appendix III

A comparison of distributed cloud with related technology

(This appendix does not form an integral part of this Recommendation.)

This Appendix identifies a comparison of the distributed cloud, edge computing, fog computing, multi-access edge computing and cloudlet. There are various technologies related to the edge of the network, such as edge computing, fog computing, cloudlet and multi-access edge computing. The edge-related technologies fully or partially utilize cloud computing technology. In the perspective of multi-cloud, distributed cloud extends a cloud to the edge of the network. Accordingly, the distributed cloud and the edge-related technologies definitely have a common point. Thus, it is necessary to compare key features and show the coverage of them among the distributed cloud and the edge related technologies. In this Appendix, the coverage of key features among the distributed cloud and the edge-related technologies are analysed and illustrated as follow:

– **Cloud computing** focuses on non-real-time services and supports periodic maintenance and service decision – making while distributed cloud extends the cloud computing capabilities to the edge and supports real-time smart processing and execution of local services. Distributed cloud takes core, regional and edge as a whole and closely interacts with one another. Resource-constrained, unreliable or bandwidth-limited network connections, or applications that demand very high bandwidth, low latency, or widespread compute capacity across many sites are considered by distributed cloud but not involved with cloud computing.

– **Edge computing** is performed on an open platform at the edge of the network near things or data sources, integrating network, computing, storage and application core capabilities and providing edge intelligent services. Edge computing meets the requirements of industrial digitalization for agile connections, real-time services, data optimization, smart application, security and privacy protection. Local devices and their capabilities are a part of edge computing while distributed cloud is not involved with local devices. The major scenario of edge computing focuses on IoT, but distributed cloud has many scenarios beside IoT. Big data analytics is considered as one of the key capabilities for edge computing while distributed cloud treats it as a service which it's carried on.

• **Fog computing** is a horizontal, physical or virtual resource paradigm that resides between smart end-devices and traditional cloud or data centres. Fog computing supports vertically isolated, latency-sensitive applications by providing ubiquitous, scalable, layered federated and distributed computing, storage and network connectivity. Rather than a substitute, fog computing often serves as a complement to cloud computing. Fog computing is mainly for IoT scenarios while distributed cloud has many scenarios beside IoT. It is similar to edge computing where the local devices are involved for fog computing but the infrastructure of distributed cloud only includes data centres.

– Multi-access edge computing **(MEC)** offers cloud-computing capabilities and an IT service environment at the edge of the network and provides ultra-low latency and high bandwidth as well as real-time access to radio network information that can be leveraged by applications. MEC is mainly for mobile scenarios and is extending to fixed mobile convergence scenarios. The scope of MEC is involved in distributed cloud.

– **Cloudlet** can be viewed as a "data centre in a box", which represents the middle tier of a three-tier hierarchy "mobile or IoT device – cloudlet – cloud", whose goal is to bring the cloud closer. It is mainly for scenarios of convergence of mobile and cloud computing. The scope of cloudlet is involved in distributed cloud.

Bibliography

[b-ITU-T X.1361] Recommendation ITU-T X.1361 (2018), *Security framework for the Internet of things based on the gateway model*.

[b-ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing*.

[b-ITU-T X.1642] Recommendation ITU-T X.1642 (2016), *Guidelines for the operational security of cloud computing*.

[b-ITU-T Y.2085] Recommendation ITU-T Y.2085 (2016), *Distributed service networking service routing*.

[b-ITU-T Y.3011] Recommendation ITU-T Y.3011 (2012), *Framework of network virtualization for future networks*.

Cloud computing infrastructure requirements

Recommendation ITU-T Y.3510

(02/2016)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Summary

Recommendation ITU-T Y.3510 provides requirements for cloud computing infrastructure; these include the essential capabilities for processing, storage and networking resources, as well as the capabilities of resource abstraction and control.

Keywords

Capability, cloud computing, control, infrastructure, networking, processing, resource abstraction, storage.

Table of Contents

1 Scope

This Recommendation identifies requirements for cloud infrastructure to support cloud services.

The scope of this Recommendation includes:

– an overview of cloud computing infrastructure;
– requirements for processing resources;
– requirements for networking resources;
– requirements for storage resources;
– requirements for resource abstraction and control.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing.*

[ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary*.

[ITU-T Y.3501] Recommendation ITU-T Y.3501 (2013), *Cloud computing framework and high-level requirements.*

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014) | ISO/IEC 17789:2014, *Information technology – Cloud computing – Reference architecture.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 cloud computing [ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

3.1.2 cloud service [ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface

3.1.3 cloud service customer [ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

NOTE – A business relationship does not necessarily imply financial agreements.

3.1.4 cloud service provider [ITU-T Y.3500]: Party which makes cloud services available.

3.1.5 emergency telecommunications (ET) [b-ITU-T Y.2205]: ET means any emergency related service that requires special handling from the NGN relative to other services. This includes government authorized emergency services and public safety services.

3.1.6 emergency telecommunications service (ETS) [b-ITU-T E.107]: A national service providing priority telecommunications to ETS authorized users in times of disaster and emergencies.

3.1.7 logical resource [b-ITU-T Y.3011]: An independently manageable partition of a physical resource, which inherits the same characteristics as the physical resource and whose capability is bound to the capability of the physical resource.

NOTE – "independently" means mutual exclusiveness among multiple partitions at the same level.

3.1.8 management system [b-ITU-T M.60]: A system with the capability and authority to exercise control over and/or collect management information from another system.

3.1.9 virtual resource [b-ITU-T Y.3011]: An abstraction of physical or logical resource, which may have different characteristics from the physical or logical resource and whose capability may not be bound to the capability of the physical or logical resource.

NOTE – "different characteristics" means simplification or extension of the resource characteristics. "different characteristics" allows the virtual resource to expose access or control methods different from the original physical or logical resource.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 hypervisor: A type of system software that allows multiple operating systems to share a single hardware host.

NOTE – Each operating system appears to have the host's processor, memory and other resources, all to itself.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CPU	Central Processing Unit
CSC	Cloud Service Customer
CSP	Cloud Service Provider
DFS	Distributed File System
DHT	Distributed Hash Table
DNS	Domain Name System
ET	Emergency Telecommunications
ETS	Emergency Telecommunications Service
I/O	Input/Output
iSCSI	Internet Small Computer System Interface
LAN	Local Area Network
NAS	Network Attached Storage
NFS	Network File System
NTP	Network Time Protocol
OS	Operating System
QoS	Quality of Service
SAN	Storage Area Network
SLA	Service Level Agreement
vCPU	virtual CPU
VI	Virtual Infrastructure
VM	Virtual Machine
VPN	Virtual Private Network

5 Conventions

In this Recommendation:

The keywords "is required" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "is prohibited" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Overview of cloud infrastructure

In this Recommendation, cloud infrastructure includes processing, storage, networking and other hardware resources as well as software assets.

Abstraction and control of physical resources are essential means to achieve the on-demand and elastic characteristics of cloud infrastructure. In this way, physical resources can be abstracted into virtual machines (VMs), virtual storages and virtual networks. The abstracted resources are controlled to meet cloud service customers' (CSCs) needs.

The main characteristics of cloud infrastructure are:

– Network centric: The cloud infrastructure consists of distributed resources including processing, storage and other hardware resources that are connected through the networks;

– On-demand resource provisioning: The cloud infrastructure dynamically provides resources according to CSCs' needs;

– Elasticity: The cloud infrastructure is capable of expanding or reducing its resources to accommodate the current workloads;

– High availability: The cloud infrastructure is capable of providing required resources under the conditions stated in the service level agreement (SLA);

– Resources abstraction: The underlying resources of cloud infrastructure (processing, storage, networking, etc.) are invisible to the CSCs.

NOTE – For high level cloud computing requirements, please refer to [ITU-T Y.3501].

7 Requirements for processing resources

Processing resources are used to provide essential capabilities for cloud services and to support other system capabilities, such as resource abstraction and control, management, security and monitoring.

The basic unit of allocation and scheduling of processing resources is a computing machine. A computing machine can be physical or virtual. The capability of a computing machine is typically expressed in terms of configuration, availability, scalability, manageability and energy consumption.

7.1 Physical machine requirements

The physical machine requirements include:

- It is recommended to support hardware resource virtualization.
- It is recommended to support horizontal scalability (e.g., adding more computing machines) and vertical scalability (e.g., adding more resources with a computing machine).
- It is recommended to use power optimization solutions to reduce energy consumption.

7.2 Virtual machine requirements

The virtual machine provides a virtualized and isolated computing environment for each guest operating system (OS).

The virtual machine requirement includes:

- It is required to support migration of virtual machines between different physical computing machines.

7.2.1 CPU virtualization

The central processing unit (CPU) virtualization allows running multiple virtual CPUs (vCPU) on a single physical CPU.

The CPU virtualization requirement includes:

- The virtual machine's vCPUs' computing capability can optionally be specified as a fraction of a physical CPU.

7.2.2 Memory virtualization

The memory virtualization includes memory allocation at the start of a virtual machine, memory utilization monitoring during virtual machine operation and memory release at the shutdown of a virtual machine.

The memory virtualization requirement includes:

- It is recommended that while a virtual machine is active, the hypervisor monitors memory usage and reallocates unused memory to other virtual machines dynamically.

7.2.3 Input/Output device virtualization

The Input/Output (I/O) virtualization allows division of the physical I/O device into several logical instances for use by different virtual machines.

The I/O device virtualization requirements include:

- It is required for the hypervisor to support I/O virtualization capabilities.
- It is required that a virtual machine is capable of using virtual I/O devices abstracted from the physical I/O devices.
- The number of virtual I/O devices is prohibited from being constrained by the number of physical I/O devices.
- The data of one virtual machine transferred through a shared physical I/O device is prohibited from being exposed to other virtual machines.
- Physical I/O devices can optionally be shared by multiple virtual machines.

7.2.4 Network interface virtualization

Network interface virtualization allows creating and deleting a virtual network interface for a guest virtual machine OS regardless of the number of physical network interfaces.

The network interface virtualization requirements include:

- It is recommended that a physical network interface can be virtualized into multiple virtual network interfaces.
- It is recommended that the virtual network interfaces from different virtual machines can be grouped into one virtual local network.

7.2.5 Duplication of virtual machine

The duplication of a virtual machine allows creating new virtual machines and virtual machine backup in the execution environment.

The duplication of a virtual machine requirement includes:

- A virtual machine can optionally be duplicated to create a new virtual machine with the same configuration.

7.2.6 Dynamic migration of virtual machine

The dynamic migration of a virtual machine is designed to provide service continuity and reliability dynamically.

The dynamic migration of virtual machine requirements include:

- It is required that the network configuration of migrated virtual machines remain unchanged after migration.
- It is recommended that cloud service providers (CSPs) support the dynamic migration of a virtual machine.

7.2.7 Static migration of virtual machine

The static migration of a virtual machine means moving the virtual machine between different physical machines which results in the operating system rebooting.

The static migration of a virtual machine requirement includes:

- It is required that CSPs support static migration.

7.2.8 Management automation

The management system may perform operations such as starting or stopping a virtual machine, rebooting a server and applying software updates automatically.

The management automation requirement with regard to virtual machines includes:

- It is recommended that CSPs automate provision, activation, deactivation and other operations over the lifetime of virtual machines.

7.3 Software resources provisioning requirements

The software resources include the software for building cloud infrastructure resource pools and the software in support of service implementation.

7.3.1 Automated provisioning and deployment

The automated provisioning and deployment of software resources can reduce provisioning time and the workload for deployment.

The automated provisioning and deployment requirements include:

- It is recommended that software resources (e.g., executable files, drivers, libraries, documents, icons, etc.) are packaged into encapsulated files, which can be provisioned and deployed automatically.
- It is recommended that software resources be automatically provisioned and deployed to target devices or platforms without operator intervention.

7.3.2 Unified software resource management

Unified software resource management includes capabilities for licence information registration, allocation, recovery, expiration notification and metering.

The unified software resource management requirement includes:

- It is recommended that CSPs manage software licences in a unified manner.

7.4 Time-sensitive services requirements

Time-sensitive services (e.g., real-time communications using voice and video media) requirements include:

- It is required to prioritize resource allocation to time-sensitive processing.
- It is required to apply clock settings best practices (e.g., based on the network time protocol (NTP) [b-IETF RFC 5905]).

8 Requirements for networking resources

Typically, there are several types of networks involved in cloud computing services delivery and composition, such as the intra-datacentre network and inter-datacentre network, as well as the access and core transport network, etc.

To illustrate the cloud computing network concepts described in this Recommendation, a generic network model, which supports cloud computing infrastructure, is shown in Figure 8-1.

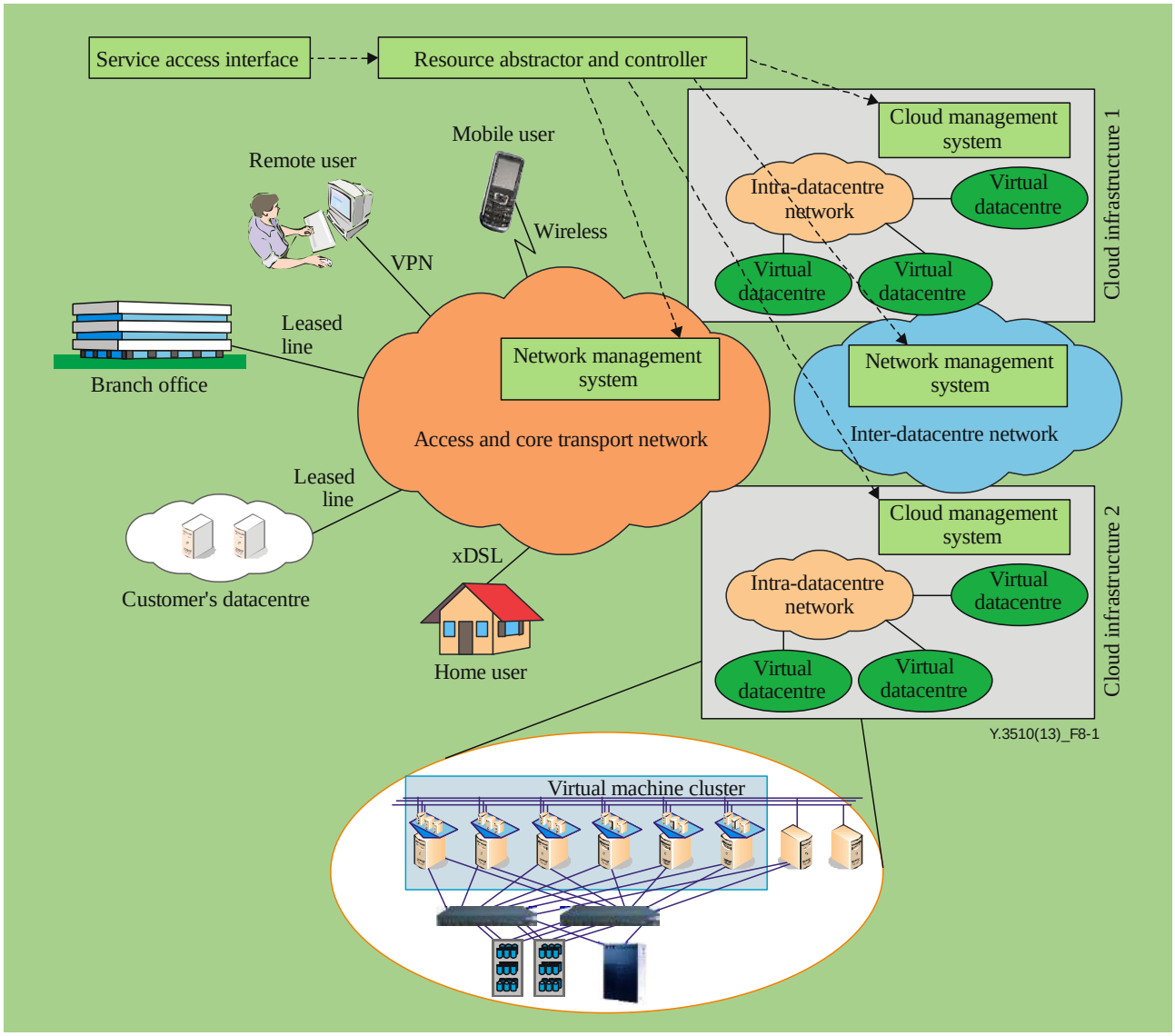


Figure 8-1 – Generic network model for cloud infrastructure

The generic network model shown in Figure 8-1 consists of the following blocks:

1) **Intra-datacentre network**: The network connecting local cloud infrastructures, such as the datacentre local area network used to connect servers, storage arrays and L4-L7 devices (e.g., firewalls, load balancers, application acceleration devices).

2) **Access and core transport network**: The network used by CSCs to access and consume cloud services deployed by the CSP.

3) **Inter-datacentre network**: The network interconnecting remote cloud infrastructures. These infrastructures may be owned by the same or different CSPs; an inter-datacentre network primarily supports the following two scenarios:
   – **Workload migration**, which means moving workloads from an enterprise datacentre to a CSP datacentre, or moving workloads from CSP to CSP (for resilience and maintenance).
   – **Server clustering** which allows transactions and storage replication for the business continuity.

Examples of inter-datacentre network models include:

1) private cloud datacentre to private cloud datacentre
2) private cloud datacentre to CSP datacentre
3) CSP datacentre to CSP datacentre.

NOTE 1 – For a description of a private cloud, please refer to [ITU-T Y.3500].

A centralized resource abstraction and control ensures the overall management of the cloud environment with:

a) Network management systems that are dedicated to network service providers. The processes supported by network management systems include management and maintenance of the network inventory and the configuration of network components, as well as fault management.

b) Cloud management systems are dedicated to CSPs. Cloud management systems support processes for maintenance, monitoring and configuration of cloud infrastructure resources.

NOTE 2 – Requirements for resource abstraction and control are provided in clause 10.

8.1 General requirements for networking resources

General requirements provided in this clause apply to networking resources of the access and core transport networks, intra-datacentre networks as well as inter-datacentre networks.

The general requirements for networking resources include:

- Networking resources (e.g., bandwidth, number of ports, network addresses) are required to be scalable;
- Networking resources are required to ensure services' performance and availability in order to meet SLA objectives;
- Networking resources are required to be able to adapt dynamically to the traffic generated by cloud services;
- Networking resources are required to support IPv4 and IPv6;
- Networking resources are recommended to support policy based control on flow by flow basis in a fine-grained manner.

8.2 Access and core transport network

The access and core transport network is used to connect the CSC to the CSP for the use of cloud services.

The access and core transport network requirement includes:

- It is recommended that the access and core transport network supports the delivery of cloud services in an optimal way in terms of performance, scalability and agility (e.g., through network programmability).

8.3 Intra-datacentre network

The intra-datacentre network is used to connect local datacentre cloud infrastructures, such as servers, storage arrays and L4-L7 devices (e.g., firewalls, load balancers, application acceleration devices).

The intra-datacentre network requirements include:

- The intra-datacentre network is recommended to provide appropriate means to cope with flexible network address space demands.
- The intra-datacentre network is recommended to provide elastic addressing for multi-tenant users.
- The intra-datacentre network is recommended to support different security policies for particular virtual machines.
- The intra-datacentre network is recommended to support different QoS policies for particular virtual machines.
- The intra-datacentre network is recommended to support the dynamic migration of virtual machines.
- The intra-datacentre network is recommended to support the traffic monitoring among virtual machines and network ports if needed.
- The intra-datacentre network is recommended to be able to provide multi-paths for particular multi-tenant users.
- The intra-datacentre network is recommended to support the establishment of a logical network among virtual machines.
- The intra-datacentre network is recommended to support public IP address and private IP address mapping.
- The intra-datacentre network is recommended to support dynamic DNS and static DNS for multi-tenant users.
- The intra-datacentre network is recommended to support network services (e.g., firewall, load balancer, virtual private network (VPN) services) for multi-tenant users.

8.4 Inter-datacentre network

The inter-datacentre network is used to interconnect different cloud infrastructures. These infrastructures may be owned by the same or different CSPs.

The inter-datacenter network requirements include:

- The inter-datacentre network is recommended to support the scalability to match the demand level of public and private clouds.
- The inter-datacentre network is recommended to be resilient;
- The inter-datacentre network is recommended to deal with virtual machine network addresses overlapping;
- The inter-datacentre network is recommended to support different logical networks.

9 Requirements for storage resources

This clause provides requirements for storage resources.

NOTE – An example of a reference model for storage resources is provided in Appendix I.

9.1 Storage space

The storage space requirement includes:

- It is required to support dynamic storage space expansion.

9.2 Storage interface

The storage interface requirements include:

- The storage resources are required to support either block storage interfaces or file system interfaces.
- The storage resources are recommended to support object storage accessed via web service data path interfaces.
- The storage resources are recommended to support structured data-sharing access interfaces.
- The storage resources can optionally support multiple types of interfaces.

9.3 Storage management

The storage management requirements include:

- It is required to provide the capabilities for user authentication and authorization.
- It is required to provide management capabilities for storage resources.
- It is required to provide basic configuration capabilities, including storage domain configuration, file system namespace configuration, storage resources configuration and local file system configuration.
- It is recommended to provide performance monitoring and statistics (e.g., disk I/O speed, disk space usage, CPU utilization, memory utilization, job completion).
- It is recommended to support alert capabilities, e.g., for event and trouble reporting.
- It is recommended to provide replication, archive and retention capabilities.

9.4 Storage availability

The storage availability requirements include:

- It is required to monitor data loss or failure.
- It is recommended to provide data backup and data recovery.
- It is recommended to provide data verification capabilities.
- It is recommended to support access through legitimate channels without time constraints, as well as the geographical constraints.
- It is recommended to support data synchronization to keep data consistency.

9.5 Data de-duplication

The data de-duplication is a method of reducing storage usage by eliminating redundant data. The data de-duplication can save resources of storage space and network bandwidth to transfer data.

The data de-duplication requirement includes:

- It is recommended for storage resources to support the data de-duplication capability.

10 Requirements for resources abstraction and control

Resources abstraction and control allows a CSP to access physical resources through software abstraction. It also provides composition, coordination, monitoring and scheduling of processing, storage and networking resources.

Resources abstraction and control directs the creation, modification, customization and release of abstracted resources. Resource abstraction and control is also responsible for controlling the interactions between resource pools and cloud services. A resource template refers to a set of standardized formatted hardware and software configuration settings for processing, storage and networking resources.

The resources abstraction and control requirements include:

- It is recommended that abstracted resources can be accessed and provisioned in a unified manner.
- It is recommended that abstracted resources are discovered, used and released through unified interfaces.
- It is recommended that abstracted resources are deployed and provisioned based on pre-defined policies.
- It is required to provide life-cycle management of resource templates (e.g., resource template creation, publication, activation, revocation and deletion).
- A resource template can optionally be applied to a group of resources at the same time.
- It is required to support monitoring of all physical and virtual resources.
- It is recommended that resource monitoring is capable of detecting the failures of resources.

11 Support of emergency telecommunications

Under emergency telecommunications (ET) [b-ITU-T Y.2205], any emergency-related service is understood as requiring special handling relative to other services.

If any component in the cloud infrastructure is used to support an emergency telecommunications service (ETS), the requirements in [b-ITU-T Y.1271] are relevant.

12 Security considerations

It is recommended that the security requirements of [b-ITU-T Y.2201], [b-ITU-T Y.2701] and the applicable X, Y and M series of ITU-T security Recommendations be taken into consideration; this includes access control, authentication, data confidentiality, communications security, data integrity, availability and privacy.

Security aspects for consideration within cloud computing environment are addressed by security challenges for CSPs, as described in [ITU-T X.1601]. In particular, [ITU-T X.1601] analyses security threats and challenges and describes security capabilities that could mitigate these threats and meet security challenges.

Appendix I

Overview and reference model for storage in a cloud environment

(This appendix does not form an integral part of this Recommendation.)

Storage resources are used to store a huge amount of data. The traditional storage system utilizes a tightly-coupled symmetry reference model which aims to work out high performance computing problems and may fulfil cloud computing scalability requirements. The next generation system adopts a loosely-coupled asymmetry reference model which centralizes metadata and controls manipulation. This reference model is not suitable for high performance computing; however, this design is to solve large capacity storage needs based on cloud computing deployment.

The applications and data in cloud environments need be delivered and maintained reliably using a tightly-coupled architecture. Other applications (e.g., search engines, media streaming) may rely on loosely-coupled architecture.

I.1 Reference model for cloud storage

Cloud storage delivers virtualized storage on demand over a network based on cluster, grid and distributed file systems. When the key issue of operation and processing in cloud computing is the storage and management of large-scale data, a large number of storage equipment need to be deployed. Hence, cloud storage is a cloud computing system for data storage and management.

Figure I.1 depicts the cloud storage reference model.

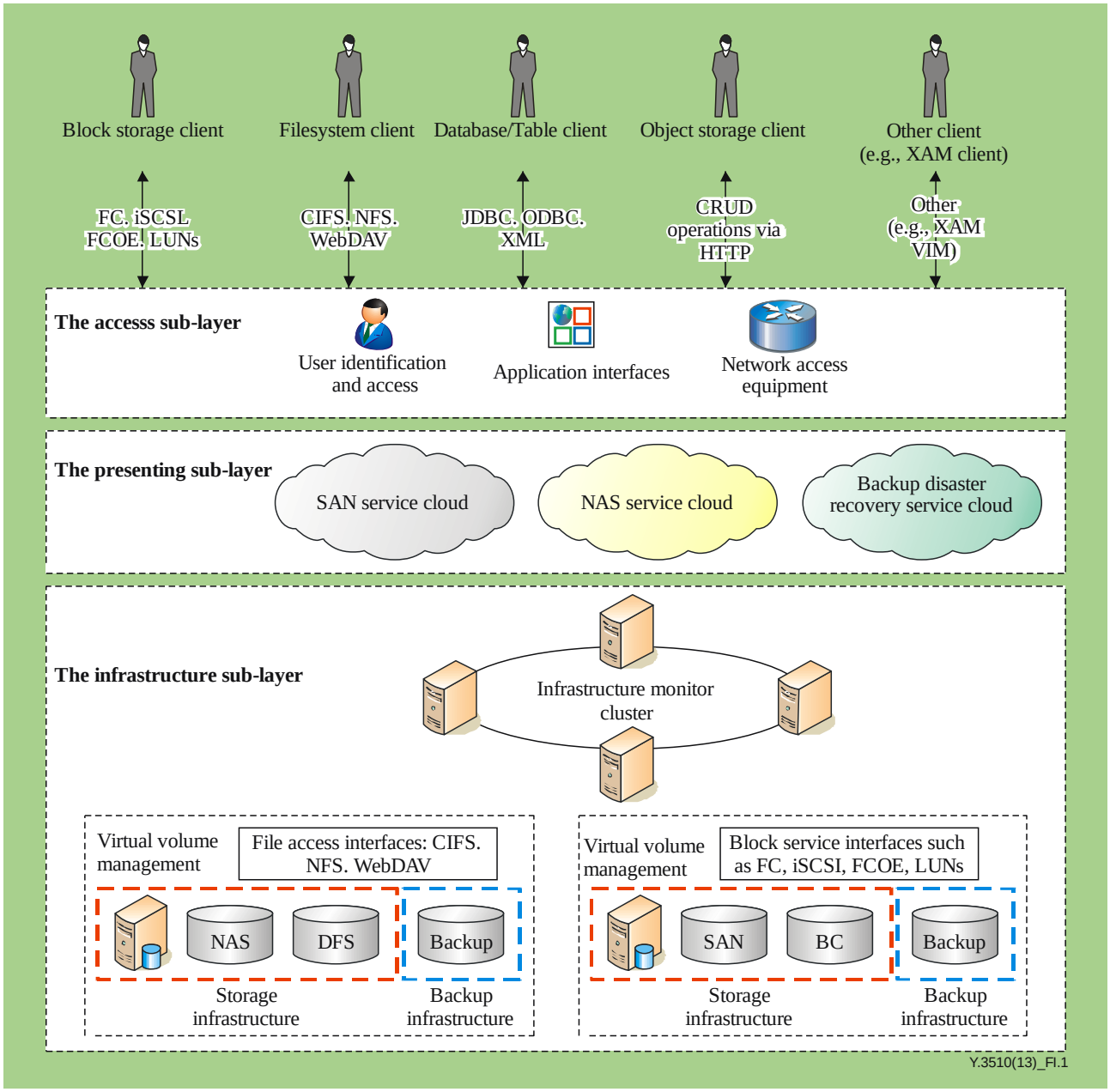


Figure I.1 – Cloud storage reference model

NOTE – The interfaces and protocols shown in Figure I.1 are examples used for illustrative purposes.

Cloud storage is the cooperating operation of multiple storage devices, multi-applications and multi-services. Not every storage system can be called cloud storage. A cloud storage system can provide functionalities such as a storage area network (SAN), network attached storage (NAS), data backup and disaster recovery.

As shown in Figure I.1, the cloud storage reference model is composed of three sub-layers which are described in the following clauses.

I.1.1 Infrastructure sub-layer

This sub-layer consists of the following 3 parts:

– The storage infrastructure is composed of common used storage devices such as fibre channel storage devices, NAS and Internet small computer system interface (iSCSI) [b-IETF RFC 3720] storage devices, as well as some related supporting appliances, such as switches for storage. Storage infrastructure will typically consist of several distributed working nodes to support high availability and reliability. A working node can include a virtual volume management element, an NAS and a distributed file system (DFS) device. Another type of working node can include a virtual volume management element, a SAN and a block control device.

– The backup infrastructure is composed of a physical type library, a virtual type library, a database and related software.

– The infrastructure monitor cluster is composed of many servers which manage and monitor all kinds of storage and backup devices, repair related links and check the redundancy and carry out centralized management. It can include a global schedule function to provide the resources location in the storage infrastructure depending on the received accessing requests and associated requested resources. The servers typically support distributed hash table (DHT) networking to provide a general accessing interface for name space management, load balance, metadata management, routing management and duplication management. The infrastructure monitor cluster can access virtual volume management elements of the storage infrastructure to realize unified volume management and policy management.

I.1.2 Presenting sub-layer

This sub-layer is the core of the service logic of the cloud storage system. It provides several storage services, such as services based on SAN or NAS, as well as backup disaster recovery services.

SAN and NAS-based services provide key storage services for the management of cloud storage, detection and repair of the faulty links, status monitoring and QoS.

Backup disaster recovery services supply high-level data protection making unnecessary the use of a specialized disaster recovery network.

I.1.3 Access sub-layer

This sub-layer consists of storage-based application interfaces, network access equipment, user identification functions and other relevant access functions. Once authenticated and authorized, users make use of the cloud storage services, such as those based on the network file system (NFS) [b-IETF RFC 3530] or iSCSI [b-IETF RFC 3720].

The access sub-layer connects users to the presenting sub-layer through the use of private or public networks.

Appendix II

Considerations on resource monitoring

(This appendix does not form an integral part of this Recommendation.)

This appendix provides considerations on resource monitoring.

II.1 Health monitoring

Health monitoring of the cloud infrastructure includes monitoring the status of resources such as the physical server hardware, hypervisor, virtual machine, physical and virtual network switches and routers and storage systems.

A resource map displays all of the technology components, including transactions, applications, web servers, network switches, virtualized components and third-party cloud services. Having such a map can play an important role in effective business service management because when there is an application or transaction problem, it can help pinpoint the infrastructure components that may be playing a role in service disruptions.

In addition, the resource map is important to provide run-time monitoring, because cloud infrastructure is constantly changing. It is necessary to ensure the management of this resource map on a continuous basis. Non-intrusive probes can be used to automatically detect infrastructure, application and transaction changes in near real-time.

II.2 Performance monitoring

Basic performance monitoring looks at the CPU, memory, storage and network performance metrics from the VM guest OS, as well as from the hypervisor. These metrics typically get monitored even in non-virtualized environments. The virtualization-specific metrics could be for specific entities that are introduced by various virtualization technologies. The behaviour of other virtualization features can also be measured as metrics, such as how frequently VM migrations are occurring or when other availability features are engaged. Then there are specialized applications built by virtualization, for example, desktop virtualization. Monitoring for such solutions needs more parameters to be collected from the VM, as well as the hypervisor, for example, how quickly VMs are provisioned to a requesting end user.

II.3 Capacity monitoring

Resource utilization is continuously evolving. Therefore, the continuous planning of various resources such as servers, desktops, networks, storage and also many kinds of software is needed. This demands periodic audits of physical and virtual resources. Capacity monitoring needs end-to-end continuous capacity monitoring of the following key metrics:

- **Server utilization**: Peak and average server resource utilization, memory, CPU, resource, server bottlenecks and correlation with a number of VMs.
- **Memory usage**: Memory utilization on each server, capacity bottlenecks and relationship with a number of VMs and with different cloud services.
- **Network usage**: Peak and average network utilization, capacity/bandwidth bottlenecks and relationship with a number of VMs and with different cloud services.
- **Storage utilization**: Overall storage capacity metrics, VM and virtual disk utilization, I/O performance metrics, snapshot monitoring and correlation with a number of VMs and with different cloud services.

II.4 Security and compliance monitoring

Virtualization introduces a new set of security risks due to VM sprawl and the introduction of new threat targets such as the hypervisor layer, virtual infrastructure (VI) configurations and potential conflicts in the way access control is managed and policies are applied. Security and compliance monitoring becomes critical

for securing the virtualized environment. Security and compliance monitoring needs end-to-end VI activity monitoring for:

- **VM sprawl**: Metrics to monitor VM activities as they get cloned, copied and, due to network migration, transfers to different storage media.
- **Configuration metrics**: Virtual server configuration monitoring to ensure that they are compliant with standards and hardening guidelines, VM configuration monitoring for software licensing policy enforcement and VI events that help enforce and detect violations of policy. This includes individual security and organization security policy monitoring.
- **Access control**: Access control monitoring and reports for role-based access control enforcement.
- **Compliance monitoring**: Metrics to validate audit and certification.

II.5 Monitoring and metering for charging and billing

In a virtualized environment the infrastructure is centralized and it is important to measure resource usage by different CSCs. This information can be used to distribute, amortize and in some cases, recover the cost correctly across the organization through a proper chargeback mechanism. Chargeback could be based on dynamic parameters such as resource usage and/or fixed parameters. To compute the correct chargeback information in a dynamic virtualized environment, it is important to monitor virtual and physical resource usage and allocations, as well as to be able to normalize the measurement across the cloud infrastructure. The monitoring and metering data for service charging should be collected and kept according to SLA objectives.

Chargeback monitoring needs end-to-end VI activity monitoring and service usage metering for:

- **Standard metrics**: All chargeable resource metrics like CPU usage, memory usage, storage usage and network usage metrics.
- **Key VI events**: VI events for virtual resource life-cycle events like start date and end date of VM creation and allocation.
- **Configuration monitoring**: VM configuration in terms of assigned resources and reservations and also applications installed to account for software licensing costs.
- **VM usage metrics**: VM uptime, number of VMs can vary depending on how the charging model is employed in the organization.

II.6 Monitoring in support of cloud services

The need for application and service monitoring is important in the cloud computing environment, especially for SLA/QoS evaluation because the application or service may have problems even if the VM or the physical server on which it is running looks normal. Application and service needs to monitor the basic health of application servers with the help of application-specific response time and throughput metrics. The analytics on this data could be used to correlate the application-observed and service-observed metrics to all layers of the infrastructure to perform a root-cause analysis in the event something going wrong. Application and service performance monitoring using the capture of network traffic is used more and more commonly in this area.

There are a few other aspects to virtual infrastructure monitoring that add to the complexity of building a comprehensive monitoring solution. All kinds of virtualization software allow the API to be able to collect metrics. However, each kind of virtualization software has its own object models. There are wide differences in features and even the behaviour of the common features. Therefore, the analytics that are to be built on the collected metrics must be developed for each kind of virtualization software.

Appendix III

Power management in cloud infrastructure

(This appendix does not form an integral part of this Recommendation.)

Datacentres are amongst the highest consumers of electricity all over the world. One distinct advantage of cloud computing is it is also able to power-manage hardware and devices. Therefore, the resources in a cloud infrastructure are recommended to be dynamically power-managed. The resources in cloud infrastructure are often arranged in trees. As some resources of a cloud infrastructure become idle, it can decrease power twigs or branches on trees. As the resource usage trends of cloud infrastructure are measured and controlled, it would be possible for these networks to put energy back into the grid by providing the grid with accurate time-based predictions of energy use. The grid can use this information to redirect energy to other destinations, or make other intelligent decisions.

Power management in cloud infrastructure represents a collection of processes and supporting technologies geared towards optimizing datacentre performance against cost and structural constraints. This includes increasing the deployable number of servers per rack when racks are subject to power or thermal limitations and making power consumption more predictable and easier to plan for.

Power management in cloud infrastructure comes in two categories: static and dynamic. Static power management deals with fixed power caps to manage aggregate power, while policies under dynamic power management take advantage of additional degrees of freedom inherent in virtualized cloud datacentres, as well as the dynamic behaviours supported by advanced platform power management technologies.

Appendix IV

Considerations on supporting of ETS

(This appendix does not form an integral part of this Recommendation.)

[b-ITU-T Y.1271] specifies the network requirements and capabilities to support ETS over both circuit-switched and packet-switched networks. Annex A of [b-ITU-T Y.1271] contains the list of functional requirements and categorizes them as essential and optional. Support for these requirements is needed for the scenario of when an ETS is offered by the CSP.

The requirements in [b-ITU-T Y.1271] can be separated into those relevant to the networking resources and those relevant to core transport network(s). Some requirements are applicable both for resources and for transport network(s). This clause considers the requirements for the networking resources category using the general requirements in clauses 8.1 and 8.2. The requirements relevant for networking resources from [b-ITU-T Y.1271] include: enhanced priority treatment, location confidentiality, restorability, interoperability, survivability/endurability, scalable bandwidth, reliability/availability and preferential treatment in congestion control measurement.

A cloud supporting ETS needs to be robust and able to support customers despite widespread damage. Another requirement is the restoration of access to cloud infrastructure resources including links connecting to the cloud. The processing nodes (virtual or physical) are to be restored quickly if damage to infrastructure resources occurs.

Cloud infrastructure resources need to adapt quickly for emergency applications, an adaptation that equates to application acceleration as noted in clause 8.1. Because ETS have requirements for different policies (QoS, security, traffic), the migration requirements in clause 8.1.5 are necessary to guarantee the SLAs among ETS customers and their CSPs.

The requirements, from [b-ITU-T Y.1271], specifically relevant to the support of ETS in core networks include: secure networks, restorability, network connectivity, mobility, coverage, survivability (connections), voice and data transmission, scalable bandwidth and reliability. Some of these requirements are applicable to both networking resources and the core transport network.

The requirements of clause 8.1, in relation to ETS, apply to ubiquitous coverage and therefore have the potential to preclude the need to establish special facilities after the occurrence of an emergency or disaster.

Reliability considerations of clause 8.1, in relation to ETS, are necessary for the network infrastructure to support survivability and endurability.

In support of ETS, the network should be smart enough for high priority applications. Some aspects of cloud services may be applicable to the offerings of priority services to facilitate disaster recovery functions, such as locating survivors and providing vital situational awareness information to government first responders and relatives of survivors affected by a disaster. Cloud computing can support complex modelling, analysis and rendering images to the first responders of disasters. [b-Tohoku]

Rapid authentication of authorized users for ETS implies awareness of the user/terminal attributes (subscriber profile data) and at the same time prevents unauthorized access, denial of service attacks and protection from intrusion.

Bibliography

[b-ITU-T E.107] Recommendation ITU-T E.107 (2007), *Emergency Telecommunications Service (ETS) and interconnection framework for national implementations of ETS*.

[b-ITU-T M.60] Recommendation ITU-T M.60 (1993), *Maintenance terminology and definitions*.

[b-ITU-T Q.1741.7] Recommendation ITU-T Q.1741.7 (2011), *IMT-2000 references to Release 9 of GSM-evolved UMTS core network*.

[b-ITU-T Y.1271] Recommendation ITU-T Y.1271 (2014), *Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit-switched and packet-switched networks*.

[b-ITU-T Y.2201] Recommendation ITU-T Y.2201 (2009), *Requirements and capabilities for ITU-T NGN*.

[b-ITU-T Y.2205] Recommendation ITU-T Y.2205 (2011), *Next Generation Networks – Emergency telecommunications – Technical considerations*.

[b-ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

[b-ITU-T Y.3011] Recommendation ITU-T Y.3011 (2012), *Framework of network virtualization for future networks*.

[b-IETF RFC 3530] IETF RFC 3530 (2003), *Network File System (NFS) version 4 Protocol*.

[b-IETF RFC 3720] IETF RFC 3270 (2004), *Internet Small Computer Systems Interface (iSCSI)*.

[b-IETF RFC 5905] IETF RFC 5905 (2010), *Network Time Protocol Version 4: Protocol and Algorithms Specification*.

[b-Tohoku] ACCJ (2011), *Responding to the Greater Tohoku Disaster: The Role of the Internet and Cloud Computing in Economic Recovery and Renewal. ACCJ Internet Economy Task Force*.

Framework of inter-cloud computing

Recommendation ITU-T Y.3511

(03/2014)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Summary

Recommendation ITU-T Y.3511 describes the framework for interactions of multiple cloud service providers (CSPs), which is referred to as inter-cloud computing. Based on several use case, and after considering the different types of service offerings, this Recommendation describes the possible relationships (peering, federation or intermediary) among multiple CSPs. By introducing the concept of primary CSP and secondary CSP, the Recommendation further describes CSP interactions for the cases of federation and intermediary patterns. Finally, relevant functional requirements are derived.

Keywords

Cloud computing, infrastructure, inter-cloud computing, network, primary CSP, requirement, secondary CSP, use case.

Table of Contents

1 Scope

This Recommendation describes the framework for interactions between multiple cloud service providers (CSPs), which is referred to as inter-cloud computing. Based on use cases involving several CSPs and after considering different types of service offerings (given in the appendices), this Recommendation describes the possible relationships among multiple CSPs, interactions between CSPs and relevant functional requirements.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1601] Recommendation ITU-T X.1601 (2014), *Security framework for cloud computing*.

[ITU-T Y.3501] Recommendation ITU-T Y.3501 (2013), *Cloud computing framework and high-level requirements*.

[ITU-T Y.3520] Recommendation ITU-T Y.3520 (2013), *Cloud computing framework for end to end resource management*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 cloud service customer [ITU-T Y.3501]: A person or organization that consumes delivered cloud services within a contract with a cloud service provider.

3.1.2 cloud service provider [ITU-T Y.3501]: An organization that provides and maintains delivered cloud services.

3.1.3 resource management [ITU-T Y.3520]: A way to access, control, manage, deploy, schedule and bind resources when they are provided by service providers and requested by customers.

3.1.4 service level agreement [b-ISO/IEC 20000-1:2011]: Documented agreement between the service provider and customer that identifies services and service targets

NOTE 1 – A service level agreement can also be established between the service provider and a supplier, an internal group or a customer acting as a supplier.

NOTE 2 – A service level agreement can be included in a contract or another type of documented agreement.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 inter-cloud computing: The paradigm for enabling the interworking between two or more cloud service providers.

NOTE – Inter-cloud computing is also referred as inter-cloud.

3.2.2 primary cloud service provider: In inter-cloud computing, a cloud service provider which is making use of cloud services of peer cloud service providers (i.e., secondary cloud service providers) as part of its own cloud services.

3.2.3 secondary cloud service provider: In inter-cloud computing, a cloud service provider which provides cloud services to a primary cloud service provider.

NOTE – The primary cloud service provider can use the services of secondary cloud service providers as part of its services offered to cloud service customers.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
B2B	Business-to-Business
CaaS	Communications as a Service
CDN	Content Distribution Network
CPU	Central Processing Unit
CSC	Cloud Service Customer
CSP	Cloud Service Provider
DRM	Digital Rights Management
IaaS	Infrastructure as a Service
ID	Identifier
IT	Information Technology
LAN	Local Area Network
NaaS	Network as a Service
P-CSP	Primary CSP
PaaS	Platform as a Service
QoS	Quality of Service
S-CSP	Secondary CSP
SaaS	Software as a Service
SDP	Service Delivery Platform
SLA	Service Level Agreement
VM	Virtual Machine
VPN	Virtual Private Network

5 Conventions

In this Recommendation:

The keywords "**is required**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

In the body of this Recommendation and its appendices, the words should, and may sometimes appear, in which case they are to be interpreted, respectively, as is recommended, and can optionally. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative are to be interpreted as having no normative intent.

6 Introduction

Inter-cloud computing describes the interworking of cloud service providers (CSPs) in order to deliver services for the users. Inter-cloud relationship between CSPs can be realized by using a service from the peer CSP or by providing a service to the peer CSP.

The case where two peer CSPs interact with each other through an inter-cloud relationship is illustrated in Figure 6-1. As shown by a pair of two arrows pointing in opposite directions in Figure 6-1, CSP A is making use of the services provided by CSP B. In this relationship, CSP A is considered as being the primary CSP while CSP B is the secondary CSP. Note that the reverse situation where CSP B is using the services offered by CSP A may also exist and in such case CSP A and CSP B are involved in two inter-cloud relationships, one for providing services to the peer CSP and the other for using the services of the peer CSP.

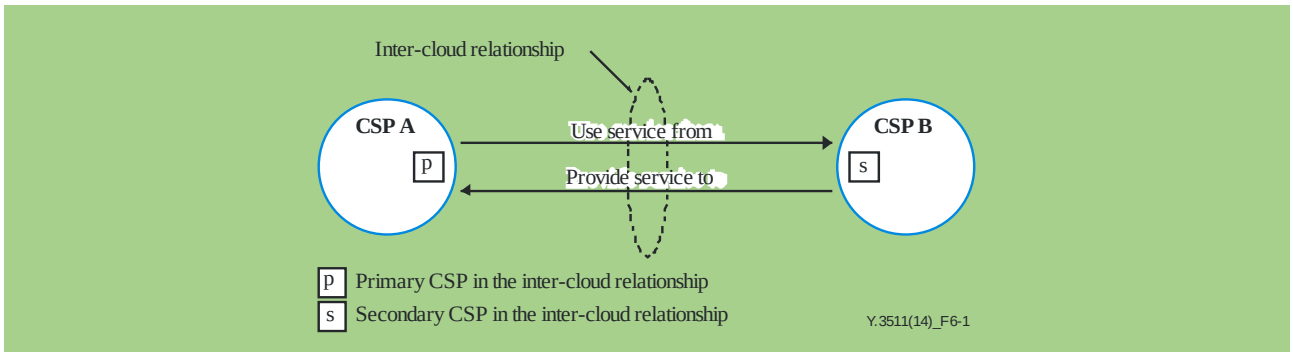


Figure 6-1 – Inter-cloud relationship between peer CSPs

Figure 6-2 illustrates in a different way the inter-cloud relationship between CSP A and CSP B, i.e., CSP A uses the service of CSP B through the application programming interface (API) provided by CSP B, shown as API (B). Although the arrow in Figure 6-2 is only one and is shown as unidirectional from CSP A to CSP B, it should be understood as being equivalent to the inter-cloud relationship shown in Figure 6-1, i.e., covering the "use service from" and "provide service to" arrows in Figure 6-1.

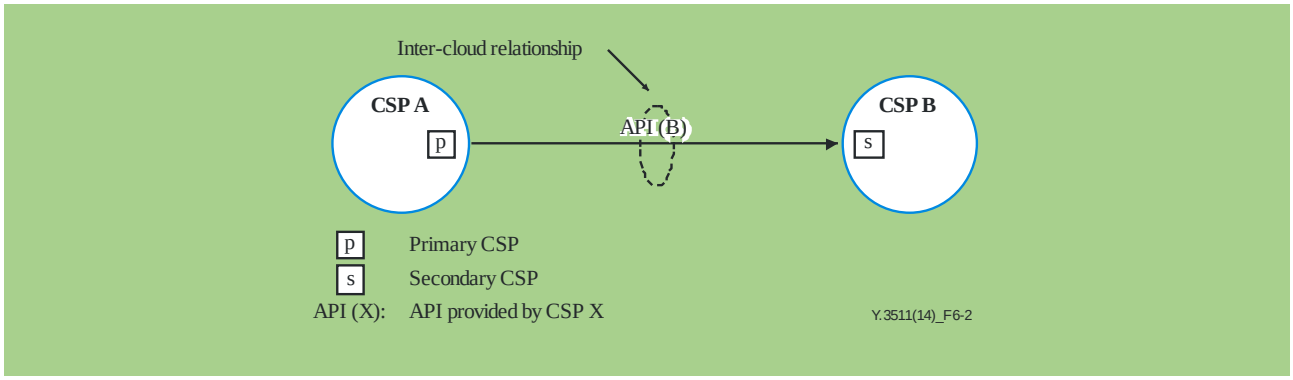


Figure 6-2 – Inter-cloud relationship using API

7 Patterns of inter-cloud

This clause introduces three patterns of inter-cloud for describing relations and interactions involving multiple CSPs, i.e.,:

– The inter-cloud peering;

– The inter-cloud federation;

– The inter-cloud intermediary.

7.1 Inter-cloud peering

In inter-cloud peering, two CSPs interwork directly with each other in order to use the services provided by the peer CSP.

NOTE 1 – Inter-cloud peering does not necessarily imply reciprocal relationships in terms of service use and service providing between the two CSPs.

NOTE 2 – Inter-cloud peering is a fundamental pattern, which may exist on its own or can be used in the two patterns described in clauses 7.2 (inter-cloud federation) and 7.3 (inter-cloud intermediary).

In inter-cloud peering, each CSP exposes its own API for cloud interworking and the CSPs interwork with each other directly by using the other CSP's API. As shown in Figure 7-1, CSP A interworks with CSP B using the API provided by CSP B and vice versa. Since the inter-cloud peering pattern can be used in the other pattern described in clauses 7.2 and 7.3, use of a common API between CSP A and CSP B is not precluded (see Figure 7-2).

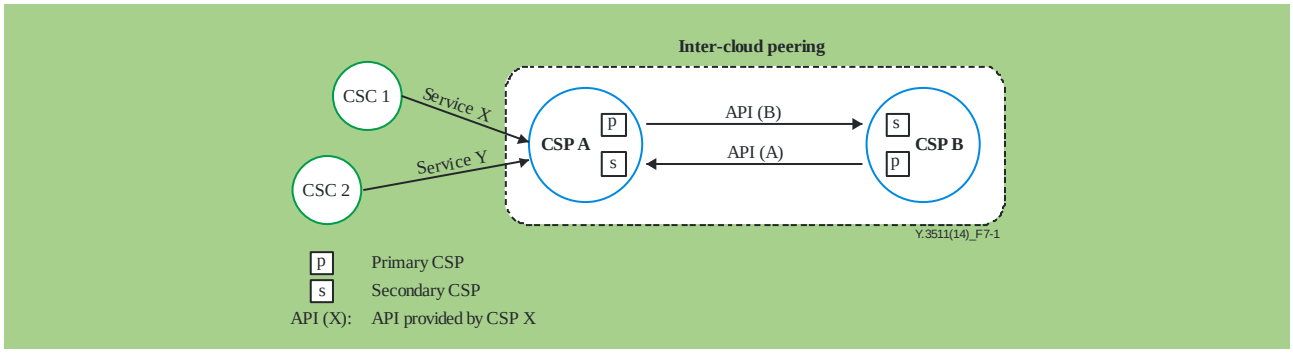


Figure 7-1 – Inter-cloud peering

As shown in Figure 7-1, the inter-cloud peering pattern consists of two inter-cloud relationships, CSP A to CSP B relationship and CSP B to CSP A relationship. CSP A is a primary CSP when using the services of CSP B provided by API (B) for providing services to its own customers (CSC1 and CSC2) and is also a secondary CSP when providing services to CSP B through its own API (A).

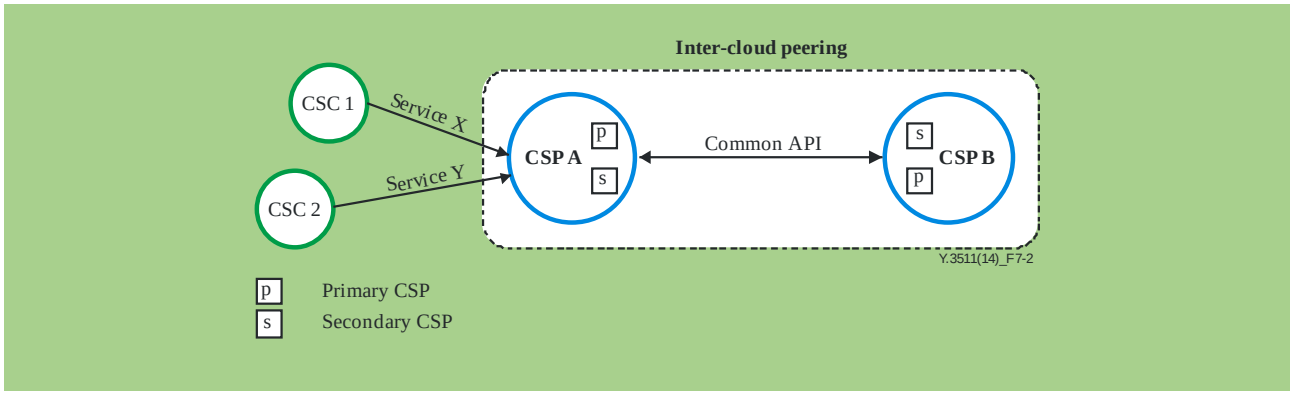


Figure 7-2 – Common API in the peering pattern

Figure 7-2 illustrates the case where a common API is used between CSP A and CSP B, i.e., API (A) and API (B) in Figure 7-1 are the same.

7.2 Inter-cloud federation

Inter-cloud federation involves using the cloud services within a group of peer CSPs who mutually combine their service capabilities in order to provide the set of cloud services required by cloud service customers (CSCs).

The multiple CSPs, which form the inter-cloud federation, establish and share the common agreement which may range from service-related policies, service level agreements (SLAs) and procedures which are relevant to the service offering and resource handling.

Based on the agreement, a CSP in the inter-cloud federation can offer its cloud services with the help of other CSPs.

A common API for cloud interworking is defined in the inter-cloud federation. As shown in Figure 7-3, each CSP interworks with the other CSPs in the inter-cloud federation through this common API.

It should be noted that the inter-cloud federation pattern does not necessarily require the fully meshed configuration of CSPs interacting with each other as shown in Figure 7-3.

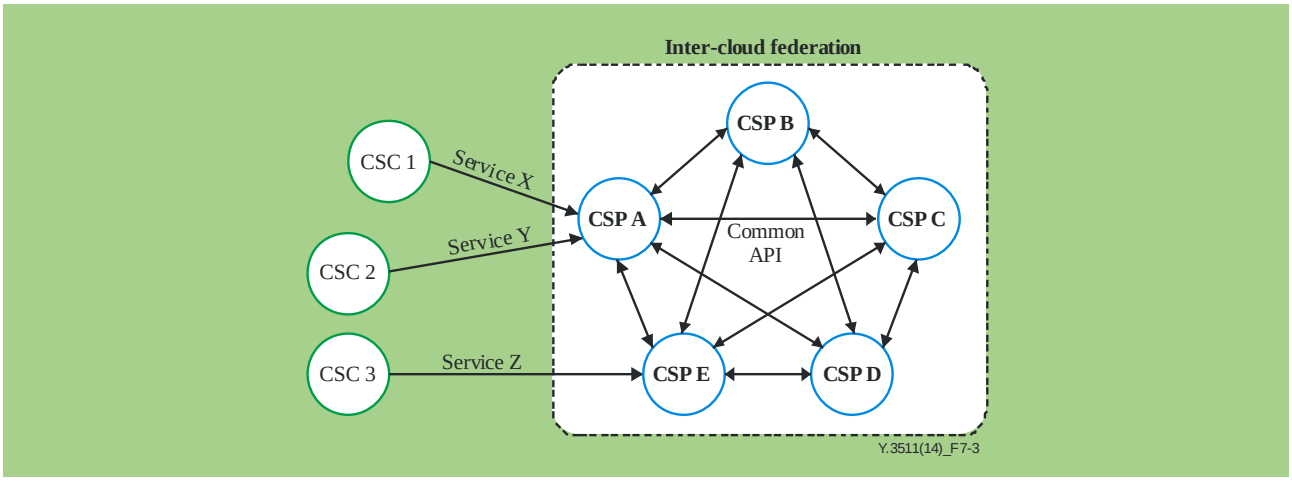


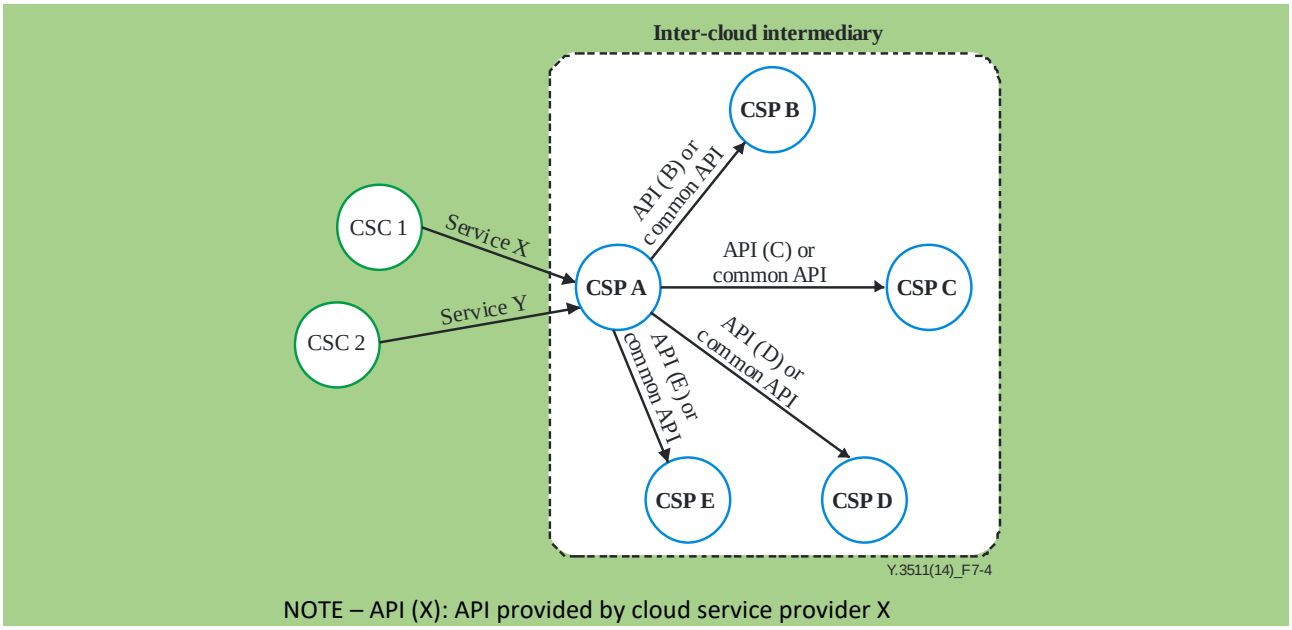
Figure 7-3 – Inter-cloud federation

7.3 Inter-cloud intermediary

In the inter-cloud intermediary pattern, the CSP interworks with one or more peer CSPs and provides intermediation, aggregation and arbitrage of services provided by these CSPs.

Service intermediation consists in conditioning or enhancing the cloud service of a peer CSP. Service aggregation relates to the composition of a set of services provided by the peer CSPs. Service arbitrage is about selecting one service offering from a group of services offered by the peer CSPs.

Interworking between a CSP providing service intermediation, aggregation and arbitrage and the peer CSPs can rely on either the inter-cloud peering pattern or the inter-cloud federation pattern. Figure 7-4 illustrates the inter-cloud intermediary pattern where CSP A provides intermediation, aggregation and arbitrage of cloud services provided by CSPs B, C, D and E.



NOTE – API (X): API provided by cloud service provider X

Figure 7-4 – Inter-cloud intermediary

8 Overview of inter-cloud computing

8.1 Relationship between intra-cloud and inter-cloud handling of resources

For collaboration among CSPs, two types of resources can be distinguished. One includes underlying physical resources of a cloud infrastructure which are controlled and managed by the CSP who owns these resources. The other type includes resources which are abstracted from the underlying physical resources and are offered as services to CSPs. During the collaboration of CSPs, such abstracted resources are also utilized during interactions between these CSPs.

Based on the abstraction, underlying physical resources will become abstracted resources. Detailed information of underlying physical resources, such as total central processing unit (CPU) cores and memories available in the infrastructure, will be hidden. During the collaboration among CSPs, only the information of abstracted resources, such as the CPU cores and memories dedicated to the given service, will be subject for interactions.

Figure 8-1 shows the relationship between intra-cloud and inter-cloud and their handling of resources.

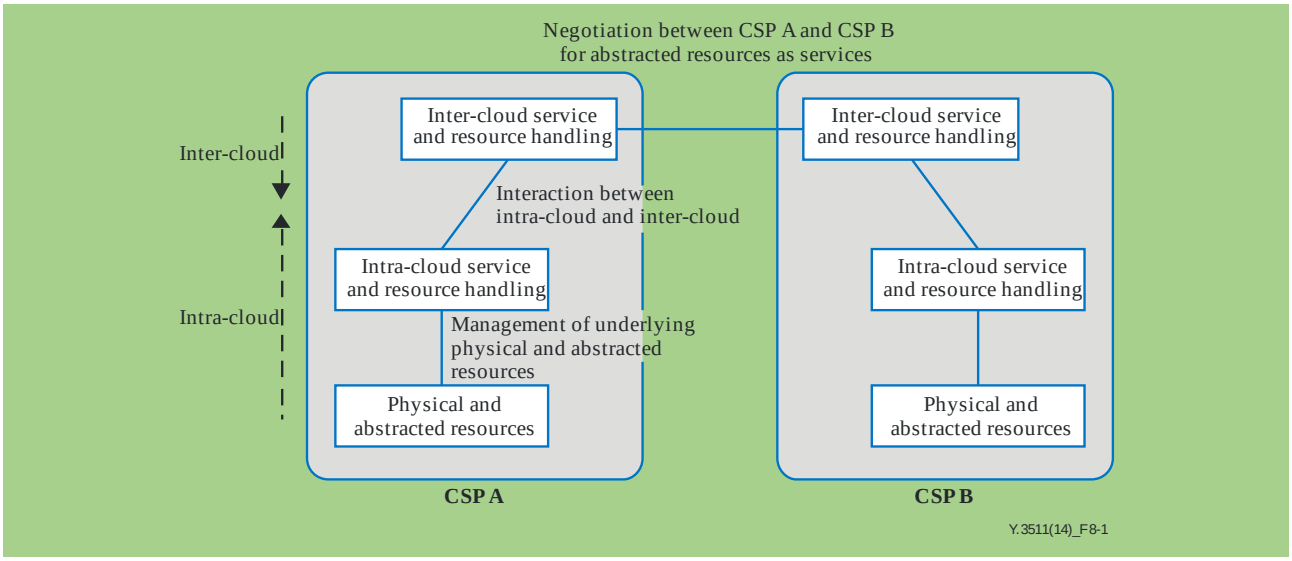


Figure 8-1 – Intra-cloud and inter-cloud relationship and handling of resources

In Figure 8-1, intra-cloud service and resource handling allows a CSP (A or B) to manage its own resources including underlying physical resources and abstracted resources. Inter-cloud service and resource handling allows a CSP to negotiate for the use of peer CSPs' abstracted resources provided as cloud services.

For example, when CSP A decides to use resources from CSP B, its intra-cloud service and resource handling will interact with its inter-cloud service and resource handling, which will then interact with CSP B. When the inter-cloud service and resource handling of CSP B receives the request from CSP A, the request will be relayed towards its own intra-cloud service and resource handling in order for CSP B to decide whether to provide the service and associated abstracted resources to the CSP A.

8.2 Overview of inter-cloud federation

8.2.1 Introduction

In the inter-cloud federation pattern, a number of CSPs provide services to CSCs. When needed (e.g., in the event of a serious shortage in resource pool), CSPs within the inter-cloud federation utilize other CSPs' resources to provide services to their customers.

Figure 8-2 illustrates the inter-cloud federation pattern.

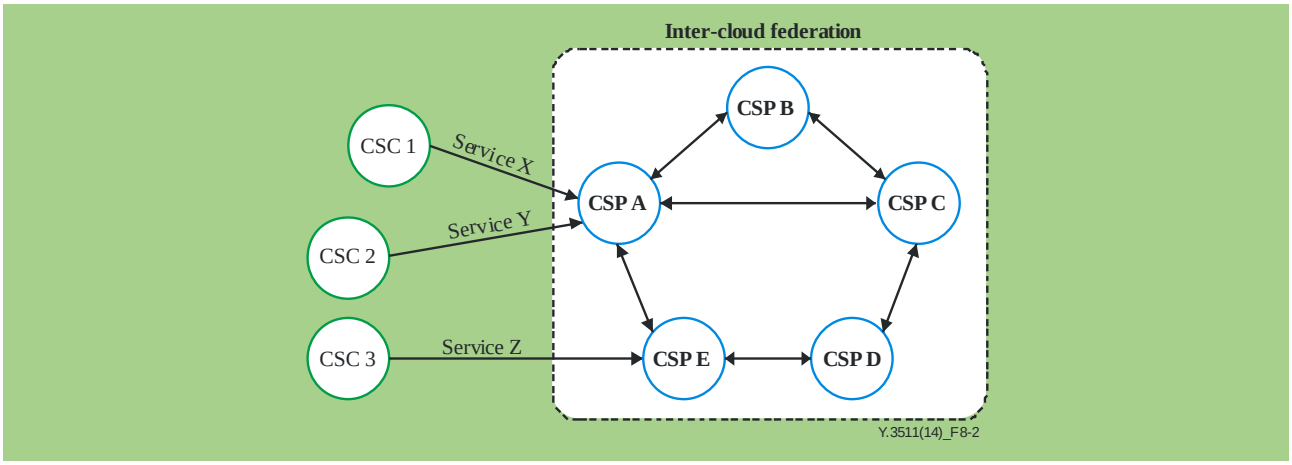


Figure 8-2 – Inter-cloud federation

As shown in Figure 8-2, CSC 1 and CSC 2 use services X and Y provided by CSP A, but the resources used for services X and Y may actually be provided by CSPs B, C or E.

8.2.2 Primary CSP and secondary CSP

In an inter-cloud federation, two or more CSPs interact to provide cloud services to CSCs. The CSP that is responsible for providing the services to a given CSC is called the primary CSP while the peer CSPs in the inter-cloud federation offering their own resources as services to the primary CSP are called secondary CSPs.

When needed, the primary CSP will make request in order to utilize the resources of secondary CSPs. The primary CSP determines which secondary CSPs will actually provide such resources (e.g., in terms of processing power, storage and networks) to the CSC. In some cases, the primary CSP may provide none of its own resources and will have to obtain all resources required for the support of services from secondary CSPs.

The roles of primary CSP and secondary CSP depend on the individual service. For example, in Figures 8-3 and 8-4, CSP A is the primary CSP and CSPs B, C and E are secondary CSPs for services X and Y. For service Z, CSP E is the primary CSP and CSPs A and D are secondary CSPs.

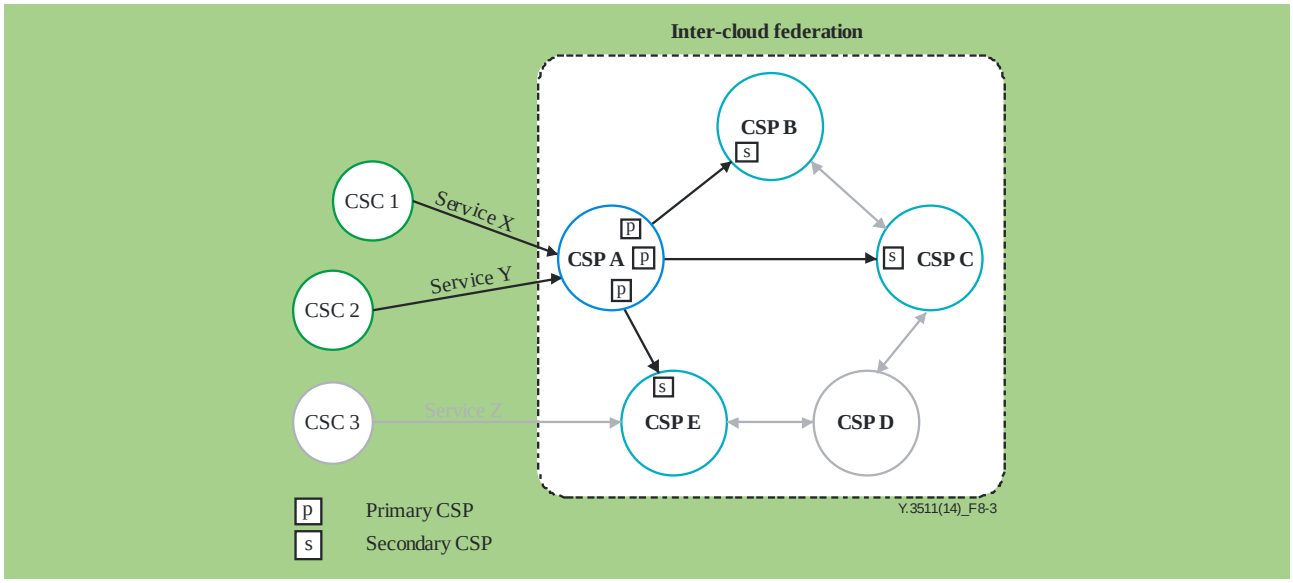


Figure 8-3 – CSP A offering services as the primary CSP with the help of secondary CSPs

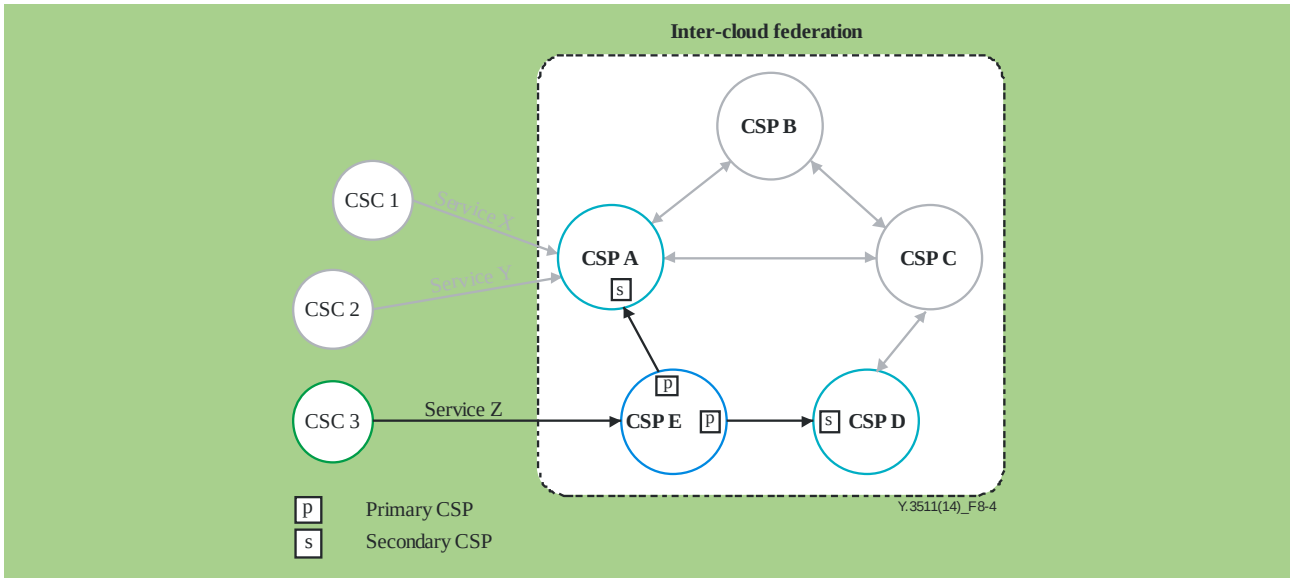


Figure 8-4 – CSP E offering services as the primary CSP with the help of secondary CSPs

A given CSP can act as a primary CSP and secondary CSP, i.e., using the services of secondary CSPs (e.g., CSP A in Figure 8-3) and providing services to a primary CSP (e.g., CSP A in Figure 8-4).

8.2.3 Network connectivity

In order to deliver cloud services based on the use of inter-cloud computing, network connectivity is required among the involved CSCs, primary CSPs and secondary CSPs. Specifically, this includes:

– Connectivity between peer CSPs. By means of this connectivity, a primary CSP can interwork with the secondary CSPs to request a service (e.g., backup of data or transfer of virtual machines between connected CSPs). In some cases, this connectivity is provided on-demand; the connectivity is established instantaneously as the need arises and removed after the need disappears;

– Connectivity between CSCs and CSP. By means of this connectivity, CSCs can use, operate, and manage their cloud services provided by CSPs. CSCs do not know on which CSPs their services actually run, but network connectivity facilitates access of CSCs to the appropriate CSP.

Figure 8-5 illustrates an example of configuration involving a Software as a Service (SaaS) CSP and multiple Infrastructure as a Service (IaaS) CSPs forming an inter-cloud federation. The SaaS CSP uses virtual machines (VMs) provided by IaaS CSPs which are members of the inter-cloud federation in order to provide SaaS services (e.g., applications such as e-commerce) to its SaaS CSCs.

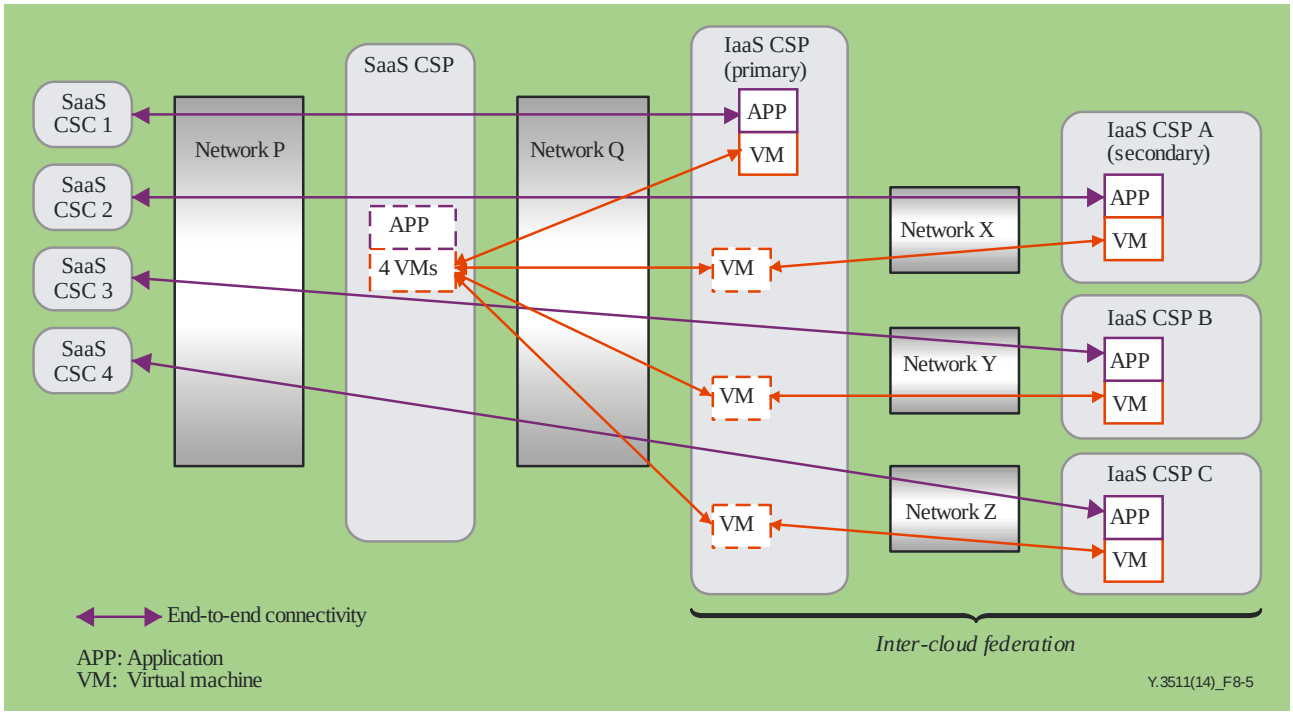


Figure 8-5 – View highlighting actual running VM and application locations

For the sake of simplicity, Figure 8-5 also shows network connectivity between different CSCs and CSPs (illustrated with "Network" boxes). These "Network" boxes may be under the responsibility of third-party providers different from the IaaS CSPs and SaaS CSPs, or may be provided by the IaaS and SaaS CSPs themselves. These "Networks" are involved in the support of end-to-end network connectivity (between the SaaS CSC and the "Application" running in the IaaS CSPs). Network connectivity supported by these "Networks" may be provided as a cloud service of the NaaS service category. Network capabilities for the support of NaaS service category are for further study.

By means of the connectivity provided by these networks, the SaaS CSCs can access the IaaS CSP on which the VMs providing the service run. The SaaS CSCs do not know on which IaaS CSPs the VMs exist, but the networks facilitate each access from SaaS CSCs to the appropriate IaaS CSP.

For the IaaS primary CSP, in order to achieve optimal resource use, it is desirable to handle information about VM availability as well as their connectivity (including bandwidth, quality of service (QoS) and cost). The IaaS CSP may choose to provide both computing and network resources jointly.

Multiple service offering scenarios including network contributions to the cloud services are described in Appendix III.

8.2.4 Interactions in the case of inter-cloud federation

Figure 8-6 shows the interactions involving multiple CSPs in the case of the inter-cloud federation pattern. In the inter-cloud federation, secondary CSPs provide their resources as one kind of service to the primary CSP.

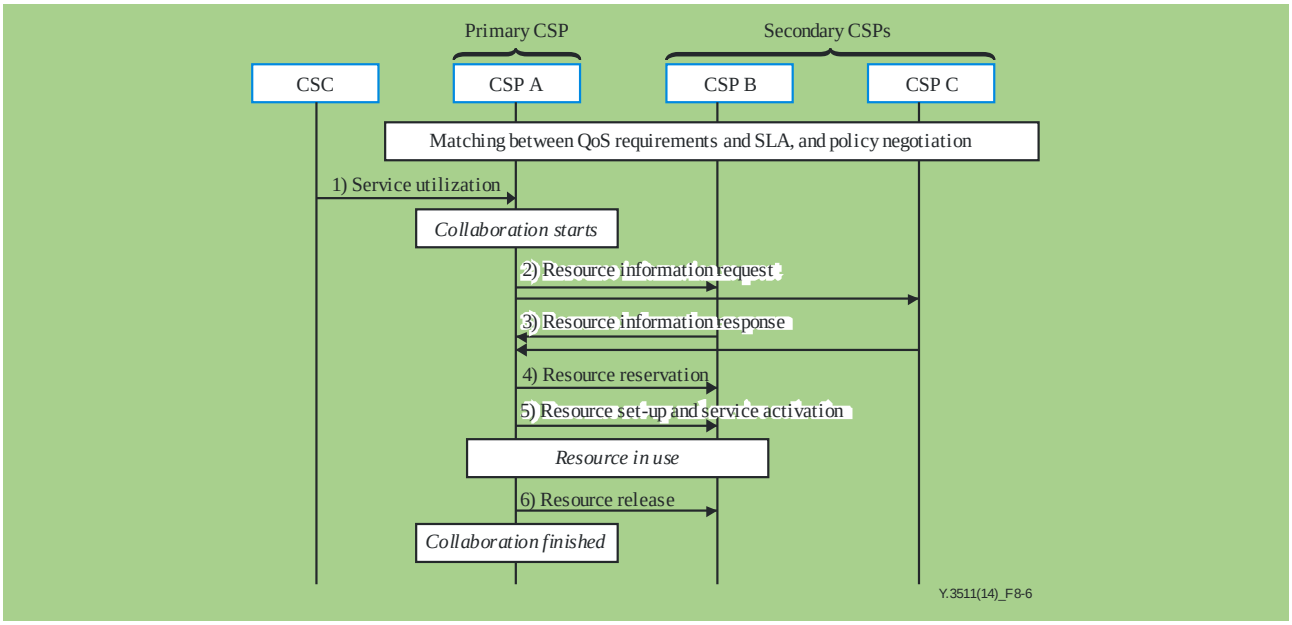


Figure 8-6 – Interaction among CSPs in inter-cloud federation

When the federation is established, the primary and the secondary CSPs perform matching between QoS requirements and SLA, and policy negotiation. The next steps as shown in Figure 8-6 are as follows:

1) The CSC starts to use the service of CSP A. CSP A is the primary CSP for this CSC;

2) The primary CSP (i.e., CSP A) decides to initiate an interaction due to a shortage of resources that results in service quality degradation. CSP A requests information about the resources (e.g., VMs and storage) from CSP B and CSP C. CSP B and CSP C are the secondary CSPs for this interaction;

3) CSP B and CSP C provide responses to CSP A regarding available resources;

4) On the basis of the received responses, CSP A reserves the resources of CSP B. In this step, CSP A estimates the performance of the resources available in CSP B and confirms that the estimated performance is acceptable;

5) CSP A sets up the resources of CSP B and activates the service (this action can be considered as VM migration or application rebuilding). As a result, service quality is maintained.

6) CSP A decides to end the collaboration with CSP B (e.g., CSP A has sufficient resources to provide services by itself or demand for services has decreased). CSP A releases the resources provided by CSP B.

These steps can be applied to every CSP involved in the inter-cloud federation. Each CSP in the federation is the primary CSP for its own CSCs and the CSPs providing resources to a primary CSP can be considered as the secondary CSPs.

The way a primary CSP requests resources from the secondary CSPs may vary from:

– "More-specific" resources request which includes detailed descriptions and may limit the number of candidate resources and resulting responses from the secondary CSPs but may obtain optimal resources if responded. However, complicated resource calculation and performance estimation may be necessary. A "more-specific" resources request is adequate when the cost associated with the offered resources is high and sensitive;

– "Less-specific" resources request soliciting more offerings and resulting in a simple and quick decision, although the offered resources may not be optimal.

A primary CSP may only receive and use a certain number of responses to reduce the processing burden caused by a large number of responses.

Details related to "more-specific" and "less-specific" resource requests are for further study.

8.3 Overview of inter-cloud intermediary

8.3.1 Introduction

The inter-cloud intermediary pattern provides the capability for CSPs to offer additional services to the CSCs and to other CSPs.

As shown in Figure 8-7, one of the central components of the inter-cloud intermediary pattern is the catalogue of service offerings. This CSP's catalogue is a registry that includes the services that the CSP offers to CSCs and to other CSPs. The catalogue provides the capability for CSCs and CSPs to obtain services from the CSP offering the services. This catalogue may be accessible through a portal and/or via a well-defined interface or API.

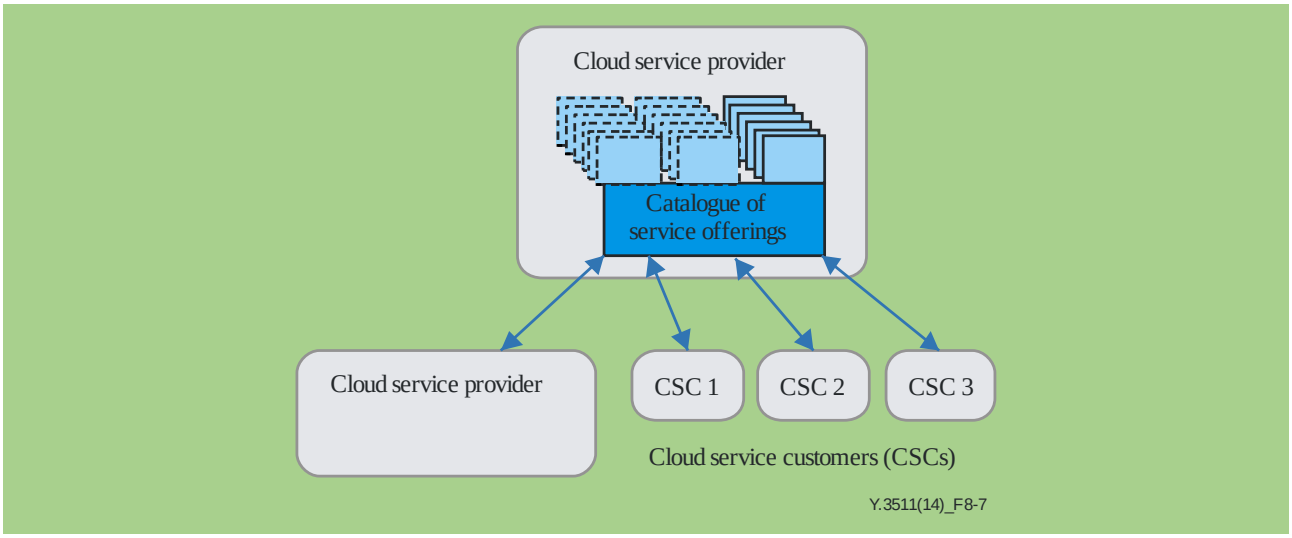


Figure 8-7 – CSCs and CSPs accessing cloud services offerings through a catalogue

In addition to the catalogue of service offerings, the CSP can include functions for the support of service intermediation, service aggregation and service arbitrage as described in clause 7.3.

8.3.2 Primary CSP and secondary CSP

The CSP that is responsible for offering the service to the CSC is the primary CSP. The CSPs that support the primary CSP by offering their services are the secondary CSPs.

In an inter-cloud intermediary pattern (see Figure 8-8), services listed in the primary CSP catalogue of service offerings may include the services hosted by the primary CSP itself or services that are provided by secondary CSPs. In most cases, the primary CSP catalogue of service offerings will be a combination of services hosted by the primary CSP and services offered by the secondary CSPs.

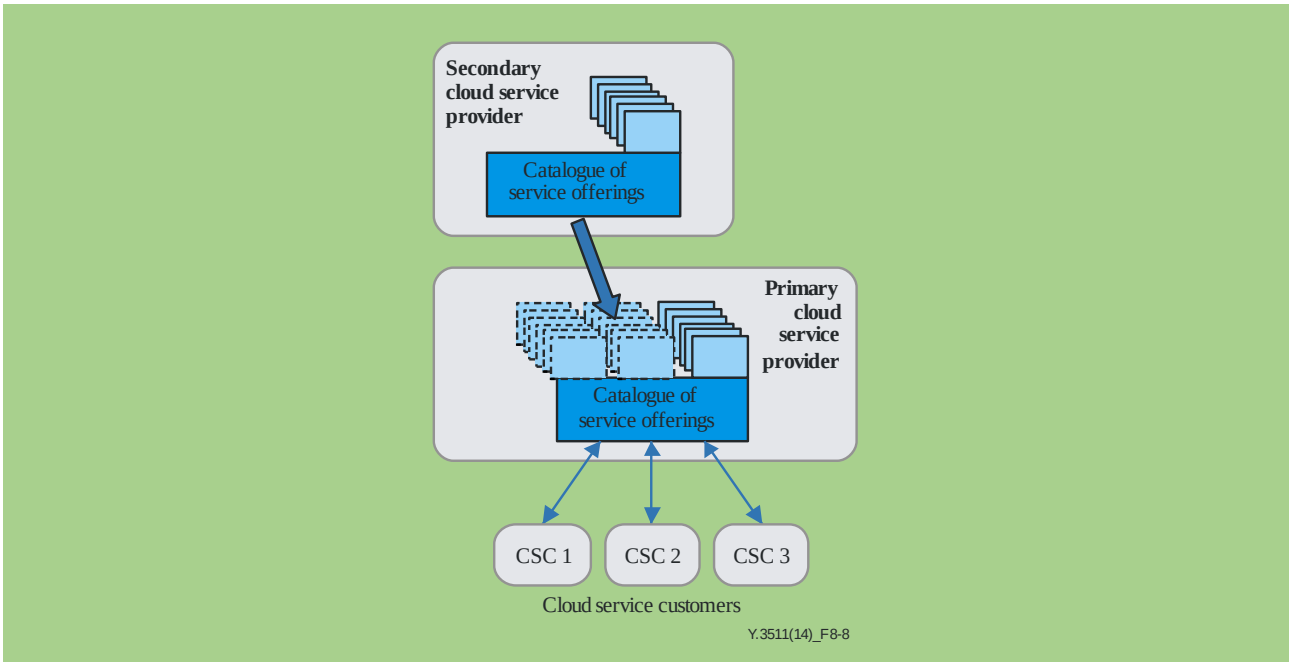


Figure 8-8 – Services provided from a secondary CSP to a primary CSP

The primary CSP may offer services from multiple secondary CSPs. Some of the services offered by the secondary CSPs may themselves be their own services or services from other CSPs. Note that the roles of primary and secondary service providers may change depending on the service under consideration.

The primary CSP serving the CSC provides the service level agreement (SLA) to the CSC and is responsible for ensuring that both services hosted by that primary CSP and services offered from a secondary CSP will meet the SLA between the CSC and the primary CSP.

8.3.3 Network connectivity

In considering network connectivity for the inter-cloud intermediary pattern, multiple levels of connectivity may be required.

In the simplest case, the CSP providing services to the CSC (the primary CSP) is hosting all of the services and is providing the network connectivity to the CSC. In this case, the CSP can offer an SLA covering both the cloud and network services.

In a more common case, the CSP providing services to the CSC (the primary CSP) will offer some of the hosted services but will also be offering services from one or more secondary CSPs. The network connectivity between the primary and the secondary CSPs may be offered as one of the primary CSP's services or it may be provided by a distinct third party network provider.

As illustrated by Figure 8-9, the primary CSP is responsible for ensuring that the SLA between the primary CSP and the CSC is met taking into account:

1) the network connectivity between the primary CSP and the CSC;
2) the services from the primary CSP;
3) the network connectivity between the primary CSP and the involved secondary CSPs;
4) the services from the secondary CSPs.

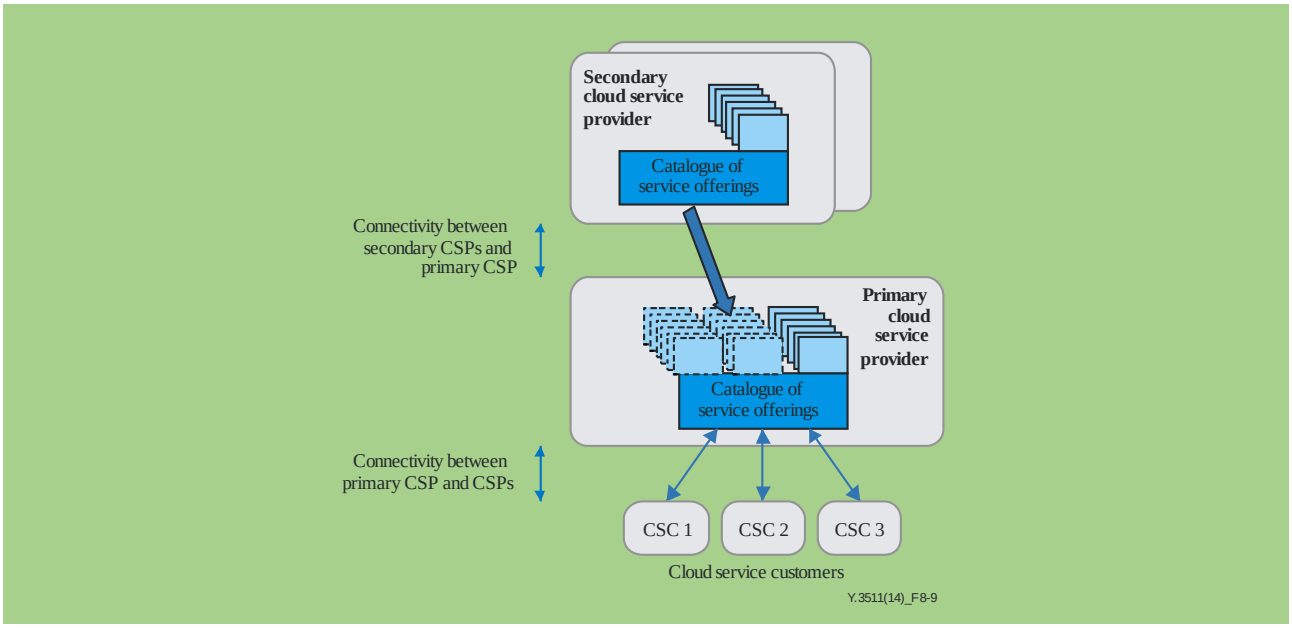


Figure 8-9 – Primary and secondary CSPs and relevant network connectivity

As illustrated in Figure 8-9, the CSCs use services provided by the primary CSP. The catalogue of service offerings in the primary CSP includes services from the secondary CSP. Since the CSCs use services through the primary CSP, the primary CSP is responsible for ensuring that the service levels provided to the CSC meet the SLA.

8.3.4 Interactions in the case of inter-cloud intermediary

Figure 8-10 shows the interactions involving a CSC and multiple CSPs in the case of the inter-cloud intermediary pattern.

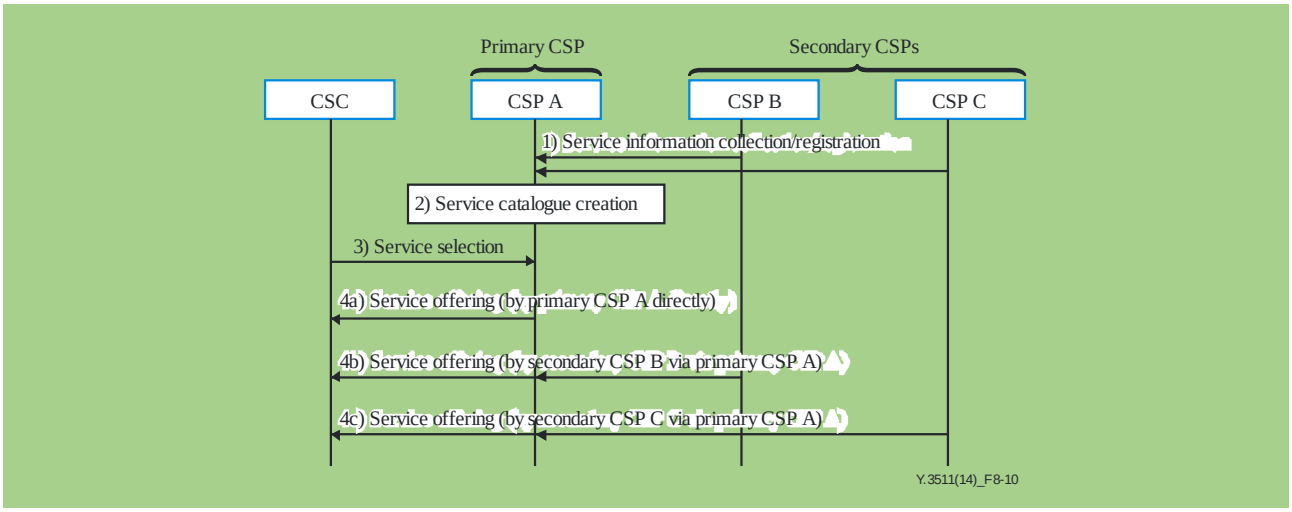


Figure 8-10 – Interactions in inter-cloud intermediary pattern

Along with the service offering, the description hereafter shows the interactions involving multiple CSPs. The steps as shown in Figure 8-10 are as follows:

1) The primary CSP collects service information from the secondary CSPs, or the secondary CSPs register their services to the primary CSP. Difference in terms of SLAs is negotiated as well;

2) The primary CSP creates the catalogue of service offerings by combining the list of hosted services and the services provided by the secondary CSPs;

3) The CSC accesses the primary CSP's catalogue of service offerings and selects one or some of the services in the catalogue;

4) The primary CSP arranges the service selected by the CSC. The service may be provided by the primary CSP, by (some of) the secondary CSP(s) or by a combination of these CSPs. The primary CSP intermediates, aggregates and/or arbitrages the services (see clause 7.3). The CSC starts using the service.

In practice, the actual process will be more complex. There are different ways for the CSC to use the services. If the requested service is hosted in the primary CSP, the CSC may access to this service directly (in the case of 4a)). If the requested service is offered by a secondary CSP, the CSC may access to the service in the secondary CSP via the primary CSP (in the cases of 4b) and 4c)). In the latter case, the network conditions, service characteristics and service agreement among the CSC, the primary CSP and the involved secondary CSP should be considered in order that the CSC accesses to the service in an appropriate manner.

9 Functional requirements for inter-cloud

This clause describes the CSPs' capabilities necessary to support different inter-cloud computing patterns described in clause 8.

The capabilities and the relevant requirements identified in this clause are complementary to the general requirements applicable to a CSP involved in inter-cloud as specified in [ITU-T Y.3501].

9.1 SLA and policy negotiation

The SLA and policy negotiation capability deals with the matching made by a primary CSP between SLA requirements of a CSC and the SLAs of secondary CSPs involved in the considered inter-cloud pattern. The subject includes the QoS related aspects. This capability also deals with the negotiation of service provisioning policies associated with the different CSPs involved in the inter-cloud pattern.

The SLA requirements (including QoS) of a CSC for a given cloud service are expected to be met by appropriate interworking with selected CSPs, even in the event of service performance degradation or a disaster.

The SLA and policy negotiation capability is required to:

– be aware of the SLA information related to the QoS and performance aspects of the CSPs involved in the inter-cloud using standard formats.

The SLA and policy negotiation capability is recommended to:

– allow comparing, negotiating and settling down service provisioning policies between multiple CSPs (for example, based on the settlement, these CSPs may be considered as a trusted group for inter-cloud support).

NOTE – In this clause, policy refers to a way for a CSP to provide services in terms of presumed reliability, including its backup scheme and target service levels. The policy affects SLAs. Policies may be different among CSPs. Policies may be negotiated beforehand and settled. This process is referred to as the policy negotiation.

9.2 Resource monitoring

The resource monitoring capability deals with the monitoring by the primary CSP of the resources of the secondary CSPs and the status attributes of these resources (e.g., usage amount, performance and quality aspects). The primary CSP collects and monitors the information from the secondary CSPs in a secure way. By monitoring the secondary CSPs' resources status (e.g., availability and dead/alive status of machines) and detecting service level performance degradation (in terms of delay and response time), the primary CSP can initiate actions to maintain service availability with the help of other secondary CSPs.

The resource monitoring capability is recommended to:

– allow describing and expressing the resource information (e.g., resource type, configuration and status) in a standard manner in order to be able to monitor these resources across multiple CSPs;

– allow updating the resource information across multiple CSPs in synchronization with the events (e.g., reserve or release of resources) involving the CSPs;
– allow periodically, or on a request basis, collecting information about the usage and performance status of the resources of multiple CSPs;
– allow periodically, or on a request basis, collecting information about the resource availability (e.g., dead or alive status of machines) of multiple CSPs;
– allow exchange of monitoring information in commonly defined ways across multiple CSPs.

9.3 Resource performance estimation and selection

The resource performance estimation and selection capability deals with the selection of resources from the candidate resources that have already been reserved in peer CSPs. This capability estimates the achievable performance of available reserved resources and assists the CSP in the selection of resources to be effectively used.

The resource performance estimation and selection capability is recommended to:

– allow estimating the achievable performance of available reserved resources (e.g., computing resources, storage resources, input/output capacity between storage resources, network bandwidth) in the secondary CSPs.

9.4 Resource discovery and reservation

The resource discovery and reservation capability deals with search, discovery and reservation of available resources in the peer CSPs. This capability also deals with reservation acknowledgement for the candidate resources that have been tentatively reserved in the peer CSPs.

The resource discovery and reservation capability is recommended to:

– enable discovery of resources available in the peer CSPs;
– allow the reservation of discovered resources in the peer CSPs;
– allow provisional reservation of discovered resources, i.e., to keep the resources to be used (as candidates), for later acknowledgement (for some of them) or release (for others);
– allow finding available resources in the peer CSPs based on different priorities (e.g., in a different order of searching);

NOTE 1 – Quality requirements may vary from service to service and each resource contribution to the service quality may vary as well. For example, if latency is critical, it should be possible to first reserve resources in the servers that are near to the user and then reserve the network resources. In contrast, if bandwidth is critical, it should be possible to first reserve resources of the networks that can provide sufficient bandwidth and then search for available resource in the servers that are connected to those networks.

– allow reservation of available resources in the peer CSPs on the basis of different priorities (e.g., early recovery, required quality guarantee, service type, etc.).

NOTE 2 – For example, a vast quantity of resources is required for recovery from a large-scale disaster. However, all required resources may not necessarily be available. In that case, it should be possible to forcefully reserve resources for lifeline services rather than for other services.

9.5 Resource set-up and activation

The resource set-up and activation capability deals with the set up and activation of reserved resources in the peer CSPs. This includes connecting to the peer CSPs via networks, remotely activating (i.e., invoking) software and transferring or copying data to enable the use of resources in the peer CSPs.

The resource set-up and activation capability is recommended to:

– allow the establishment of reserved resources in a peer CSP;
– allow accessing to the configuration and policy settings of reserved resources in the peer CSPs.

9.6 Cloud services switchover and switchback

The cloud services switchover and switchback capability deals with the switchover of the CSC's end-user access to cloud services from the primary CSP to a peer CSP to which the services may be provided in order to cope with degradation in service performance or a serious problem. It also deals with the switchback to the primary CSP when it is able to provide the services again. It should be noted that the reasons for switch-over ranges from a load distribution between CSPs, in which the primary CSP role is maintained as it is, to a serious problem, in which the primary CSP role is delegated to the peer CSP. The capability differences to reflect those reasons need further study.

The cloud service switchover and switchback capability is recommended to:

– allow switching over CSC's end-user access to a peer CSP (acting as primary CSP) without manual operation from the CSC, in order to allow the CSC's end user to use services in a similar manner to the way they did before the access was switchover;

– allow switching back the CSC's end-user access to the primary CSP when this CSP has recovered from the reasons that led to the switchover (e.g., a disaster or load distribution between peer CSPs is no longer needed).

9.7 Resource release

The resource release capability deals with the release by a CSP of the peer CSPs' (reserved and/or used) resources after determining that these resources are no longer needed, e.g., based on monitoring the results such as disaster recovery has been completed or load has been reduced.

The resource release capability is recommended to:

– allow releasing by the CSP of resources reserved, activated and/or set up in the peer CSPs;

– allow updating the peer CSP's resource configuration information;

– allow erasing and/or transferring back cloud application data received during the resource reservation.

9.8 CSC information exchange

The CSC information exchange capability deals with exchanging CSC profiles and associated information between a primary CSP and the secondary CSPs. The information associated with a CSC is initially maintained by the primary CSP. When the primary CSP requests that the secondary CSPs should provide additional resources and run applications over the secondary CSP resources, the secondary CSPs may need to perform customer management by inheriting the CSC profiles and associated information given by the primary CSP. Activation of CSC information exchange needs prior agreement of the CSC.

The CSC information exchange capability is required to:

– be activated only with the prior agreement of the CSC;

– be able to manage CSC profiles and associated information.

The CSC information exchange capability is recommended to:

– be able to exchange CSC profiles and associated information among multiple CSPs according to a pre-determined protocol and format, with the condition that the CSC is informed of and agrees to the exchange.

9.9 Primary CSP role delegation

The primary CSP role delegation capability deals with transferring the primary CSP role to one of the secondary CSPs, e.g., in the event of a serious problem caused by natural disasters or permanent service termination occurring at the current primary CSP. In preparation for the serious problem or permanent service termination at the primary CSP, all management information associated with the primary CSP is shared with the secondary CSPs, while the absolute controllability of the information, i.e., permission to update the information, is still held by the primary CSP. When the serious problem or service termination

occurs, the absolute controllability for a given primary CSP role, i.e., permission, is transferred to one of the designated secondary CSPs. By transferring the responsibility of the primary CSP role with associated management information, the service can continue even if the primary CSP's systems are seriously damaged, e.g., due to a natural disaster or the CSP stops a service due to economic decisions (refer to use cases in clauses I.4 and I.5). Activation of the primary CSP role delegation needs prior agreement of the CSC.

The primary CSP role delegation capability is required to:

– be activated only with the prior agreement of the CSC.

The primary CSP role delegation capability is recommended to:

– allow a CSP to discover peer CSPs that are capable of inheriting the primary CSP role, and enable the CSP to negotiate with these peer CSPs as to whether they can accept the inheritance;
– allow a CSP to transfer its management information associated with the primary CSP role in a reliable manner (e.g., periodically) to the peer CSPs that have accepted the permission transfer with that CSP;
– allow the controllability of the information associated with the primary CSP role to be transferred to the secondary CSPs with minimum interruptions;
– allow a CSP to cancel the permission transfer arrangements.

9.10 Inter-cloud service handling

The inter-cloud service handling capability deals with the primary CSP offering cloud services to its CSCs based on the handling of services provided by the secondary CSPs. This capability can be used for inter-cloud intermediary pattern.

The inter-cloud service handling capability is required to:

– support service intermediation, i.e., conditioning or enhancing the cloud service of a peer CSP;
– support service aggregation, i.e., providing the composition of a set of services provided by the CSPs;
– support service arbitrage, i.e., selecting one service offering from a group offered by the peer CSPs.

10 Security considerations

The security framework for cloud computing is described in [ITU-T X.1601] covering security challenges for CSPs. In particular, [ITU-T X.1601] analyses security threats and challenges in the cloud computing environment and describes security capabilities that could mitigate these threats and meet security challenges.

Appendix IV identifies important aspects that should be considered when developing Recommendations addressing inter-cloud security aspects.

Appendix I

Use cases from the inter-cloud perspective

(This appendix does not form an integral part of this Recommendation.)

This appendix describes use cases in which multiple cloud computing systems interact with each other to satisfy the specified requirements and how cloud systems work in each use case.

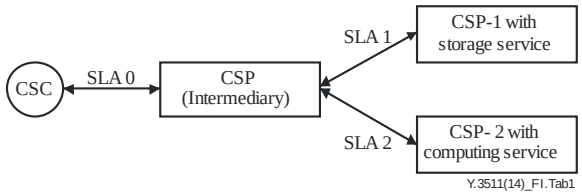
I.1 SLA mapping in intermediary pattern

This use case illustrates the SLA mapping between the primary CSP in inter-cloud intermediary pattern (called CSP-Intermediary) and other secondary CSPs.

Multiple CSPs contribute to, or impact concurrently, the SLA between the CSP-Intermediary and the CSC when an orchestrated service is provided.

Table I.1 shows SLA mapping in an inter-cloud intermediary pattern.

Table I.1 – SLA mapping in an inter-cloud intermediary pattern

Use case	
Use case title	SLA mapping in an inter-cloud intermediary pattern
Relevant roles	CSC and CSP
Use case description	– The primary CSP in an inter-cloud intermediary pattern (CSP-Intermediary) is the contact point for CSC and there is SLA (SLA0) between them. – The CSP-Intermediary integrates services from multiple CSPs, for instance, storage service from CSP-1 and computing service from CSP-2. There are business-to-business (B2B) level SLAs between CSP-Intermediary and CSP-1, CSP-2 respectively (SLA1, SLA2). – For the CSP-Intermediary, in order to guarantee SLA0 for CSC, it is necessary to map SLA0 to SLA1 and SLA2, because SLA0 is actually implemented by SLA1 and SLA2.
Information flow	SLA mapping may be performed via explicit information exchange or off-line negotiation.
High-level figure describing the use case	
Derived requirements for cloud capability	– The capability to support SLA negotiation between CSP-Intermediary and other CSPs is recommended. – The capability to support coordination of the SLAs from multiple CSPs (which is related to a business decision) is recommended.

I.2 Performance guarantee against an abrupt increase in load (offloading)

Table I.2 shows an inter-cloud use case where performance is guaranteed in case of an abrupt increase in load.

NOTE – The following legend applies to the Figures in Tables I.2 to I.5:

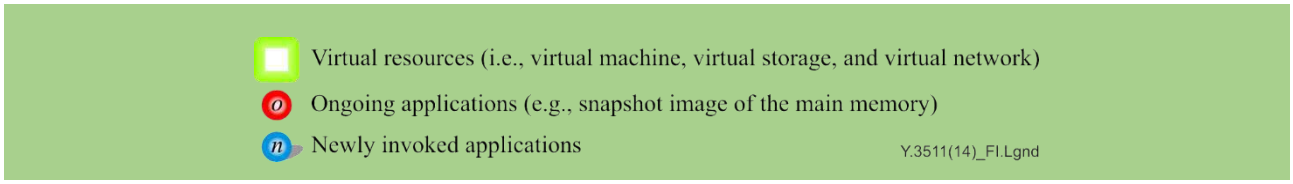


Table I.2 – Inter-cloud use case: Performance guarantee against an abrupt increase in load

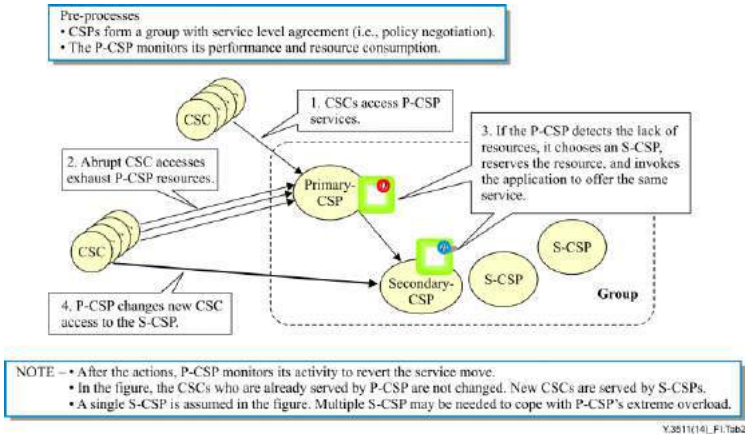
Use case	
Use case title	Inter-cloud use case: Performance guarantee against an abrupt increase in load
Relevant roles	CSP and CSC
Use case description	– A CSP guarantees its service performance, even when an unexpected surge in access to the service arises, by using cloud resources provided by other CSPs on a temporary basis. – When overload is detected at a CSP, available resources in other CSPs are autonomously discovered and reserved through the inter-cloud federation. – Network connections among interworking CSPs are instantaneously established or reconfigured. Then service-related data including user identifier (ID), user data and application data are transferred from the original CSP to the CSP that is leasing the resources. – Access from CSCs is appropriately changed to the interworking CSPs so as to distribute the load and thus mitigate the overload of the original CSP.
Information flow	– Relevant CSPs are supposed to join a common trusted alliance (i.e., federation) in advance and set up the service level agreements (SLAs). – A CSP inquires about the resource availability of other CSPs in the federation and requests reservation of the available resources that meet the quality requirements of the CSC. The requested CSPs reply whether or not they are able to lease the requested resources. – The cloud resource management (e.g., CRUD: create, read, update and delete) are operated across multiple CSPs. The management is to enable cloud resources to be leased from different CSPs in the federation. – The relevant CSPs exchange monitoring and auditing information of the leased resources.
High-level figure describing the use case	

Table I.2 – Inter-cloud use case: Performance guarantee against an abrupt increase in load

Use case	
Derived requirements for the cloud capability	The capability is required to support: – Policy negotiation including SLA management among the multiple CSPs within a pre-established group (i.e., federation); NOTE – Policy refers to a way for a CSP to provide services in terms of presumed reliability of a machine, including its backup scheme and target service levels. The policy may be different with each CSP. To maintain the same quality of service to the CSC even when the CSP changes, the difference should be negotiated beforehand and settled. This process is referred to as policy negotiation. The same note applies to the other use cases. – Self-performance monitoring at a CSP. If the performance degrades, the CSP should initiate the next configured actions; – Discovery, reservation, use and release of cloud resources in a dynamic manner (i.e., not relying on the pre-configuration) on other CSPs within a federation; – Application invocation over the reserved resources on other CSPs within a federation; – Alteration and reversion (i.e., switchover and switchback) of CSC access from one CSP to another CSP in a dynamic manner (i.e., not relying on the pre-configuration) within a federation; – Exchange of monitoring and auditing information among the multiple CSPs within a federation; – Exchange of authentication information about CSC (user/enterprise) authentication status among the multiple CSPs within a federation.

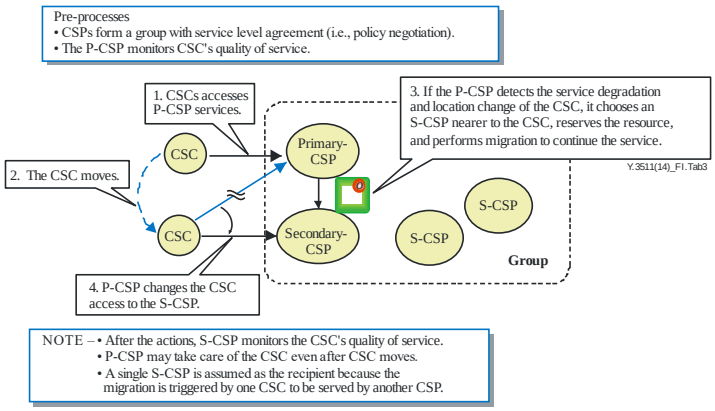
I.3 Performance guarantee regarding delay (optimization for user location)

Table I.3 shows inter-cloud use case for performance guarantee regarding delay.

Table I.3 – Inter-cloud use case: Performance guarantee regarding delay

Use case	
Use case title	Inter-cloud use case: Performance guarantee regarding delay
Relevant roles	CSP and CSC
Use case description	– CSPs guarantee their service performance (in particular, network delay and response time), even when a CSC moves to a remote location (e.g., on a business trip), by using cloud resources provided by another CSP located close to the CSC on a temporary basis. – When degradation in the response time is detected for a CSC at a CSP, available resources are autonomously discovered and reserved in another CSP that is near the CSC based on the user's location information.

Table I.3 – Inter-cloud use case: Performance guarantee regarding delay

Use case	
	– Network connections among interworking CSPs are instantaneously established or reconfigured. Then service-related data including user identifier (ID), user data and application data are transferred from the original CSP to the CSP that is leasing the resources. – Access from CSCs is appropriately changed to the interworking CSP so as to achieve route optimization and thus mitigate the performance degradation caused by the distance from the original CSP. – As a result, the CSC, who keeps the same user ID, can continuously access the service at the same level of response time as before.
Information flow	– Relevant CSPs are supposed to join a common trusted alliance (federation) in advance and set up the service level agreements (SLAs). – A CSP inquires about the resource availability of other CSPs in the federation, and requests a reservation of available resources that meet the quality requirements of the CSC. The requested CSPs reply whether or not they are able to lease the resources. – The cloud resource management (e.g., CRUD: create, read, update and delete) are operated across multiple CSPs. The management is to enable the leasing of cloud resources from different CSPs in the federation. – The relevant CSPs exchange monitoring and auditing information of the leased resources.
High-level figure describing the use case	
Derived requirements for the cloud capability	The capability is required to support: – Policy negotiation including SLA management among the multiple CSPs within a pre-established group (i.e., federation); – CSC service level monitoring at CSP. If the service level degrades, the CSP should initiate the next configured actions; – Discovery, reservation, use and release of cloud resources, based on CSC location, in a dynamic manner (i.e., not relying on the pre-configuration) on other CSPs within the federation; – Capability migration (e.g., virtual machine (VM) and applications) over the reserved resources on other CSPs within the federation; – Alteration and reversion (i.e., switchover and switchback) of CSC access to one CSP to another CSP in a dynamic manner (i.e., not relying on the pre-configuration) within the federation; – Exchange of monitoring and auditing information among the multiple CSPs within the federation; – Exchange of authentication information about CSC (user/enterprise) authentication status among the multiple CSPs within the federation.

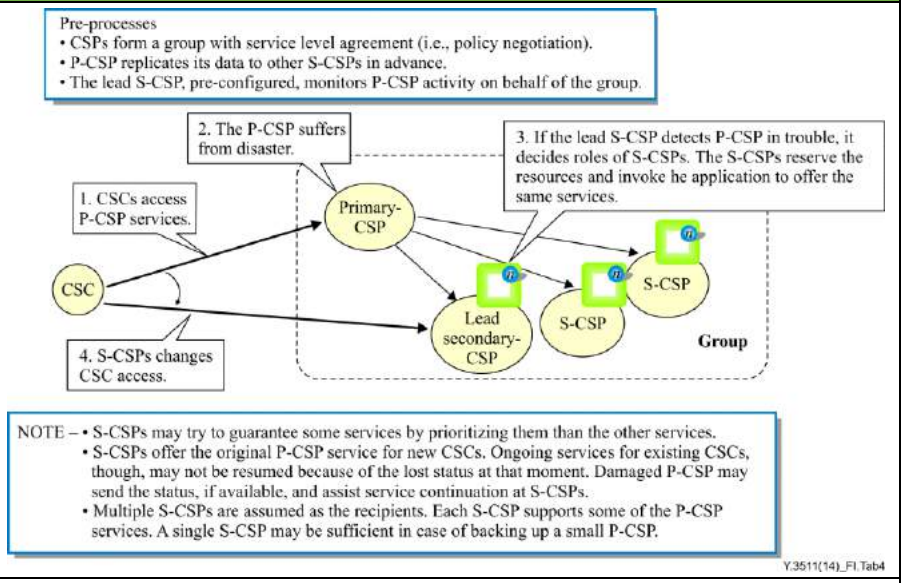
I.4 Guaranteed availability in the event of a disaster or large-scale failure

Table I.4 shows inter-cloud use case for guaranteed availability in the event of a disaster or large-scale failure.

Table I.4 – Inter-cloud use case: Guaranteed availability in the event of a disaster or large-scale failure

Use case	
Use case title	Inter-cloud use case: Guaranteed availability in the event of a disaster or large-scale failure
Relevant roles	CSP and CSC
Use case description	– CSPs continue offering their service using the resources leased from each other, even when systems in one CSP are damaged due to natural disasters or large-scale failures. – Available resources in other CSPs are autonomously discovered and reserved through the inter-cloud federation. – The services with a high priority are only recovered if available resources are not sufficient to recover all services. In examining the availability of resources provided by other CSPs, the guaranteed level of quality of the resources is taken into account. – The services requiring early recovery are recovered using available resources on a best-effort basis even if their quality requirements are partly satisfied. – Network connections among interworking CSPs are instantaneously established or reconfigured. The lead CSP, which is preconfigured and governs the recovery procedure, manages the roles of available CSPs and instructs service continuation based on the original CSP data. – Access from CSCs is appropriately distributed to the interworking CSPs so as to achieve the disaster recovery and thus mitigate the service discontinuity.
Information flow	– Relevant CSPs are supposed to join a common trusted alliance (federation) in advance and set up the service level agreements (SLAs). – The lead CSP, which is preconfigured and governs the recovery procedures, inquires about the resource availability of other CSPs in the alliance to recover its cloud services to meet quality requirements of the CSCs. The requested CSPs reply whether or not they are able to lease the resources. – The cloud resource management (e.g., CRUD: create, read, update and delete) is operated across multiple CSPs. The management is to enable leasing of cloud resources from different CSPs in the alliance. – The relevant CSPs exchange monitoring and auditing information of the leased resources.

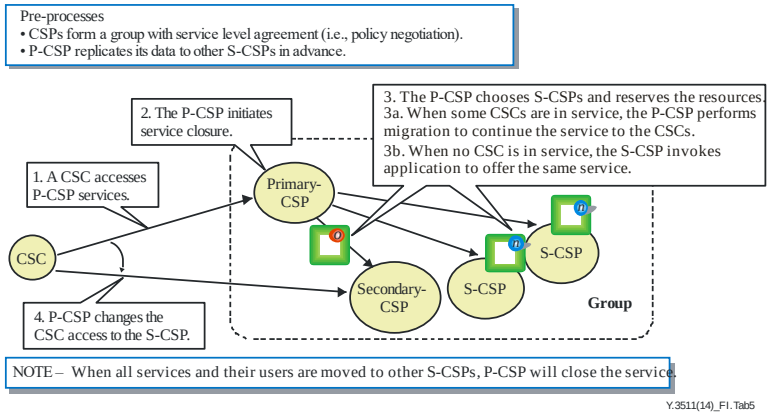
Table I.4 – Inter-cloud use case: Guaranteed availability in the event of a disaster or large-scale failure

Use case	
High-level figure describing the use case	
Derived requirements for cloud capability	The system is required to support: – Policy negotiation including SLA management among the multiple CSPs within a pre-established group; – Self-activity monitoring at a CSP or mutual activity monitoring among the CSPs in a pre-established group. If the activity disappears, the detecting CSP should initiate the pre-configured actions; – Discovery, reservation, use and release of cloud resources in a dynamic manner (i.e., not relying on the pre-configuration) on other CSPs within the federation; – Application invocation over the reserved resources on other CSPs within the federation; – Alteration and reversion (i.e., switchover and switchback), in a dynamic manner (i.e., not relying on the pre-configuration), of CSC access to any CSP within the federation; – Exchange of monitoring and auditing information among the multiple CSPs within the federation; – Exchange of authentication information about CSC (user/enterprise) authentication status among the multiple CSPs within the federation.

I.5 Service continuity (in the case of service termination of the original CSP)

Table I.5 shows an inter-cloud use case for service continuity in the case of service termination of the original CSP.

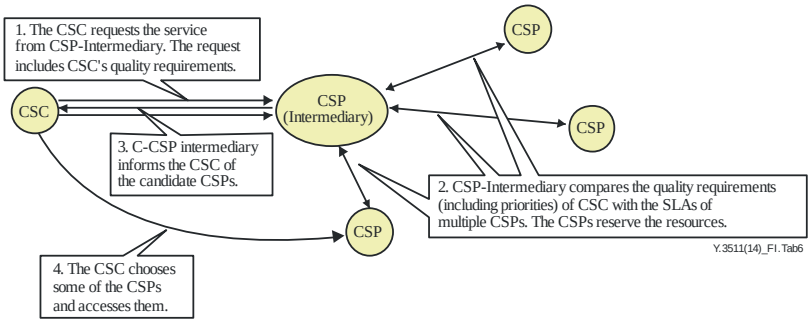
Table I.5 – Inter-cloud use case: Service continuity

Use case	
Use case title	Inter-cloud use case: Service continuity
Relevant roles	CSP and CSC
Use case description	– The cloud service offering continues through the collaboration with other CSPs, even when the original CSP terminates its business. – Available resources in the CSPs other than the service-terminating CSP are discovered and reserved in advance. – Network connections among the interworking CSPs are established or reconfigured. Then service-related data including user identifier (ID), user data and application data are transferred from the original CSP to the new CSPs. – Access from CSCs is appropriately changed to the interworking CSPs so that the same service is continuously offered. – If the capabilities (VM and applications) at the original CSP migrate to other CSPs, the CSC, who keeps the same user ID, can continuously access the service at the same level of performance as before.
Information flow	– The relevant CSPs are supposed to join a common trusted alliance in advance and set up the service level agreements (SLAs). – The terminating CSP inquires about the resource availability of other CSPs in the alliance and requests a reservation of the available resources to continue the services. – The cloud resource management (e.g., CRUD: create, read, update and delete) are operated across multiple CSPs. The management is to enable leasing of the cloud resources from different CSPs in the federation.
High-level figure describing the use case	
Derived requirements for cloud capability	The system is required to support: – Policy negotiation including SLA management among the multiple CSPs within a pre-established group (federation); – Discovery, reservation, use and release of the cloud resources in a dynamic manner (i.e., not relying on the pre-configuration) across the multiple CSPs within the federation; – Capability migration (e.g., VM and applications) among multiple CSPs within the federation; – Alteration (i.e., switchover) of the CSC access, in a dynamic manner (i.e., not relying on the pre-configuration), from one CSP to another CSP within the federation; – Exchange of authentication information about CSC (user/enterprise) authentication status among the multiple CSPs within the federation.

I.6 Market transactions in inter-cloud intermediary pattern

Table I.6 shows inter-cloud use case for market transactions in inter-cloud intermediary pattern.

Table I.6 – Inter-cloud use case: Market transactions in inter-cloud intermediary pattern

Use case	
Use case title	Inter-cloud use case: Market transactions in inter-cloud intermediary pattern
Relevant roles	CSP and CSC
Use case description	– The primary CSP in an inter-cloud intermediary pattern (CSP-Intermediary) mediates between CSPs meeting the CSC's quality requirements and provides the list of selected CSPs to the CSC. – The CSP-Intermediary coordinates multiple services offered by other CSPs.
Information flow	– The SLAs of the CSPs are submitted to the CSP-Intermediary in advance. – A CSC requests the CSP-Intermediary to select CSPs that provide a service which satisfies the CSC's quality requirements. – The CSP-Intermediary compares the CSC quality requirements with the SLAs of other CSPs. Then the CSP-Intermediary discovers and reserves the CSP resources that meet the CSC's quality requirements. – The CSP-Intermediary returns the CSP candidate list to the CSC. – The CSC selects a CSP or CSPs on the list. – The CSP-Intermediary sends a cloud service adaptation request to the selected CSP to invoke the service and adapt it to concrete cloud services and resources. – The CSP returns an adaptation response to the CSP-Intermediary.
High-level figure describing the use case	
Derived requirements for cloud capability	The system is required to support: – Policy negotiation including SLA management among the multiple CSPs including CSP-Intermediary in a pre-established group; – Discovery, reservation, use and release of cloud resources in a dynamic manner (i.e., not relying on the pre-configuration) on other CSPs within the federation; – Creation of the network connections in a dynamic manner (i.e., not relying on the pre-configuration) from the CSC to the selected CSP that provides the resources; – Flexible reallocation of applications, to meet requirements at different stages in its lifecycle, across multiple CSPs.

Appendix II

Use cases from cloud service providers' views

(This appendix does not form an integral part of this Recommendation.)

This appendix describes nine inter-cloud related use cases from the perspective of the cloud service provider.

Introduction to participants

For the purpose of this analysis, the following participants are considered. Each of the boxes in Figure II.1 represents a cloud service provider (CSP).

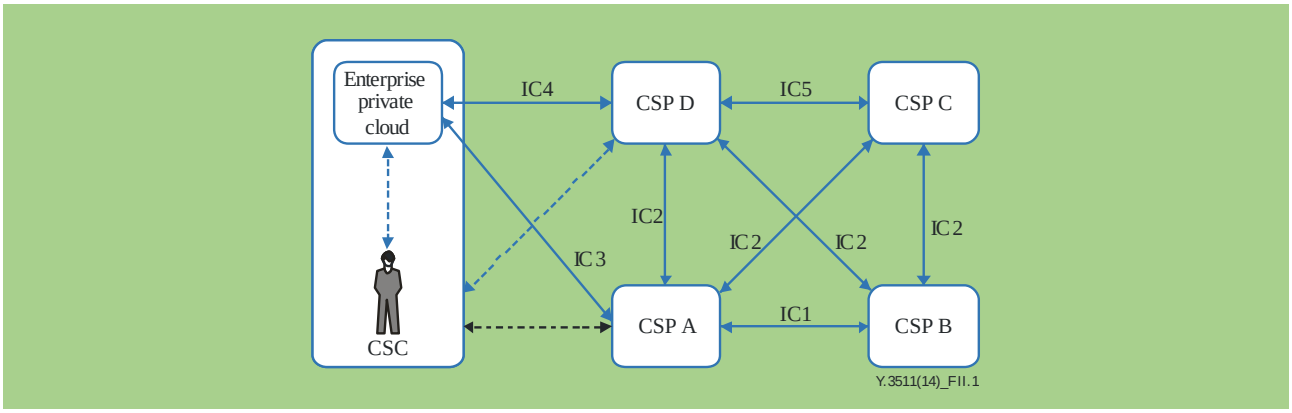


Figure II.1 – Inter-cloud participants and relationships

Participant	Description
User	The human or machine end-user of the overall cloud computing service.
CSP	Cloud service provider: Party (e.g., information technology (IT) or telecom organization) which makes cloud services available. This may include any of the cloud services (SaaS, CaaS, PaaS, IaaS, and NaaS).
Enterprise private cloud	IT resources within an enterprise that are constructed using cloud computing technologies, but which are owned and operated by the enterprise for their own internal use.
Not included for inter-cloud	– Hosting services using non-cloud technologies. – Connectivity services not employing cloud technologies.

The above categorization of participants is for the purpose of use case analysis only and does not imply specific business or regulatory situations. Not all participants identified will be present in all situations. Some organizations may fulfil multiple participant roles.

Relationship	Description
ICn	Inter-cloud relationship (focus of study)

The relationships labelled on the diagram are used to clarify the use cases and do not necessarily indicate information flows or interfaces that require standardization by ITU. The relationships shown as dashed lines (- - - -) in Figure II.1 are included for completeness and are outside the scope of inter-cloud.

II.1 Use case 1 – Cloud service rebranding

CSP-A wishes to offer browser-based office productivity suite services to their users but does not want to run a data centre or build the applications. CSP-A resells the office suite services built and operated by CSP-D, using CSP-A branding, IP network connectivity (IC2), and customer management, while CSP-D develops and maintains the applications and runs the service.

II.2 Use case 2 – Discovery

CSP-A offers a directory service for cloud services to their users. CSP-D and CSP-C both advertise their cloud service offerings into CSP-A's directory (IC2). Enterprise CSC wishes to find a disaster recovery backup provider, uses CSP-A's directory (IC3) to determine that CSP-D offers this service at a good price, and connects with CSP-D via CSP-A's network (IC4) to use the service.

II.3 Use case 3 – Intermediary

CSP-A offers an intermediary service. Enterprise CSC requests the CSP-A to provide hosting of a virtual machine (IC3), CSP-A determines that CSP-D offers the best match of requirements, reserves the resources at CSP-D and creates the necessary connectivity (IC2). Enterprise CSC might or might not know the identity of CSP-D, depending on the requirements of the SLA.

II.4 Use case 4 – Platforming

CSP-D develops a cloud computing application to host consumer music collections under their own brand. CSP-D subscribes to CSP-C's PaaS offering (IC5) and deploys their SaaS application onto CSP-C's PaaS. Consumers connect their devices to CSP-A's application, which is actually running at CSP-C's datacentre (IC2) via virtual private network (VPN).

II.5 Use case 5 – Offloading

Enterprise CSC runs an engineering simulation package which requires significant amounts of computing power at infrequent intervals. CSC's private cloud does not have sufficient peak capacity to handle this effectively, so they have contracted with CSP-A to provide additional compute power (IC3). Due to the success of CSC's business, they now need more peak computing power than CSP-A can provide from CSP-A's own cloud data centre, so CSP-A reserves additional computing resources from CSP-D, handles the load and bills CSC accordingly.

II.6 Use case 6 – Virtual data centre expansion

CSP-A has encountered resistance to expansion of their cloud data centres due to environmental considerations. CSP-A therefore orders 1000 new virtual machine (VM) instances from CSP-D and establishes a VPN bridge such that the new VMs appear to be on the same virtual local area network (LAN) as used in their own data centre.

II.7 Use case 7 – Distributed media

A broadcaster (CSC) will be hosting a major television sporting event series with a global audience and wishes to offer both live and on-demand streaming of the event to many types of devices. CSC requests CSP-A to provide global distribution. CSP-A establishes connection of the live source feeds to CSP-D, which provides secure media reformatting as part of their PaaS offering (IC2), returning digital rights management (DRM)-protected streams/files suitable for playing on many types of devices. CSP-A also develops a global authentication tool and deploys this on PaaS offerings from other CSPs worldwide (IC1, IC2). CSP-A also books capacity in content distribution network (CDN) services worldwide. When the event begins, millions of consumer devices are able to authenticate themselves on their local network provider and stream the content from an efficient local source.

II.8 Use case 8 – Cloud storage expansion

A scientific organization (CSC) collects very large volumes of data in a short period of time that will take years to study. They have sufficient CPU power to analyse this over time but the volume exceeds the storage capacity of their own cloud. CSC contracts with CSP-D to provide additional storage capacity. CSC requests CSP-A to provide very high bandwidth connectivity between CSC and CSP-D. CSC writes the incoming data directly to CSP-D's cloud data storage, and then reduces the network bandwidth to normal levels. CSC is now able to run queries on their data directly at CSP-D or to download interesting parts of the data to their private cloud for intensive processing.

II.9 Use case 9 – Service delivery platform components

A business conference organization (CSC) wishes to rapidly develop and deploy an interactive media conferencing application to multiple venues for an upcoming event. CSP-A offers a service delivery platform (SDP) that includes pre-built components for such services. The CSC developers write their application using several off-the-shelf PaaS, NaaS and CaaS components provided by the SDP platform and are thus able to quickly and reliably create a complex multimedia application and deploy this to CSP-A's SDP.

Appendix III

Abstract service offering models for inter-cloud computing

(This appendix does not form an integral part of this Recommendation.)

This appendix describes several abstract service offering models relevant to inter-cloud computing and provides supplementary information to the description provided in the main body of the Recommendation.

Inter-cloud computing performed over multiple CSPs allows a CSP (i.e., the primary CSP) to offer new services with respect to expanded service items (cf. clause III.1) and enhanced service operations (cf. clause III.2).

III.1 Service item expansion

In terms of service variety, there are roughly two types of cloud expansions; one refers to adding more of the same resources that the primary CSP already has, and the other refers to adding features based on the resources that differ from those the primary CSP has.

Figure III.1 shows these two expansions.

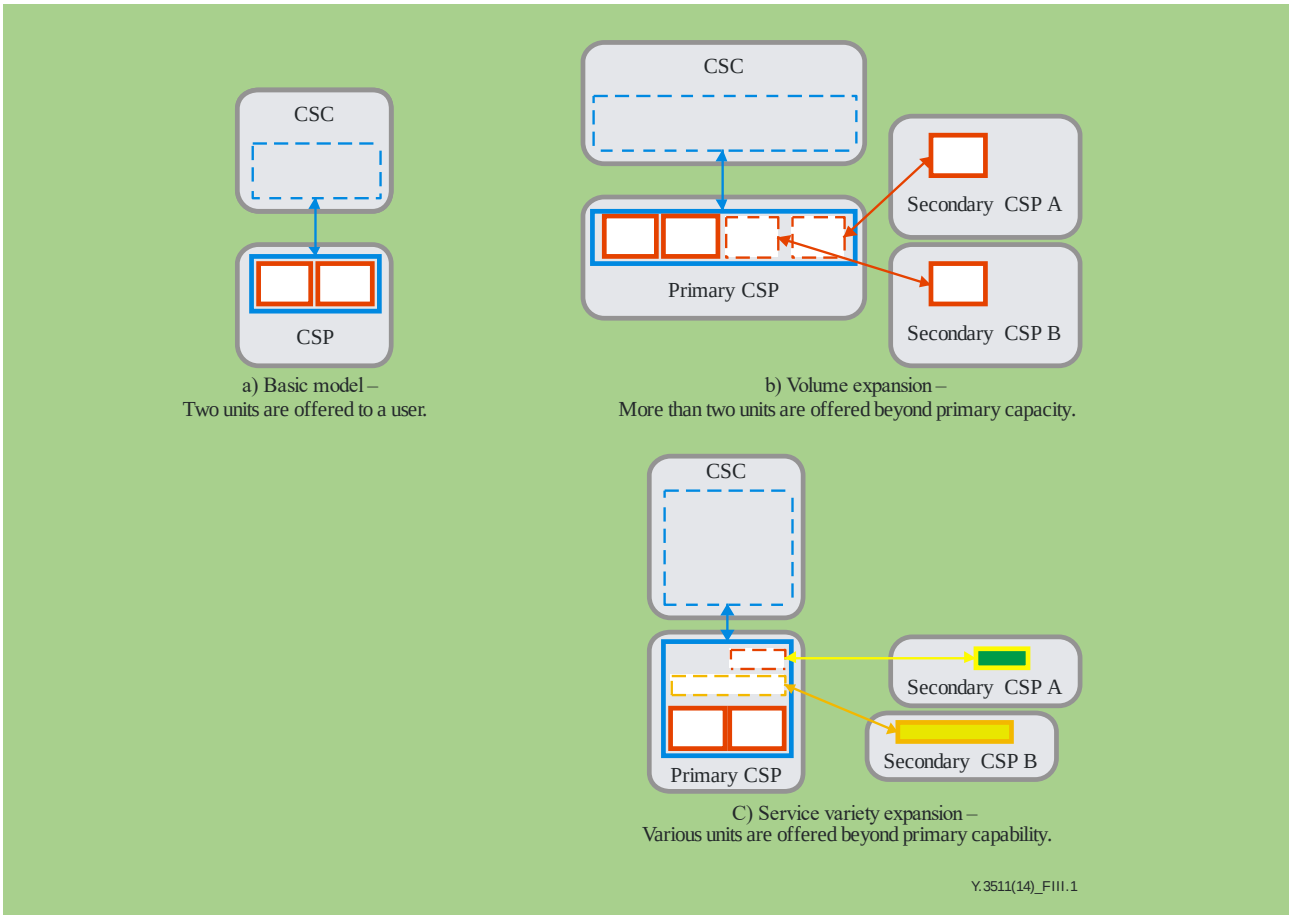


Figure III.1 – Service item expansion – Volume and variety expansions in inter-cloud computing

In the basic model shown in Figure III.1-a, a single CSP offers a service consisting of two resource units. A typical example of such a resource is a virtual machine (VM). The CSP by itself offers two VMs to a given CSC.

In the volume expansion shown in Figure III.1-b, two additional VMs are provided by the secondary CSPs A and B. With their support, the primary CSP can offer a volume-expanded service, which now consists of four VMs.

In the service expansion shown in Figure III.1-c, two new resources that are different from the primary CSP's resource are added by secondary CSPs A and B. These might be software packages or platform-type applications. With the support of the secondary CSPs, the primary CSP can offer a wide-variety service, which now consists of various service components.

From the viewpoint of inter-cloud patterns, which are described in clauses 7 and 8, inter-cloud federation is suitable for volume-based service expansion. The description of the inter-cloud federation in clause 8.2 focuses on resource reservation, use and release. Inter-cloud intermediary is suitable for variety-based service expansion. The description of the inter-cloud intermediary in clause 8.3 underlines the significance of the catalogue of service offerings.

III.2 Service operation enhancement

Inter-cloud interaction enables not only service expansion as described in clause III.1, which matters more at the beginning of a service offering, but can also enhance the ways that services are offered. This relates more to the entire process of offering a service.

Figure III.2 shows two such enhancements.

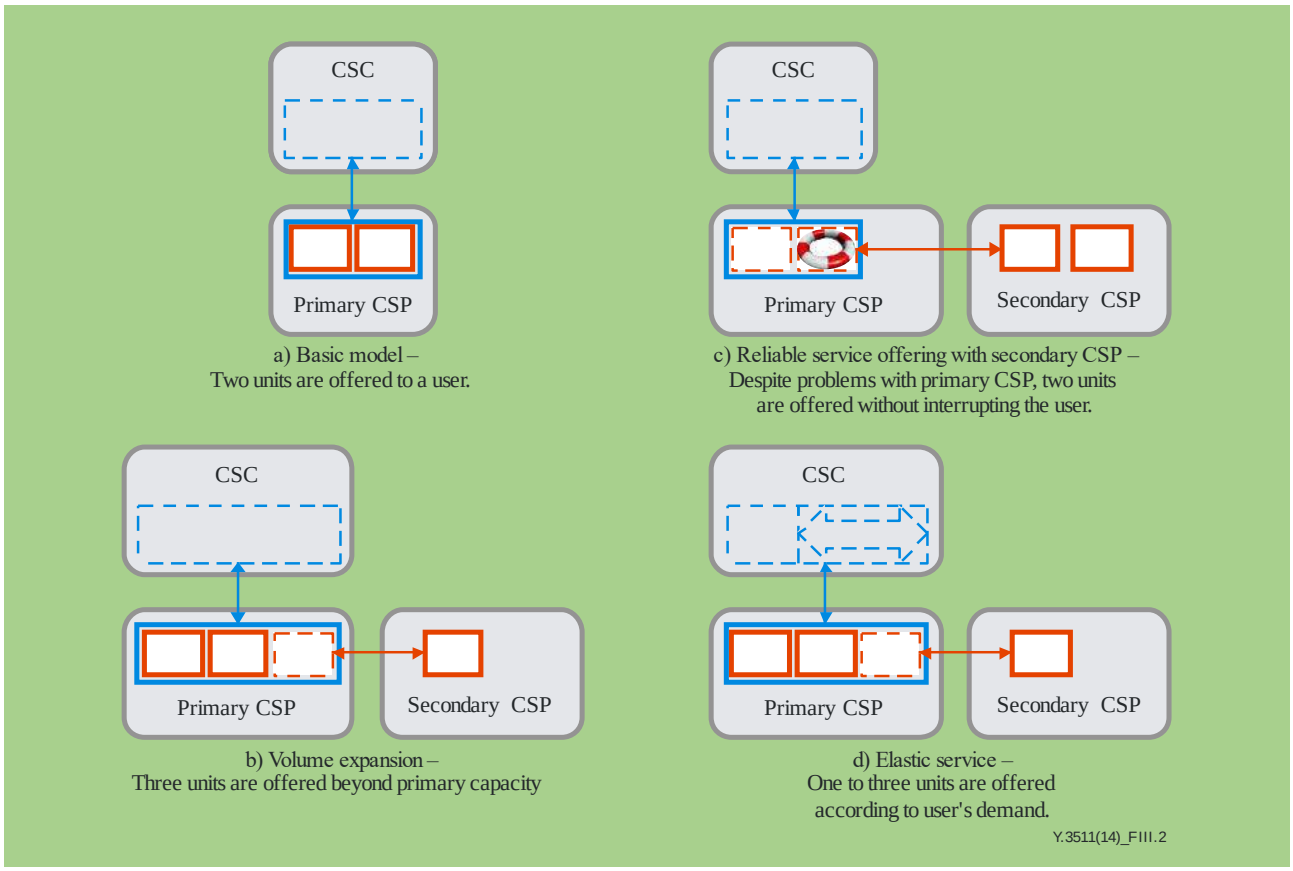


Figure III.2 – Operational enhancement in inter-cloud computing

In Figure III.2, volume expansions are assumed. For the sake of comparison, Figures III.2-a and III.2-b depict item expansion as already discussed in clause III.1, whereas cases c) and d) depict operation enhancement.

The basic scenario is shown in Figure III.2-a again, which offers two resource units (e.g., two VMs) to a user. A simple service item expansion is shown in Figure III.2-b.

With the help of secondary CSPs, the primary CSP can keep offering the service even if something unexpected happens to the primary CSP, which is shown in Figure III.2-c. Due to the availability of cloud technology across multiple CSPs, the secondary CSP can compensate for the unavailable resources by offering alternative resources on behalf of the primary CSP. The primary CSP can offer the same service continuously with minimal or no interruption to the user.

Another scenario, shown in Figure III.2-d is to offer an elastic service, in which the service capacity is adjusted in accordance with the user's demand. In this scenario, the secondary CSP should start and stop its resource offering according to the primary CSP's control. Interaction with the user involves changing the resource offering.

III.2.1 CSC-initiated operation and CSP-initiated operation

Looking at the scenarios in Figure III.2 from the viewpoint of who initiates operations, the reliable service in Figure III.2-c and the elastic service in Figure III.2-d are different.

With the reliable service, the service continuity should be achieved without disturbing the user. The problem should be solved on the CSP side, without necessarily revealing the problem to the user. This may impose a specific requirement. In order not to disturb the user, the primary and secondary CSPs should move the user application, if necessary, and continue the service by themselves. This may include installation and activation of the user application.

The requirement for resource set-up and activation, which is described in clause 9.5, corresponds to this case.

With the elastic service, the CSC may change the use of the CSP's resources explicitly or the primary CSP may change the resource offerings by somehow sensing the CSC's demand.

III.3 Consideration on network connectivity

The description here is meant to supplement clauses 8.2.3 and 8.3.3 on network connectivity.

Networks should, at least, support connectivity between the CSC and the CSP, between the CSPs, and within the CSPs. Based on the primary-secondary model of inter-cloud computing over multiple CSPs, these network parts correspond to:

1) a network between the CSC and the primary CSP;

2) networks between the primary and the secondary CSPs;

3) a network in the primary CSP, and;

4) networks in the secondary CSPs.

From the CSP's perspective, networks 1) and 2) are external, whereas networks 3) and 4) are internal.

Figure III.3 explicitly shows the external networks of 1) as "Network Q" and 2) as "Network X", "Network Y", and "Network Z".

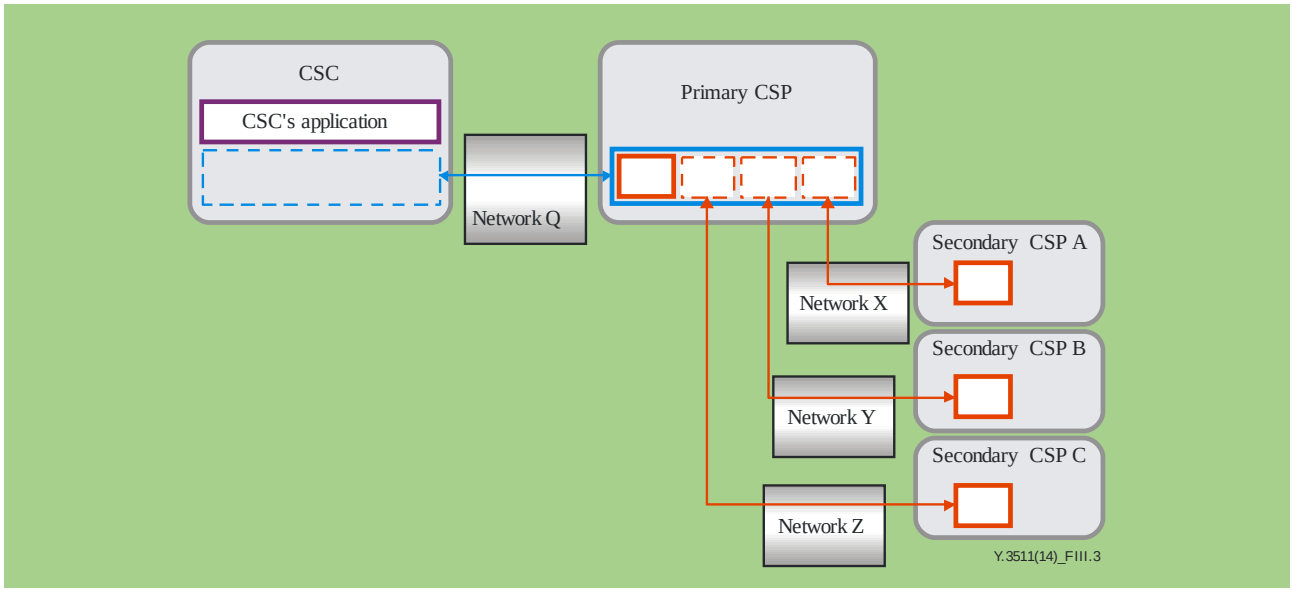


Figure III.3 – Networking in inter-cloud

More networks can be involved as shown in the example provided in Figure III.4.

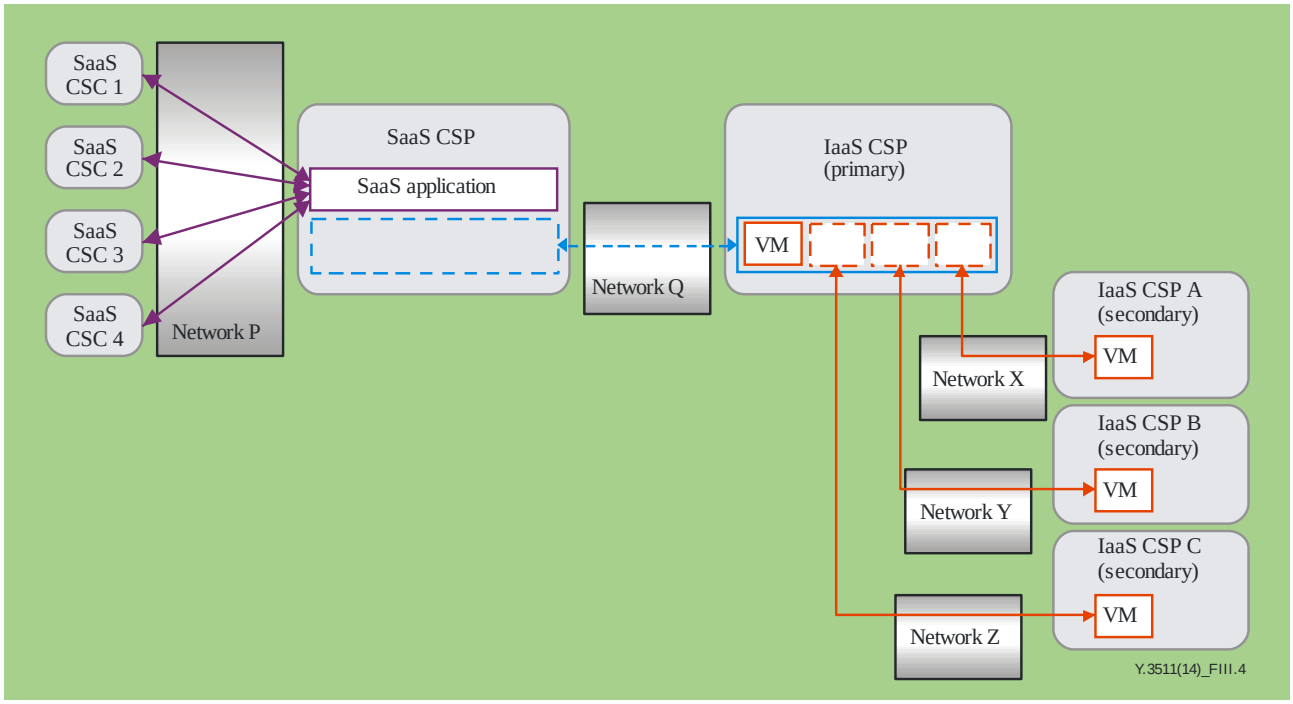


Figure III.4 – Inter-cloud view including SaaS CSCs

In Figure III.4, the IaaS CSP (right side of the figure) provides VMs for the SaaS CSP in order to provide its SaaS application for SaaS CSCs (left side of the figure). In this case, the SaaS CSCs use the SaaS application provided by the SaaS CSP. The SaaS CSP uses VMs, which are provided by IaaS CSPs, on which the SaaS application is executed. Some of the actual VMs are provided by the primary CSP, and some are provided by the secondary CSPs.

Figure III.5 shows the same service offering in a different representation.

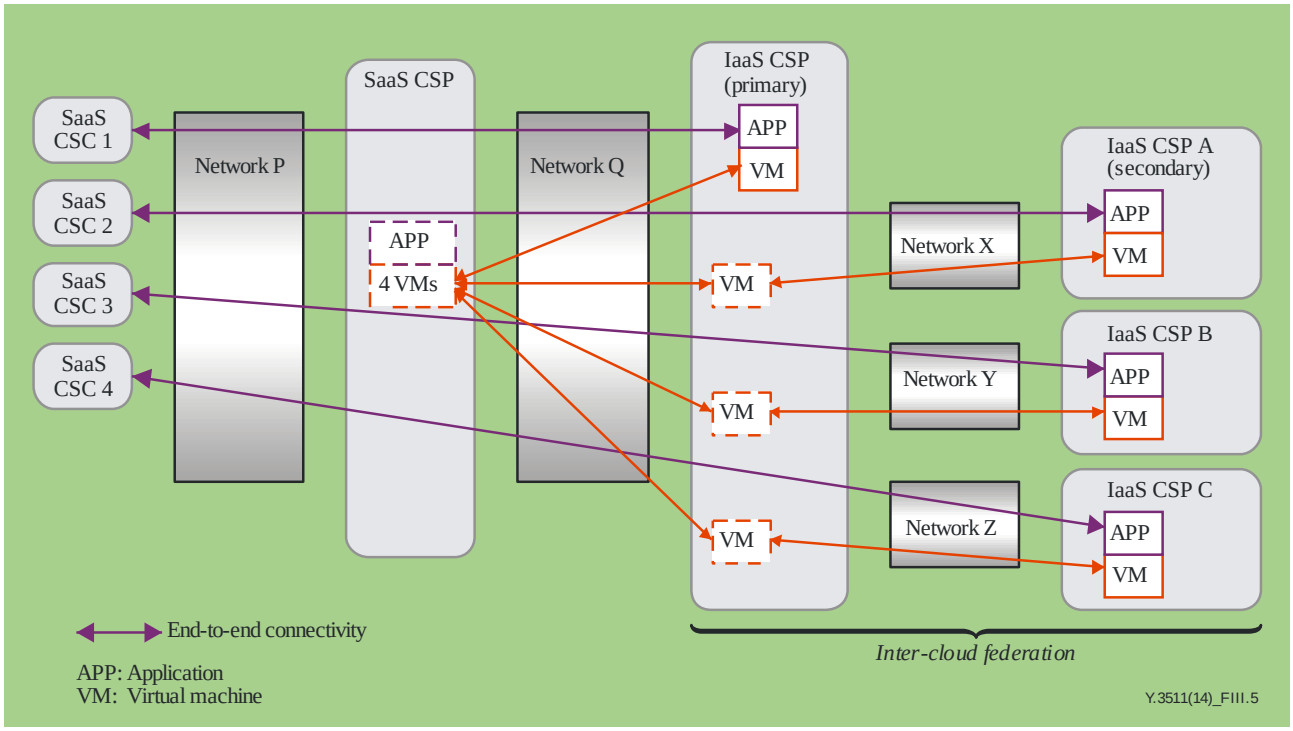


Figure III.5 – View highlighting actual running VMs and application locations (same Figure 8-5)

The SaaS CSCs expect an application service to be provided by the SaaS CSP. In reality, the SaaS CSP relies on IaaS CSP resources and runs its application over the IaaS-CSP's resources. From the IaaS CSP's perspective, the IaaS CSP should, at least:

1) provide VMs, which are now distributed over multiple secondary IaaS CSPs,

2) keep running the application over the distributed VMs, and

3) allow continuous access to the distributed applications from the user (i.e., SaaS CSC users).

In response to the expectations of 1), 2), and 3) above, specific requirements are derived.

The requirements on general resource handling in clauses 9.1, 9.2, 9.3, 9.4, and 9.7 relate to 1).

The requirements on resource set-up and activation in clause 9.5 relate to 2).

The requirements on switchover and switchback of the cloud service user access in clause 9.6 relate to 3).

In a simple implementation, these different networks are designed and operated independently. Such a network configuration is straightforward and easy to operate. However, it may cause inefficient operation, where the user traffic path traverses through an unnecessary route with longer delay. In more sophisticated implementations, the locations of these users, providers and VMs are taken into account and more efficient operation will be achieved.

The capabilities of the networks shown in Figure III.5 may be further offered as NaaS. The detailed requirements and functions for NaaS are under study.

Appendix IV

Inter-cloud security aspects

(This appendix does not form an integral part of this Recommendation.)

This appendix provides important aspects to be considered regarding inter-cloud security matters.

One important aspect is the multiple and sometimes complicated CSP and CSC inter-cloud relationships such as those described in clause 7 of this Recommendation. For these multiple inter-cloud relationships, appropriate secured mechanisms should be supported during the peer CSPs interactions such as the services request phase (e.g., access control), service usage phase as well as the security of network connectivity between the CSPs.

Other aspects to be considered include:

– Establishment of a trust relationship between CSPs is important given that the multiple CSPs involved in inter-cloud may be administrated by different parties. In case of an inter-cloud federation, the involved CSPs may establish trust relationships among them prior to any interactions between them or during inter-cloud interactions (e.g., service requests between CSPs);

– CSC profiles may be shared among the CSPs involved in the federation. In this case the CSC profile should be handled in a secure manner and in respect of privacy rules and regulations.

Bibliography

[b-ITU-T Y.3510] Recommendation ITU-T Y.3510 (2013), *Cloud computing infrastructure requirements.*

[b-ISO/IEC 20000-1:2011] ISO/IEC 20000-1:2011, *Information technology – Service management – Part 1: Service management system requirements*.

[b-FG Cloud TR-Part 1] FG Cloud TR-Part 1 (2012), *Technical Report: Part 1: Introduction to the cloud ecosystem: definitions, taxonomies, use cases and high-level requirements*, http://www.itu.int/pub/T-FG-CLOUD-2012-P1.


BIG DATA

Big data – Cloud computing based requirements and capabilities

Recommendation ITU-T Y.3600

(11/2015)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Summary

Recommendation ITU-T Y.3600 provides requirements, capabilities and use cases of cloud computing based big data as well as its system context. Cloud computing based big data provides the capabilities to collect, store, analyse, visualize and manage varieties of large volume datasets, which cannot be rapidly transferred and analysed using traditional technologies.

Keywords

Big data, big data ecosystem, cloud computing, data analytics, data storage, real-time analysis.

Table of Contents

1 Scope

This Recommendation provides an approach to use cloud computing to meet existing challenges in the use of big data. This Recommendation addresses the following subjects:

- Overview of big data;
  - Introduction to big data;
  - Big data ecosystem and roles;
  - Relationship between cloud computing and big data;
- Cloud computing based big data system context and benefits;
- Cloud computing based big data requirements;
- Cloud computing based big data capabilities.

Note that use cases of cloud computing based big data are provided in Appendix I and II.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing*.

[ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary*.

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014) | ISO/IEC 17789:2014, *Information technology – Cloud computing – Reference architecture*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 **activity** [ITU-T Y.3502]: A specified pursuit or set of tasks.

3.1.2 **cloud computing** [ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications and storage equipment.

3.1.3 **cloud service customer** [ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

NOTE – A business relationship does not necessarily imply financial agreements.

3.1.4 **cloud service partner** [ITU-T Y.3500]: Party which is engaged in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer, or both.

3.1.5 **cloud service provider** [ITU-T Y.3500]: Party which makes cloud services available.

3.1.6 **metadata** [b-ITU-T M.3030]: Data that describes other data.

3.1.7 **role** [ITU-T Y.3502]: A set of activities that serves a common purpose.

3.1.8 **sub-role** [ITU-T Y.3502]: A subset of the activities of a given role.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 big data: A paradigm for enabling the collection, storage, management, analysis and visualization, potentially under real-time constraints, of extensive datasets with heterogeneous characteristics.

NOTE – Examples of datasets characteristics include high-volume, high-velocity, high-variety, etc.

3.2.2 big data as a service (BDaaS): A cloud service category in which the capabilities provided to the cloud service customer are the ability to collect, store, analyse, visualize and manage data using big data.

3.2.3 party: Natural person or legal person, whether or not incorporated, or a group of either.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
BDaaS	Big Data as a Service
BDAP	Big Data Application Provider
BDC	Big Data service Customer
BDIP	Big Data Infrastructure Provider
BDSP	Big Data Service Provider
BDSU	Big Data Service User
CCRA	Cloud Computing Reference Architecture
CDR	Charging Detailed Record
CGF	Charging Gateway Function
CSC	Cloud Service Customer
CSN	Cloud Service partner
CSP	Cloud Service Provider
DP	Data Provider
DPI	Deep Packet Inspection
HTML	Hyper Text Mark-up Language
IaaS	Infrastructure as a Service
IoT	Internet of Things
PDA	Personal Digital Assistant
PDSN	Packet Data Serving Node
SNS	Social Network Service
SQL	Structured Query Language
XML	Extensible Markup Language

5 Conventions

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

In the body of this document and its annexes, the words shall, shall not, should, and may sometimes appear, in which case they are to be interpreted, respectively, as is required to, is prohibited from, is recommended, and can optionally. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative are to be interpreted as having no normative intent.

6 Overview of big data

6.1 Introduction to big data

With the rapid development of information and communications technology (ICT), Internet technologies and services, huge amounts of data are generated, transmitted and stored at an explosive rate of growth. Data are generated by many sources and not only by sensors, cameras or network devices, but also by web pages, email systems and social networks as well as by many other sources. Datasets are becoming so large and so complex or are arriving so fast that traditional data processing methods and tools are inadequate. Efficient analytics of data within tolerable elapsed times becomes very challenging. The paradigm being developed to resolve the above issues is called big data.

For the purpose of this Recommendation it is understood, that within the big data ecosystem, data types include structured, semi-structured and unstructured data. Structured data are often stored in databases which may be organized in different models, such as relational models, document models, key-value models, graph models, etc. Semi-structured data does not conform to the formal structure of data models, but contain tags or markers to identify data. Unstructured data do not have a pre-defined data model and are not organized in any defined manner. Within all data types data can exist in formats, such as text, spreadsheet, video, audio, image, map, etc.

Big data are successfully used in many fields, if traditional methods and tools have become inefficient, where data processing is characterized by scale (volume), diversity (variety), high speed (velocity) and possibly other criteria like credibility (veracity) or business value. These characteristics, usually called the Vs, can be explained as follows:

– Volume: refers to the amount of data collected, stored, analysed and visualized, which big data technologies need to resolve;
– Variety: refers to different data types and data formats that are processed by big data technologies;
– Velocity: refers to both how fast the data is being collected and how fast the data is processed by big data technologies to deliver expected results.

NOTE – Additionally, veracity refers to the uncertainty of the data and value refers to the business results from the gains in new information using big data technologies. Other Vs can be considered as well.

Taking into account the above Vs' described characteristics, big data technologies and services allow many new challenges to be resolved and also create more new opportunities than ever before:

– Heterogeneity and incompleteness: Data processed using big data can miss some attributes or introduce noise in data transmission. Even after data cleaning and error correction, some incompleteness and some errors in data are likely to remain. These challenges can be managed during data analysis. [b-CRA-BDWP]
– Scale: Processing of large and rapidly increasing volumes of data is a challenging task. Using data processing technologies, the data scale challenge was mitigated by the evolution of processing and storage resources. Nowadays however data volumes are scaling faster than resources can evolve. Technologies such as parallel databases, in memory databases, non-SQL databases and analytical algorithms allow this challenge to be resolved.

– Timeliness: The acquisition rate and timeliness, to effectively find elements in limited time that meet a specified criterion in a large dataset, are new challenges faced by data processing. Other new challenges are related to the types of criteria specified and there is a need to devise new index structures and responses to the queries having tight response time limits.

– Privacy: Data about human individuals, such as demographic information, Internet activities, commutation patterns, social interactions, energy or water consumption, are being collected and analysed for different purposes. Big data technologies and services are challenged to protect personal identities and sensitive attributes of data throughout the whole data processing cycle while respecting applicable data retention policy.

Positive resolving of the above challenges opens new opportunities to discover new data relationships, hidden patterns or unknown dependencies.

6.2 Big data ecosystem

This clause describes an environment, called the big data ecosystem through roles and sub-roles. It also defines necessary activities for roles providing and consuming big data services as well as relationships between roles.

The big data ecosystem includes the following roles:

– data provider;

– big data service provider;

– big data service customer.

The big data ecosystem is shown in Figure 6-1.

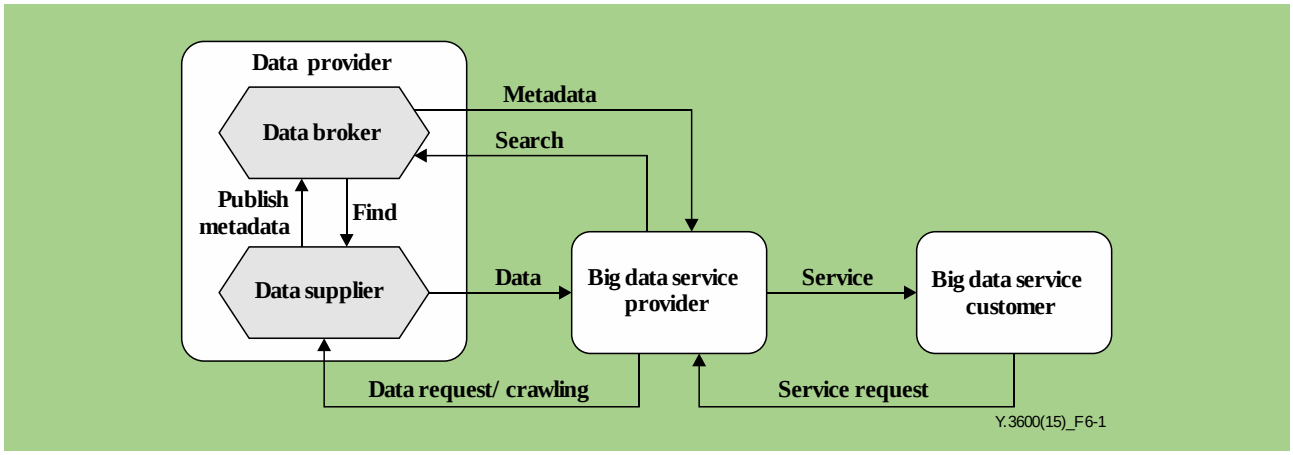


Figure 6-1 – Big data ecosystem

6.2.1 Data provider (DP)

The data provider (DP) role consists of two sub-roles:

– data supplier;

– data broker.

6.2.1.1 Data supplier

The data supplier provides data from different sources to the data broker, which can be accessed by the big data service provider. The data supplier's activities include:

– generating data;

– creating metadata information describing the data source(s) and relevant attributes;

– publishing metadata information to access the metadata.

6.2.1.2 Data broker

The data broker serves to connect between the data supplier and the big data service provider. The data broker can act as a clearinghouse, open data mart, etc. and its activities include:

– providing a meta-information registry to the data supplier for publishing their data sources;

– finding on-line open-data sources and registering corresponding meta-information;

– providing a service catalogue to the big data service provider for searching usable data.

6.2.2 Big data service provider (BDSP)

The big data service provider (BDSP) supports capabilities for big data analytics and infrastructure. The big data service provider can act as a form of big data platform, an extension of the existing data analytics platform, etc. Big data service provider activities include:

– searching data sources (from the data broker) and collecting data by requesting and crawling;

– storing data to a data repository;

– integrating data;

– providing tools for data analysis and visualization;

– supporting data management such as data provenance, data privacy, data security, data retention policy, data ownership, etc.

6.2.3 Big data service customer (BDC)

The big data service customer (BDC) is the end-user or is a system that uses the results or services from a big data service provider. The big data service customer may produce new services or knowledge on consumer activities and furnish them outside of the big data ecosystem. Big data service customer activities include:

– requesting big data services from the big data service provider;

– using the outputs of big data services.

6.3 Relationship between cloud computing and big data

Big data refers to technologies and services which extract valuable information from the extensive datasets characterized by the Vs, while cloud computing is, as defined in [ITU-T Y.3500], the paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

Big data needs on-demand high performance data processing and distributed storage as well as variety of tools required to accomplish activities of the big data ecosystem which are described in clause 6.2. Cloud computing meets the challenges of big data as described in clause 6.1. The burst nature of workloads makes cloud computing more appropriate for big data challenges such as scalability and timeliness. The big data ecosystems, which are supported by a cloud computing system context, can be referred to as cloud computing based big data. Cloud computing based big data is addressed in detail in clause 7.

7 Cloud computing based big data

This clause describes a cloud computing based big data system context that is effective for supporting big data. It also provides benefits of cloud computing based big data.

7.1 Cloud computing based big data system context

Cloud computing based big data system context is described with new sub-roles and activities based on the architectural user view defined in [ITU-T Y.3502]. This clause describes how cloud computing can support the three main roles in a big data ecosystem: data provider, big data service provider and big data service customer.

Cloud computing sub-roles can be mapped to big data roles as shown in Table 7-1.

Table 7-1 – Mapping table between big data ecosystem roles and cloud computing based big data system context sub-roles

Big data ecosystem roles	Cloud computing based big data system context sub-roles
Data provider	CSN:data provider
Big data service provider	CSP:big data infrastructure provider, CSP:big data application provider
Big data service customer	CSC:big data service user

Figure 7-1 illustrates the cloud computing sub-roles for big data. Figure 7-1 also identifies activities specific for big data and assigns them to cloud computing sub-roles. Arrows used in Figure 7-1 show the data and service flows within a cloud computing based big data system context.

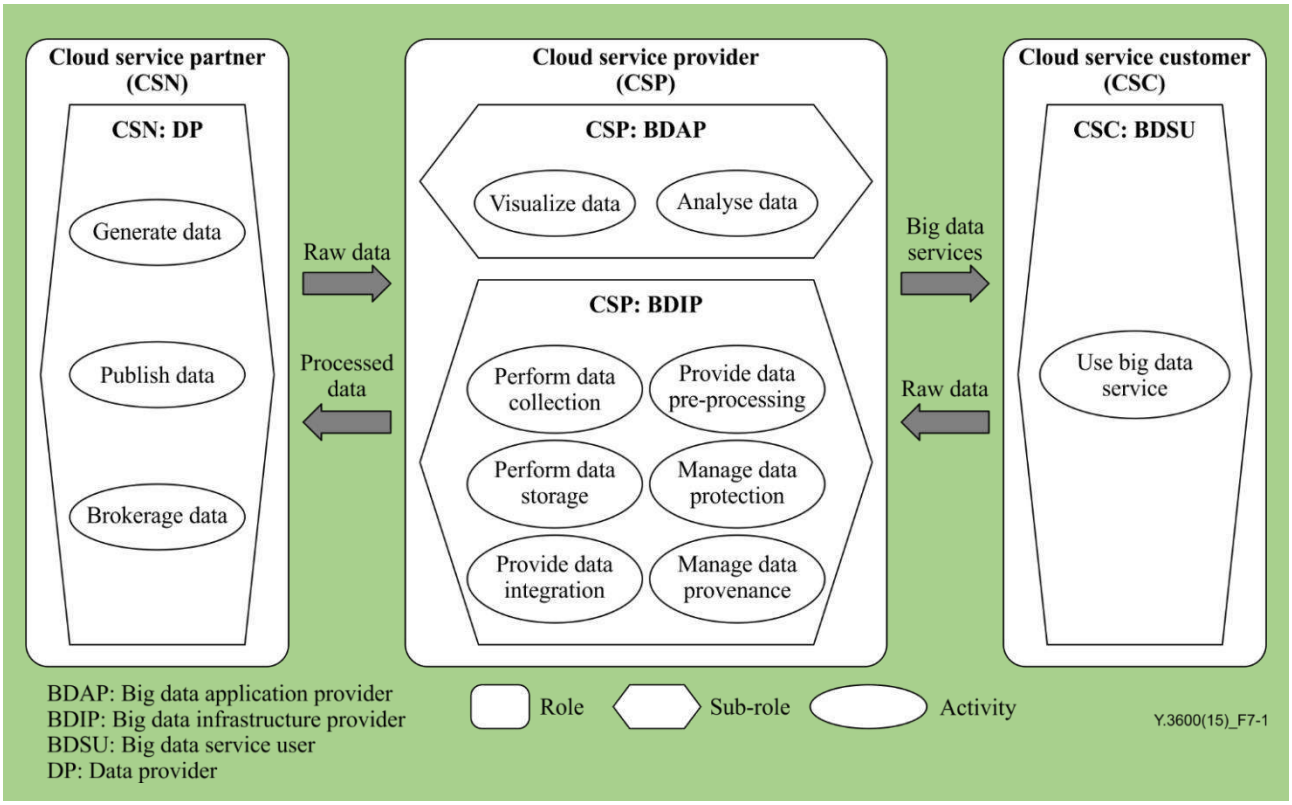


Figure 7-1 – Cloud computing based big data system context

Figure 7-2 illustrates, as an example scenario, how cloud computing supports big data services from the viewpoints of CSP: Big data application providers (BDAPs) and CSP:Big data infrastructure providers (BDIPs). A cloud based big data service, which is provided by a CSP:BDAP or a CSP:BDIP, utilizes other sub-roles of the cloud service provider.

The CSP provides services of application and platform capability types such as software as a service and platform as a service and these services can be used by the CSP:BDAP to perform data analysis, visualization and other big data applications. In addition, the CSP:BDIP can use the cloud services of cloud infrastructure capability types such as compute as a service, data storage as a service, infrastructure as a service and network as a service to perform big data services for data collection, data processing, data management, etc.

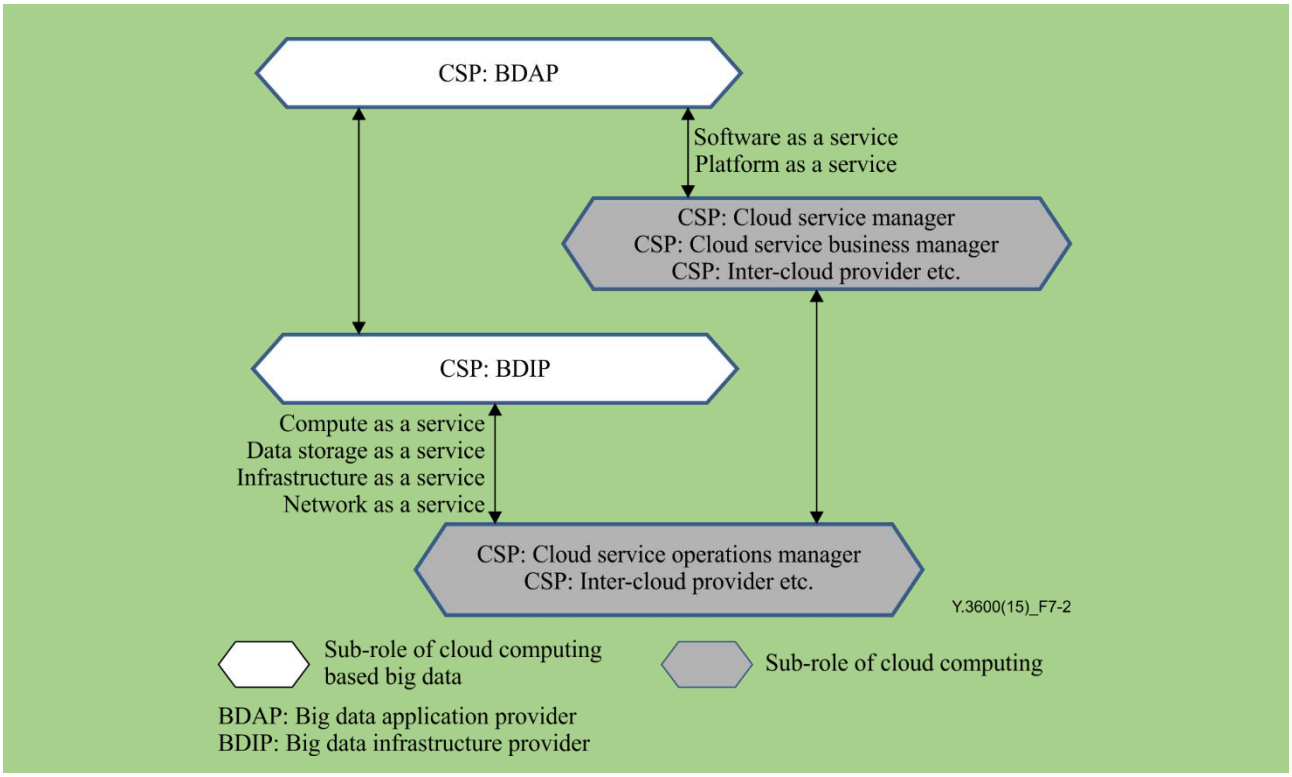


Figure 7-2 – An example scenario of cloud computing support for big data

NOTE – Figure 7-2 considers cloud service categories based on Table A.1 of ITU-T Y.3500.

7.1.1 CSN:data provider (CSN:DP)

CSN:data provider (CSN:DP) is the sub-role of the cloud service partner (CSN) generating and publishing new data or information which feeds into the big data system for discovery, access and transformation. The CSP:data provider's activities include a generate data activity, a publish data activity and a brokerage data activity.

7.1.1.1 Generate data activity

The generate data activity involves gathering data from several kinds of sources. The data can be generated in a variety of types such as structured data, semi-structured data and unstructured data.

The data sources include public data (data from governments, organizations, Internet, etc.), private/enterprise data and application based data, such as social network service (SNS) and Internet of Things (IoT) data.

7.1.1.2 Publish data activity

The publish data activity is the process of registering metadata of data to the CSN. It provides metadata for brokerage data activity.

NOTE – metadata is delivered to the CSP:BDIP through brokerage data (see clause 7.1.1.3) with the data catalogue which includes data access methods, data use policy, etc.

7.1.1.3 Brokerage data activity

The brokerage data activity involves providing metadata of data to the CSP: BDIP.

Types of brokerage data activities include:

– providing a data registry to the CSN:DP for publishing their data sources;
– finding an on-line data source and registering its metadata;
– providing a catalogue to the CSP:BDIP for searching appropriate data.

7.1.2 CSP: big data application provider (CSP:BDAP)

The CSP: big data application provider (CSP:BDAP) is a sub-role of the CSP executing a set of data lifecycle operations to meet the requirements of data analysis and visualization, as well as the security and privacy requirements. The CSP:BDAP utilizes the services from the CSP:BDIP for big data services and provides analysis result to the CSC: big data service user (CSC:BDSU).

Types of CSP:BDAP activities include:

– visualizing data;

– analysing data.

7.1.2.1 Visualize data activity

The visualize data activity is responsible for presenting data with multiple styles, such as statistical graphics, forms, diagrams, charts, reports, etc., through visualization and reporting tools and services. The big data service user (BDSU) can easily and quickly understand the meaning of data through data visualization. Direct interaction between reporting tools and CSC operational systems is also supported.

Types of big data visualize activities include:

– business intelligence;

– data reporting;

– data exploration.

7.1.2.2 Analyse data activity

The analyse data activity is a process to extract and discover useful information or valuable insights from big data.

Types of big data analyse activities include:

– statistical analysis;

– predictive analysis;

– content analysis.

7.1.3 CSP:big data infrastructure provider (CSP:BDIP)

CSP:big data infrastructure provider (CSP:BDIP) is the sub-role of the CSP providing cloud computing resources (such as system hardware, a network, storage and computing platforms) in order to execute big data processing, while protecting the privacy, retention policy and integrity of data.

Types of CSP:BDIP activities include:

– performing data collection;

– performing data storage;

– providing data pre-processing;

– providing data integration;

– managing data protection;

– managing data provenance.

7.1.3.1 Perform data collection activity

The perform data collection activity is responsible for gathering and searching of data. Data in a cloud computing environment that could be transported through Internet, such as web, video, audio, radio frequency identification (RFID), sensor and social network data and data obtained in other ways can be categorized into three types as follows:

– structured data, such as record data persistent in databases;

– semi-structured data, such as data stored in XML, HTML and other format documents;

– unstructured mass data, such as log files, video and audio data.

7.1.3.2 Perform data storage activity

The perform data storage activity allows storing of the data collected and the pre-processing results using storage resources and building of corresponding databases to manage and manipulate the data.

7.1.3.3 Provide data pre-processing activity

The provide data pre-processing activity realizes extraction, transformation and de-noising of the collected data. Since there are many different data formats and data types of the collected data, the transformation and extraction of complex data into simple structured data facilitates and speeds up the data analysis process.

The data de-noising process filters out the defects in data to eliminate negative effects in the normal analysis process.

7.1.3.4 Provide data integration activity

The provide data integration activity is responsible for combining, forming, coordinating or blending data from disparate sources and for solving the issues of bulk data movement, replication, synchronization, virtualization, data quality and data services.

7.1.3.5 Manage data protection activity

The manage data protection activity is responsible for protecting data so that the protected data may not be collected, stored and disclosed to whom may not be appropriate.

7.1.3.6 Manage data provenance activity

The manage data provenance activity manages information about the origin and generation process methods of data. Such information is useful for debugging, transformations, auditing, evaluating the quality of and trust in data, modelling authenticity and implementing access control for derived data.

7.1.4 CSC:big data service user (CSC:BDSU)

CSC:big data service user (CSC:BDSU) is the sub-role of the CSC performed by end-users or other systems in order to use the services from the CSP:BDAP and CSP:BDIP.

Types of CSC:BDSU activities include:

– use big data service;

7.1.4.1 Use big data service

The use big data service involves using the services of a CSP:BDAP and a CSP:BDIP in order to accomplish tasks.

Use big data service activity typically involves:

– provision of user credentials to enable the CSP:BDAP and CSP:BDIP to authenticate the user and grant access to the big data service;
– invocation of the big data service.

7.2 Benefits of cloud computing based big data

One of the main purposes of big data is to extract deep information from large volumes of data. Large volumes of data can be analysed using two key methods; the scale-up method and the scale-out method. The scale-up method uses a large system with enough resources to analyse a huge amount of data. In contrast, the scale-out method uses many separate processing nodes, where each processing node analyses a portion of data. The scale-out method has the ability to scale just by adding more processing nodes. Cloud computing can provide big data with cost-effective elastic processing, storage and network resources.

The key benefits of cloud computing based big data are:

– **Scalability**. Big data needs to have capabilities to store and process large volumes of data. Therefore, scalability is very important for big data. However, the additional systems for big data require a lot of time and cost management. Cloud computing can provide flexible scalabilities to big data without additional expansion of infrastructure. It allows the big data service user to easily upscale or downscale the resources quickly.

– **Resiliency**. Cloud computing can support big data to have resiliency capabilities to maintain an acceptable level of service in the face of faults affecting normal operation.

– **Cost effectiveness**. Big data facilitates fast and scalable data processing such as system log analysis and click streams analysis. For many systems and platforms, there are huge volumes of log data and traditionally databases are used to perform log analysis. But the cost to perform data analysis (including costs of storage, system maintenance, etc.) is too high when traditional mechanisms are used. Cloud computing can offer flexible and scalable resources in a cost effective manner.

– **Efficient analysis**. In order to extract more valuable insights, big data applications and services need a well-defined analytic strategy as well as processing power. The cloud computing based big data service may dynamically use the required resources.

– **Deep information extraction**. Big data develops new business insights and mechanisms including prediction and decision assistance. This is different from conventional systems because the data processing logic to handle the raw data and what kind of information can be extracted from datasets is already known.

8 Requirements of cloud computing based big data

8.1 Data collection requirements

The data collection requirements include:

1) It is required for the CSP:BDIP to support collecting data from multiple CSN:DPs in parallel;

2) It is recommended for the CSN:DP to expose data to the CSP:BDAP by publishing metadata;

3) It is recommended that the CSP:BDIP supports collecting data from different CSN:DPs with different modes;

NOTE – Data could be collected in different modes, such as pull mode in which the data collection process is initiated by CSP:BDIP, or push mode in which the data collection process is initiated by the CSN:DP.

4) It is recommended for the CSN:DP to provide a brokerage service to the CSP:BDIP for searching accessible data;

NOTE – Brokerage provides data a catalogue which has data information such as data specification, data instructions, electronic access methods, license policy, data quality, etc.

5) It is recommended that the CSP:BDIP integrates data delivered by the CSC and data publicly available;

6) Data collection can optionally be performed by the CSP:BDIP in real-time.

8.2 Data pre-processing requirements

The data pre-processing requirements include:

1) It is required for the CSP:BDIP to support data aggregation;

NOTE – Data from different sources can be organized in the same model or data format, as described in clause 6.1.

2) It is recommended that the CSP:BDIP provides the dedicated resources for pre-processing;

NOTE – Pre-processing includes extraction, transformation and de-noising of the collected data.

3) It is recommended that the CSP:BDIP supports unification of data collected in different formats;

NOTE –Unification of data is for example to unify data about persons/locations/dates extracted from web pages, pictures, videos, SNS data and calling logs to text format.

4) It is recommended for the CSP:BDIP to support extraction of data from unstructured data or semi-structured data into structured data.

NOTE – This requirement can be applied also to data storage.

8.3 Data storage requirements

The data storage requirements include:

1) It is required for the CSP:BDIP to support different data types with sufficient storage space, elastic storage capacity and efficient control methods;

2) It is required for the CSP:BDIP to support storage for different data formats and data models;

NOTE – Data formats include text, spreadsheet, video, audio, image, map, etc. Data models include relational models, document models, key-value models, graph models, etc. (as described in clause 6.1).

3) It is required that the CSP:BDIP provides a flexible licensing policy for the databases;

NOTE – As database systems may be covered by vendor licenses, the CSP:BDIP that offers a database as part of the big data service needs the ability to adapt the licensing conditions to the particular service and the CSC:BDSU requirements.

4) It is recommended that the CSP:BDIP provides different types of databases;

NOTE – Examples of database types include relational databases (RDB), object relational databases (ORDB), object oriented databases (OODB), NoSql (not only SQL) databases, etc.

5) It is recommended for the CSN:DP to expose application programming interfaces (APIs) for data delivery;

6) It is recommended that the CSP:BDIP fulfils storage and database performance demands.

7) It is recommended that the CSP:BDIP supports a data retention policy covering a data retention period before its destruction after termination of a contract. This is to protect the big data service customer from losing private data through an accidental lapse of the contract.

8.4 Data analysis requirements

The data analysis requirements include:

1) It is required for the CSP:BDAP to support analysis of various data types and formats;

2) It is required for the CSP:BDAP to support batch processing;

3) It is required for the CSP:BDAP to support association analysis;

NOTE – Association analysis is the task of uncovering relationships among data.

4) It is required for the CSP:BDAP to support different data analysis algorithms;

NOTE – Data analysis algorithms include classification, clustering, regression, association, ranking, etc.

5) It is required that the CSP:BDAP provides flexible licensing policy for the analytical applications;

6) It is recommended for the CSP:BDAP to support user defined algorithms;

7) It is recommended for the CSP:BDAP to support data processing in distributed computing environments;

8) It is recommended for the CSP:BDAP to support data indexing;

9) It is recommended that the CSP:BDAP supports data classification in parallel;

10) It is recommended that the CSP:BDAP provides different analytical applications;

11) It is recommended that the CSP:BDAP supports customization of analytical applications;

12) It is recommended for the CSP:BDAP to support real-time analysis of streaming data;

13) It is recommended for the CSP:BDAP to support user behaviour analysis;

NOTE – User behaviour includes user-related information, collected users' behaviour in real-time, environmental information and the analysed information from the cumulative users' information on a CSP:BDIP's storage. Scope of behaviour analysis is based on the user's agreement in advance.

14) The CSP:BDAP can optionally perform analysis of different data types and formats in real-time.

8.5 Data visualization requirements

The data visualization requirements include:

1) It is required that the CSP:BDAP provides a flexible licensing policy for the reporting tool;
2) It is recommended that the CSP:BDAP supports different tools or plug-ins with multiple styles of data visualization;

   NOTE – Visualization styles include statistical graphics, forms, diagrams, charts, etc.
3) It is recommended that the CSP:BDAP supports customization of the reporting tools;
4) It is recommended that the CSP:BDAP supports integration of reporting tools with CSC reporting systems;
5) It is recommended that the CSP:BDAP supports integration of reporting tools with CSC operational systems;
6) It is recommended that the CSP:BDAP supports composed services which could combine two or more big data services to the CSC:BDSU.

8.6 Data management requirements

The data management requirements include:

1) It is required for the CSP:BDIP to manage metadata information such as creating, controlling, attributing, defining and updating;

   NOTE – Metadata contains critical information such as persistent identification of the data, the fixity and the access rights of the stored data.
2) It is required for the CSP:BDIP to track a data history which contains the source of data and the data processing method;
3) It is required for the CSP:BDAP to support distributed cluster monitoring tools to monitor the health and status of computing clusters;
4) It is required for the CSP:BDIP to support data preservation policy management rules;

   NOTE – Provided rules include data retirement and refreshment methods.
5) It is recommended for the CSP:BDIP to support network resource monitoring;
6) It is recommended for the CSP:BDIP to support management of data lifecycle operations;

   NOTE – Data lifecycle operations include data generation, transmission, storage, use and deletion.

8.7 Data security and protection requirements

The data security and protection requirements include:

1) It is required for the CSP:BDIP to protect data collection, data storage, data transmission and data processing with security mechanisms;
2) It is required for the CSP:BDIP to support data protection;
3) It is required that the CSP deletes CSC related data and analytical results according to the lifetime defined by the CSC or on the CSC's demand;
4) It is recommended that the CSP supports implementing the CSC's data protection and security policies over data and analytical results;
5) It is recommended that the CSP:BDIP supports redundancy mechanisms and transaction logging.

9 Cloud computing based big data capabilities

9.1 Data collection capabilities

Data collection capabilities include:

– Data source intelligent recognition, which offers the capabilities to locate the data sources and detect the types of data being collected;

– Data adaptation, which offers the capabilities to transform and organize the data being collected with targeted data structures and attributes (numbering, location, ownerships, etc.);

– Data integration, which offers the capabilities to integrate data from different data sources (different data types) using metadata or ontology;

– Data brokerage, which offers the capabilities to provide a brokerage service for searching data.

9.2 Data pre-processing capabilities

Data pre-processing capabilities include:

– Data extraction, which offers the capabilities to extract information from the semi-structured data or unstructured data;

– Data transmission, which offers the capabilities to transport datasets (static data and real-time data) from data sources or between one location to another keeping the integrity and consistency;

– Data de-noising, which offers the capabilities to eliminate noise information from a mixture of signal data and noise data;

– Data aggregation, which offers the capabilities to aggregate data which come from different sources in the same data model or data format.

9.3 Data storage capabilities

Data storage capabilities include:

– Data storing, which offers the capabilities to store different types and formats of data with elastic storage capacity;

– Data registration, which offers the capabilities to create, update and delete the metadata with corresponding changes in data storage;

NOTE – In the case of unstructured data registration, the data registration component can request the transforming of raw data to semi-structured data such as JavaScript object notation (JSON) or binary JavaScript object notation (BSON) to define semantic relationships among different datasets for knowledge sharing.

– Data access, which offers the capabilities to access data through multiple interfaces, such as web service interfaces, file system interfaces, database interfaces and so on;

– Data indexing, which offers the capabilities to create and update indexes for datasets;

– Data duplication and backup, which offers the capabilities to duplicate and make backups for datasets.

9.4 Data analytics capabilities

Data analytics capabilities include:

– Data preparation, which offers the capabilities to transform data into a form that can be analysed. These capabilities include exploring, changing and shaping of the raw data;

– Data analysis, which offers the capabilities of investigation, inspection and modelling of data in order to discover useful information;

– Workflow automation, which offers the automation processes, in whole or part, during which data or functions are passed from one step to another for actions, according to a set of procedural rules;

– Analysis algorithm adaptation, which offers the capabilities to apply algorithms of classification, regression, clustering, association rules, ranking, etc. to process the datasets according to the CSC demands;
– Distributed processing, which offers the capabilities to distribute the processing tasks to a cluster of computing nodes;
– Data application, which offers the capabilities to support applications or application plug-ins to use the analysis results of datasets.

9.5 Data visualization capabilities

Data visualization capabilities include:

– Data visualization, which offers the capabilities to create, configure, deliver and customize the visual representation of data analysis results.
– Data reporting, which offers the capabilities to make reports of summary, key elements and analysis results of datasets.

9.6 Data management capabilities

Data management capabilities include:

– Data provenance, which offers the capabilities to manage information pertaining to any source of data including the party or parties involved in generation and introduction processes for data;
– Data preservation, which offers the capabilities to manage the series of activities necessary to ensure continued access to data according to relevant policy;
– Data ownership, which offers the capabilities to manage property rights of data possession and disposition according to the change of data status (e.g., after data integration);
– Processes monitoring, which offers the information related to data processing;

NOTE – This capability can include information such as the success of the job and task, running time, resource utilization, etc.

– Metadata management, which offers the capabilities of creating, defining, attributing, controlling and updating metadata information.

9.7 Data security and protection capabilities

Data security and protection capabilities include:

– Access control, which offers the capabilities to manage the rights of parties to control or influence the information related to them;
– Policy control, which offers the capabilities to control policies of data protection and security;
– Data security, which offers the capabilities to apply the storage, network and service related security mechanisms, including administrative, operational and maintenance issues.

10 Security considerations

Security aspects for consideration within cloud computing environments, including cloud infrastructure, IaaS, NaaS, DaaS are addressed by security challenges for CSPs, as described in [ITU-T X.1601]. In particular, [ITU-T X.1601] analyses security threats and challenges, and describes security capabilities that could mitigate these threats and meet security challenges.

Relevant security requirements of [b-ITU-T Y.2201], [b-ITU-T Y.2701] and applicable X, Y and M series of ITU-T Recommendations need to be taken into consideration, including access control, authentication, data confidentiality, data retention policy, network security, data integrity, availability and privacy.

Appendix I

Use cases of cloud computing in support of big data

(This appendix does not form an integral part of this Recommendation.)

Table I.1 – Personalization customized service using big data

Title	Personalization customized service using big data
Description	There are lots of network devices such as laptop computers, smart phones, smart pads, PDAs, health equipment, etc. Owners of these devices can access Internet and support network services in order to get some information, to buy something, to see movies, etc. Each activity might be logged such as network access information, records of visiting a website as well as usage of a service category in network service providers. This data volume can be of a tremendous size due to so many devices accessing Internet at same time. Consequently, data processing can become a big data problem. More meaningful information can however be extracted from big data. In this scenario, the CSP:BDIP should have capabilities to collect data and store said data, and the CSP:BDAP should have capabilities to analyse data which are related to the web service user's activities. The CSP:BDAP also has the task of providing the results of analysis to the CSC:BDSU. CSP:BDIP can store relevant information of the web service user's activities in the big data storage and provides this data to the CSP:BDAP. The CSP:BDAP can receive requests for operations with data and get some other information (e.g., weather information, season, holiday information, etc.) from external data sources which are supported by the CSN:DP. The CSP:BDAP may know the patterns or preferences of the user through analysis of the user's activities and pre-stored information. The CSP:BDAP can then provide the user's pattern information and the user's preferences to the CSC:BDSU. Such information is very helpful in enabling the CSC:BDSU to advertise to or support the web service users.
Roles/sub-roles	– CSP:BDIP – CSP:BDAP – CSN:DP – CSC:BDSU

Table I.1 – Personalization customized service using big data

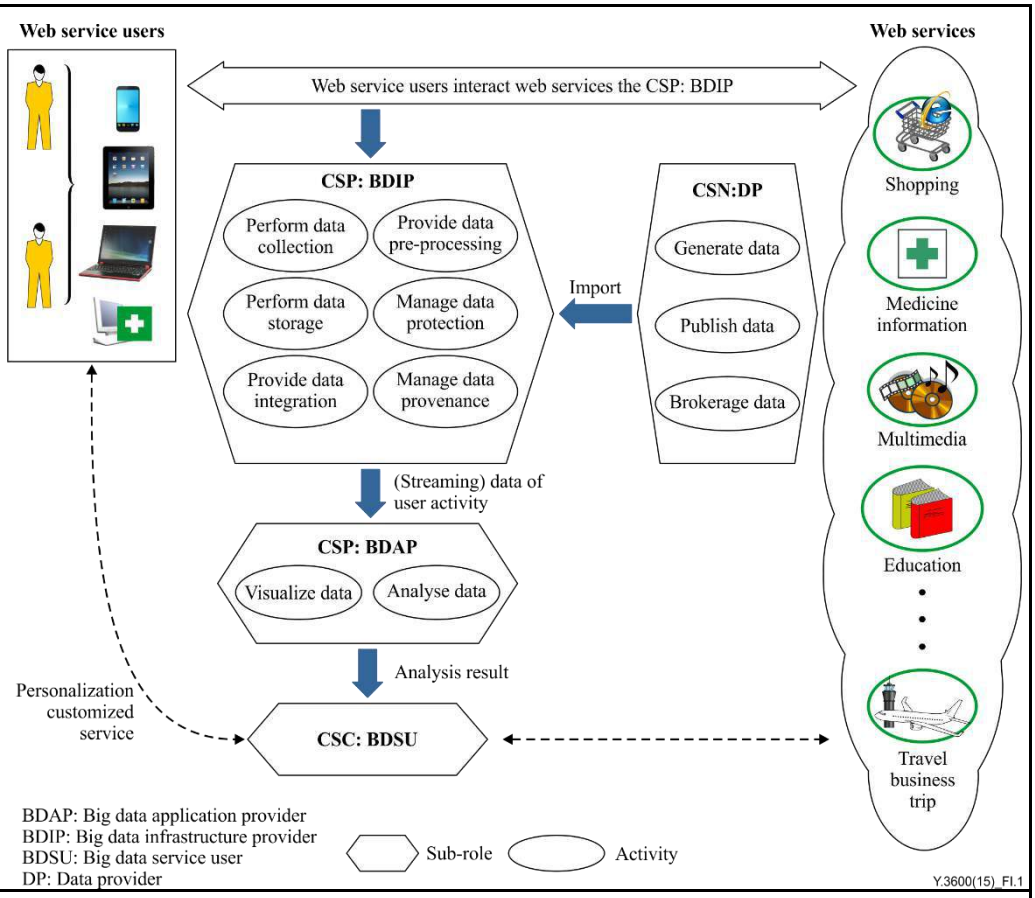
Figure	
Pre-conditions (optional)	– The CSP:BDIP can recognize the source and destination of the packet from the user under permission using personal user information
Post-conditions (optional)	
Derived requirements	– Data collection (refer to clause 8.1, requirements 1, 2) – Data preprocessing (refer to clause 8.2, requirements 1, 4) – Data storage (refer to clause 8.3, requirement 1, clause 8.7, requirement 3) – Data analysis (refer to clause 8.4, requirement 1, 12) – Data application (refer to clause 8.5, requirement 6, clause 8.1, requirement 4) – Data management (refer to clause 8.6, requirements 2, 4)

Table I.2 – The massive and high resolution multimedia data service

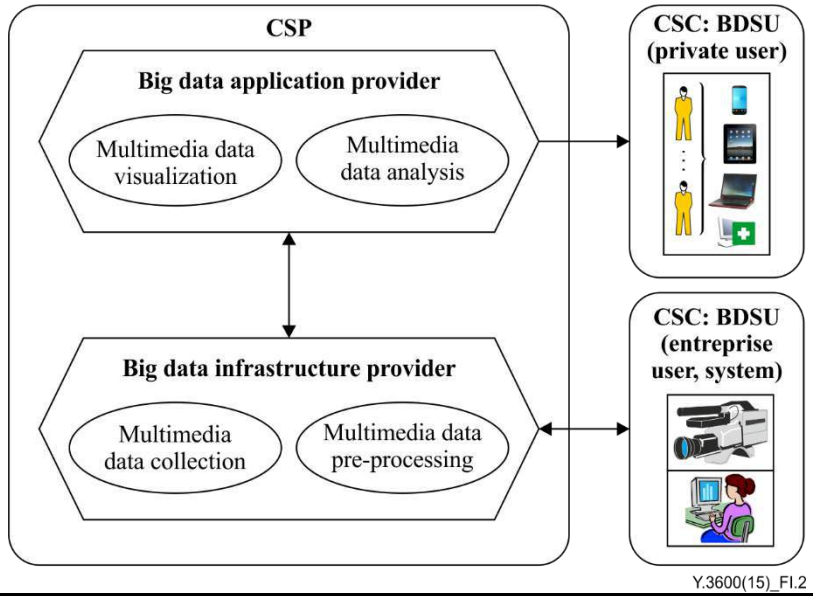
Title	The massive and high resolution multimedia data service
Description	In this use case, the cloud service provider should support the CSP:BDIP provider to collect, process and transmit the massive multimedia data using cloud services. In addition, the CSP should support the CSP:BDAP to provide massive multimedia related application services. The CSP:BDAP can provide the multimedia analysis and visualization to the user and provide the multimedia collection (transmission), processing and storage to the user or the CSP:BDAP.
Roles/sub-roles	– CSP – CSP:BDIP – CSP:BDAP – CSC:BDSU
Figure	
Pre-conditions (optional)	
Post-conditions (optional)	
Derived requirements	– Acceleration processing (refer to clause 8.2, requirement 2) – Network monitoring (refer to clause 8.6, requirement 5)

Table I.3 – E-commerce platform big data analysis

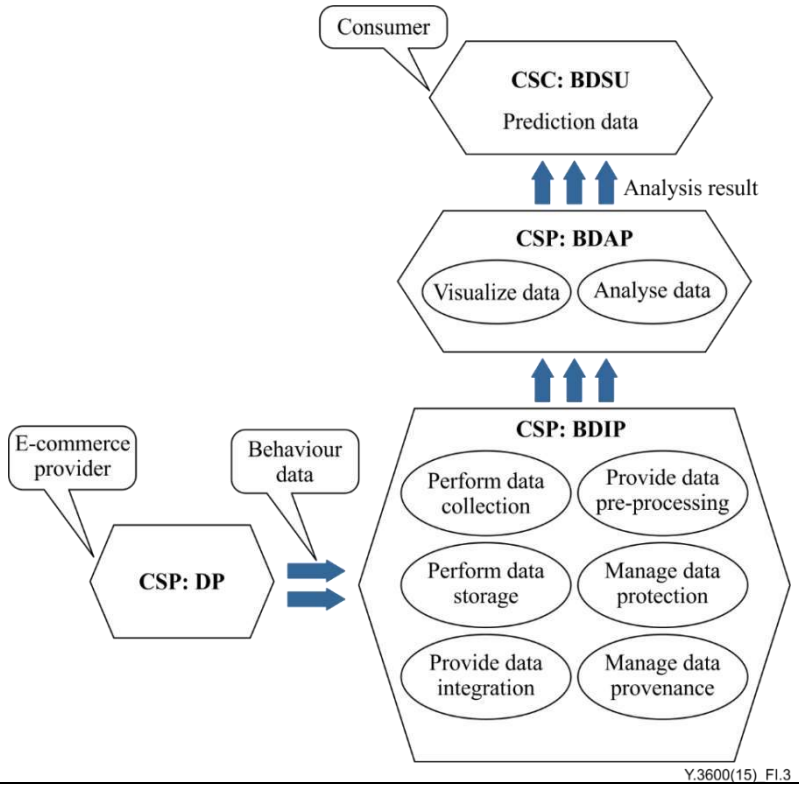
Title	E-commerce platform big data analysis
Description	Consumers shop online using an e-commerce platform, including search and checking of product information. The CSC:BDSU (e-commerce platform providers) use big data applications to implement backend supporting services, such as product recommendations, sales volume prediction, user behaviour analysis, etc. Customers get online shopping related services, such as authentication, products searching, checking, ordering and shipping through the front-end functions of the e-commerce platform. The e-commerce provider manages (creates, reads, updates and deletes) the information about products and inventory information through back-end functions of the e-commerce platform. Related big data application services are built upon the private or public big data infrastructure provided by the CSP:BDIP. The operational data of the e-commerce platform is collected, stored and pre-processed by the CSP:BDIP. In addition the CSP:BDAP analyses the operational data to give the prediction information. Privacy rules are followed, if applicable.
Roles/sub-roles	– CSN:DP – CSP:BDAP – CSP:BDIP – CSC:BDSU
Figure	
Pre-conditions	– The CSN:DP can provide user consumption behaviour data such as shopping frequency, often purchased items, payment capacity, etc.
Post-conditions	– The CSP:BDAP can have responsibility for providing analysis result of user consumption behaviour data such as prediction information and user behaviour analysis. – The CSC:BDSU gives accurate and personalized sales and promotions such as product recommendations, sales volume prediction and user behaviour analysis.
Derived requirements	– Data collection (refer to clause 8.1, requirements, 3, 6) – Data analysis (refer to clause 8.4, requirements 8, 9, 12) – Data management (refer to clause 8.7, requirement 5)

Table I.4 – Internet social network services big data analysis

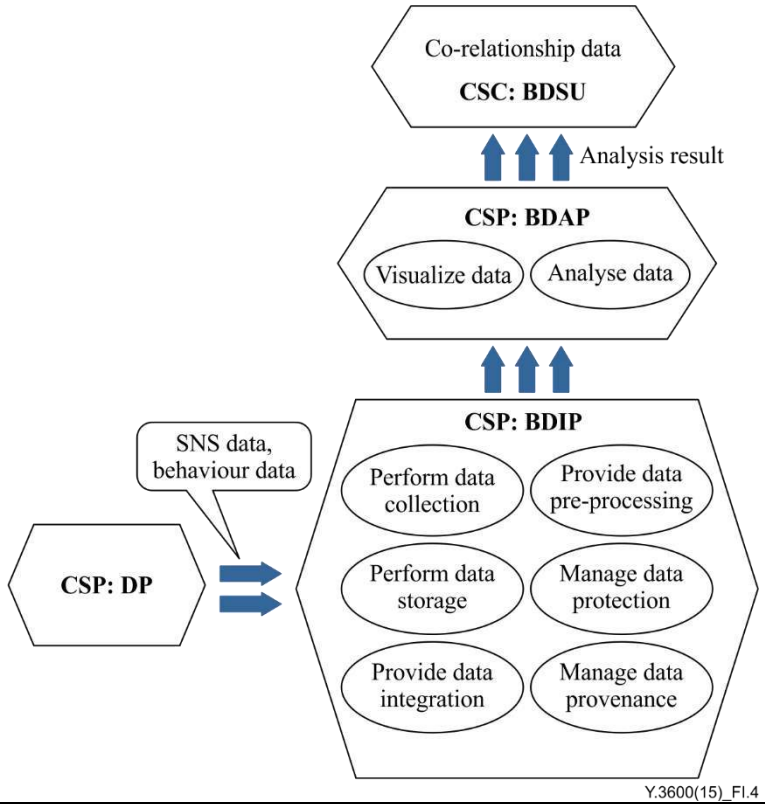
Title	Internet social network services big data analysis
Description	Social network service (SNS) providers use big data application services to analyse the relationships between social network service users. Social network service users register to SNS services with parts of their background information, such as education and working experience, professional skills, etc. The data provider (SNS platform provider) saves the registered users information in databases. The SNS platform provider uses big data services provided by the CSP:BDIP and CSP:BDAP who use cloud computing systems and technologies, such as distributed databases, computing frameworks, cache systems, etc. The SNS platform provider could analyse the behaviour of the SNS users and their co-relationships between each other. The CSC:BDSU (SNS platform provider) could push and promote the contact information to the SNS users that the pushed persons may have some relationship with receivers through pop messages or emails. Privacy rules are followed, if applicable.
Roles/sub-roles	– CSN:DP – CSP:BDAP – CSP:BDIP – CSC:BDSU
Name	
Pre-conditions	– The CSN:DP can provide the raw data reflecting the behaviours of the SNS users.
Post-conditions	– The CSP:BDAP can have responsibility for providing analysis results of network user behaviour to the CSC:BDSU. It can have responsibility for providing the co-relationships between the users of an SNS. The CSP:BDAP should follow the privacy rules, if applicable. – The CSC:BDSU utilizes data of co-relationships between the users of an SNS to give recommendations of new services or new friends in an SNS, etc., following privacy rules, if applicable.
Derived requirements	– Data storage (refer to clause 8.3, requirements 1, 2, 5, clause 8.7, requirement 1) – Data analysis (refer to clause 8.4, requirements 6, 7)

Table I.5 – Mobile network user behaviour big data analysis

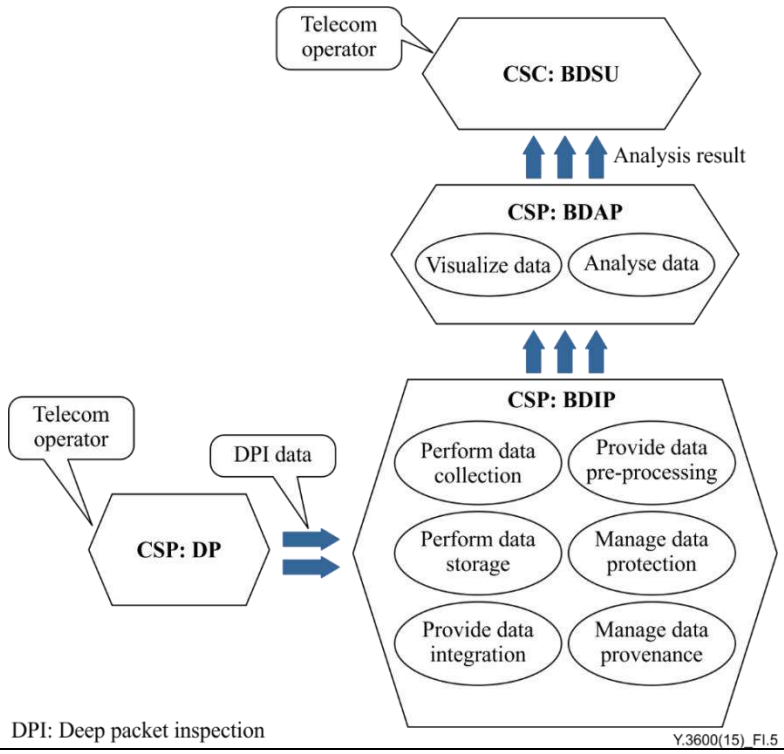
Title	Mobile network user behaviour big data analysis
Description	Telecom operators use big data application services to analyse Internet accessing behaviour of mobile network users. Telecom mobile network users use a 3G/4G network to access mobile Internet services (web browsing, social networking, e-commerce, music, video, mobile television, etc.) using mobile devices, such as mobile phones, tablet computers, PDAs and so on. Optical splitter and deep packet inspection (DPI) devices have been deployed along with the PDSN or serving general packet radio service support node (SGSN) devices. DPI devices capture the data packets of mobile network devices from the optical splitter and extract the Internet access attributes information. Telecom operators set up private big data infrastructure using cloud computing technologies or buy services from the CSP:BDIP and build big data application services or buy services from the CSP:BDAP. Telecom operators could push and promote value added services, applications and advertisements for suitable mobile network users such as a CSC:BDSU. Privacy rules are followed, if applicable.
Roles/sub-roles	– CSN:DP – CSP:BDAP – CSP:BDIP – CSC:BDSU
Figure	
Pre-conditions	– The CSN:DP can provide the raw data which reflects mobile network users' behaviour.
Post-conditions	– The CSP:BDAP can have responsibility for providing analysis results of mobile network user behaviour to the CSC:BDSU. The analysis results show the users' habits of using network services, such as in which time slots the users may access which websites or applications. – The CSC:BDSU pushes and promotes the value added services, applications and advertisements for suitable mobile network users.
Derived requirements	– Data collection (refer to clause 8.1, requirement 1) – Data storage (refer to clause 8.3, requirement 1) – Data analysis (refer to clause 8.4, requirements 2, 7, 12) – Data application (refer to clause 8.4, requirement 13, clause 8.7, requirement 1)

Table I.6 – Big data based mobile network (3G/4G) billing detail query

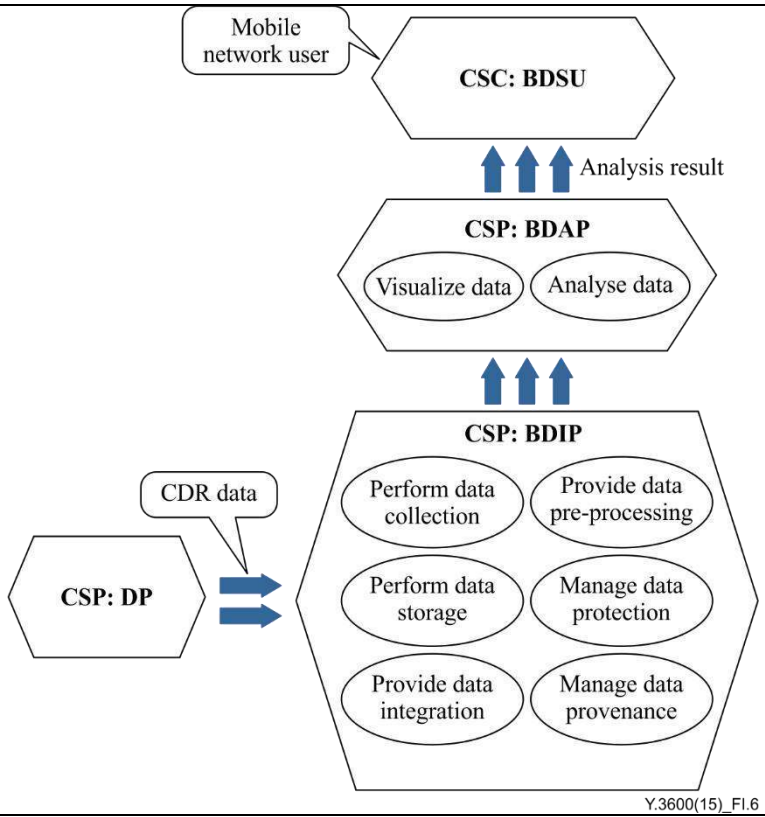
Title	Big data based mobile network (3G/4G) billing detail query
Description	Telecom operators use big data application services to provide detailed billing information of mobile network users. Telecom mobile network users use 3G/4G networks to access mobile internet services using mobile devices such as mobile phones and tablet computers .The access network devices, such as PDSN or combined GPRS service node (SGSN/CGSN) devices, record all kinds of billing information of each of the mobile network users into a standardized format, such as a charging detail record (CDR). A charging gateway function (CGF) modular collects different charging records and forwards these charging records to the billing system. The billing system keeps and processes all the CDRs from different CGFs and finally generates the charging bill for each mobile user. Telecom operators set up big data infrastructure and store huge amounts of user billing detail information. Mobile network users could quickly query the detailed billing information based on the big data infrastructure and big data applications. A mobile network user could get the statistics and analytics information for instance in terms of time, type of website and applications accessed through a 3G/4G mobile network for his/her internet access actions through 3G/4G mobile networks. Privacy rules are followed, if applicable.
Roles/sub-roles	– CSN:DP – CSP:BDAP – CSP:BDIP – CSC:BDSU
Figure	
Pre-conditions	– CSN:DP can provide CDR data of network users

Table I.6 – Big data based mobile network (3G/4G) billing detail query

Post-conditions	– CSP:BDAP can have functionalities for providing analysis result of network users' CDR data to the CSC:BDSU. – CSC:BDSU could quickly query the detailed billing record for each internet access based on the analysis result.
Derived requirements	– Data collection (refer to clause 8.1, requirement 3) – Data storage (refer to clause 8.3, requirement 4) – Data analysis (refer to clause 8.4, requirement 8) – Data application (refer to clause 8.5, requirement 2)

Table I.7 – Intelligent transport big data analysis

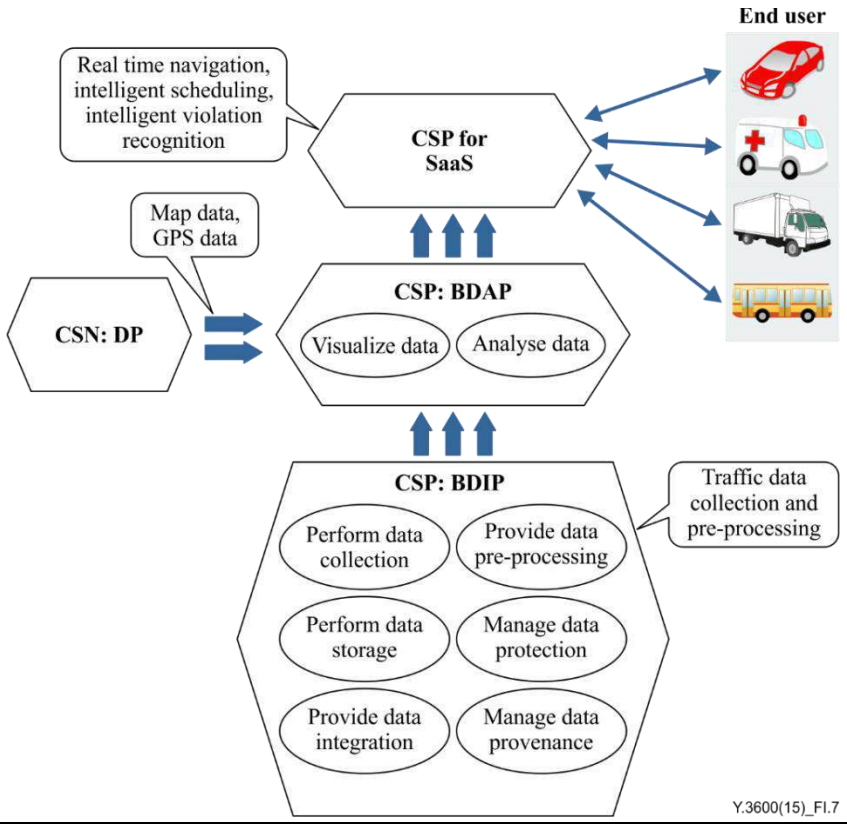
Title	Intelligent transport big data analysis
Description	The public transportation traffic information on the main roads is collected by an intelligent transport platform. Intelligent transport platform providers use big data applications to implement backend supporting services such as traffic volume prediction, route traffic analysis and route navigation optimization.
Roles/sub-roles	– CSN:DP – CSP:BDAP – CSP:BDIP – CSC:BDSU
Figure	

Table I.7 – Intelligent transport big data analysis

Pre-conditions	– The speed sensors and high-resolution cameras are installed at intersections and key points of roads in the city and outskirts. – The traffic of vehicles and the status of roads data are collected in real time. – The big data applications for intelligent transport systems are built upon the private or public big data infrastructure.
Post-conditions	– Real time and accurate route navigation based on the shortest path algorithm and route traffic could be provided to private and business vehicle drivers of all types of vehicles on the road except drivers of track vehicles. – Accurate scheduling for bus departures is established on the real time analysis and prediction of road traffic. – Automatic recognition of violations of road traffic laws such as speeding, running red lights, drink-driving, running through restricted areas, fatigue driving, etc.
Derived requirements	– Data analysis (refer to clause 8.4, requirement 3, 9,12)

Appendix II

Use cases of cloud computing based big data as analysis services

(This appendix does not form an integral part of this Recommendation.)

Table II.1 – Continuous product improvement

Title	Continuous product improvement
Description	A software game manufacturing company would like to concentrate on application development as a basic activity and the area of investment. In order to continuously improve its products, the company needs an analytics solution to collect and analyse the associated market and users' feedback. The company embedded monitoring functions in the software games to observe users' behaviours, activities and preferences of available game options. In addition a questionnaire is included in the game application for obtaining offline users' feedback. Other sources of information about the game perception are Internet forums, discussion lists and social communities, as well as press and television publications. Given the large number of game users, the company has a lot of information to sift through every month. But the amount of data can change depending on the schedule of new games publication, so proper planning and smart organization of feedback data analysis would help the company's IT team in their use of big data analytics to improve business success. The game company builds an analytical solution based on big data as a service (BDaaS) by defining: – the schedule of BDaaS activity depending on games publication time; – requirements for data collection directly from the application using embedded monitoring functions; – requirements for collection of Internet and press data related to the game in order to analyse users' and market opinions and its evolution; – requirements for social media data analysis of game users' opinions and direct exchange between users; – the access method to the user generated questionnaire data about the game; – database selection for all data collected about the game; – requirements for analytics and reporting to emphasize the opinions about the application, identify strong and weak points, gaps and spare elements; – monitoring criteria to analyse the intensity of new opinions on appearance generated by users to identify the application maturity level, which allows decisions to be made about ending involvement in the product; – performance objectives to be reached by the BDaaS system. The game company orders a BDaaS including the following elements: – specification of data sources, which need to be serviced; – data integration goals for overall analytics; – database functionalities; – data storage functionalities (data types, variety, lifetime); – analytical tool functionalities; – access to analytical tool configuration and customization; – reporting schemes and integration with the company internal systems; – data collected and results of analysis available only for the company, even if publicly available data are used.
Roles/sub-roles	– The cloud service provider should support the CSP:BDIP role to collect, process, store and delete data according to the CSC (i.e., the game manufacturing company) specifications. In addition, the CSP should support the CSP:BDAP role to provide analytical applications with integration of CSC systems, as well as reporting solutions.

Table II.1 – Continuous product improvement

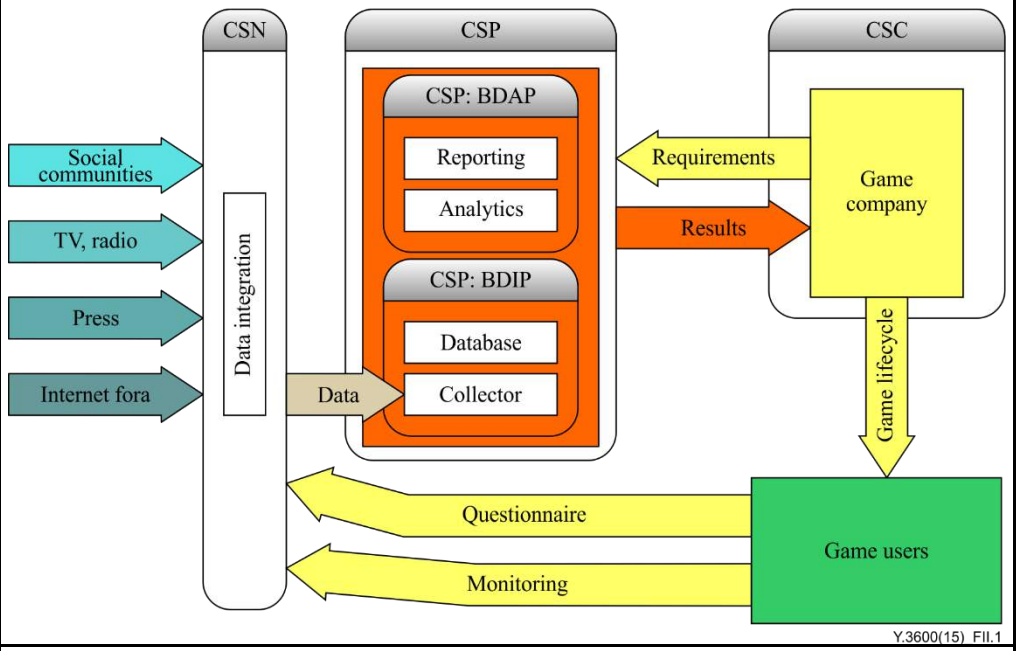
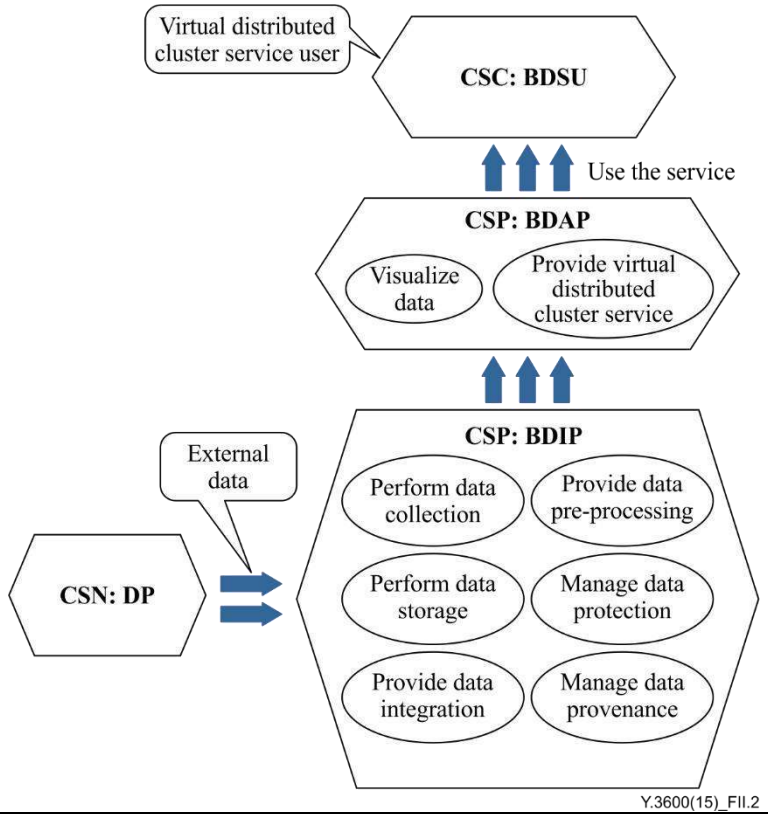
Figure	
Pre-conditions (optional)	The game company has to plan the analytical solution to support application development. The solution utilization can vary depending on the new products being launched, so the investment in a solution may prove to be ineffective.
Post-conditions (optional)	The game company can define analytical campaigns for each product and optimize the analysis effectiveness. Only currently required capabilities are used from the BDaaS solution in a pay-as-you-go model.
Derived requirements	– Data collection (clause 8.1, requirements 1, 3, 5) – Data pre-processing (clause 8.2, requirements 3, 4) – Data storage (clause 8.3, requirements 1, 2, 3, 4, 6, 7) – Data analysis (clause 8.4, requirements 5, 10, 11) – Data visualization (clause 8.5, requirements 1, 3, 4, 5) – Data security and protection (clause 8.7, requirement 4)

Table II.2 – Virtualized distributed cluster service

Title	Virtualized distributed cluster service
Description	A virtual distributed cluster service is a typical web service which makes it easy to have a cluster of machines quickly and cost-effectively processing vast amounts of data provided by a CSP. The virtual distributed cluster service uses distributed clustering software as a framework, to distribute the customers' data and processing across a resizable cluster of virtual machine instances in cloud resource pools. Three steps that are often included by the CSC using a virtual cluster service are: 1) **Upload data**. The CSC:BDSU uploads the data that needs to be analysed to the cloud storage space that belongs to the CSC:BDSU. In addition the CSC:BDSU could use the data provided by the CSN:DP. 2) **Create virtual distributed cluster**. The CSC:BDSU creates and configures the distributed cluster by specifying data inputs, outputs, cluster size, security settings and other necessary parameters.

Table II.2 – Virtualized distributed cluster service

	3) **Monitor and collect**. CSC:BDSU monitors the health and progress of the distributed cluster using the tools provided by the CSP. When the distributed processing job is completed the CSC:BDSU retrieves the output in the specified storage space. A virtual distributed cluster service could be used in a variety of applications, including log analysis, web indexing, data warehousing, machine learning, financial analysis, scientific simulation and bioinformatics.
Roles/Sub-roles	– CSN:DP – CSP:BDAP – CSP:BDIP – CSC:BDSU
Figure	
Pre-conditions (optional)	– The CSC:BDSU has registered in the service platform of the CSP of the virtual distributed cluster service. – The CSC:BDSU has applied the cloud storage space for accepting the input data and output data from the virtual distributed cluster service cluster.
Post-conditions (optional)	– The CSC:BDSU could quickly create the specified cluster with the desired number of virtual machines and software versions. – The CSC:BDSU gets the processing results after a planned time period.
Derived requirement	– Data storage (refer to clause 8.3, requirement 1) – Data analysis (refer to clause 8.4, requirements 2, 4, 7) – Data management (refer to clause 8.6, requirements 1, 2, 3, 4, 5, 6) – Data security and protection (refer to clause 8.7, requirements 2, 3, 4)

Appendix III

Mapping of big data ecosystem roles into user view of ITU-T Y.3502

(This appendix does not form an integral part of this Recommendation.)

Table III.1 shows the results of mapping between the sub-role of the cloud computing reference architecture (CCRA) user view and the performance of similar roles in the big data ecosystem. A similar sub-role with a data supplier does not exist in CCRA. A big data service customer and a CSC may be considered to perform similar activities. Similarly, a data broker and CSN: cloud service broker may be considered in the same manner. If the CCRA is assumed to contain the big data service area, the activities for the CSN: cloud service broker should be extended in the data perspective. The big data service provider is related to all sub-roles of the CSP. This means that the big data service provider could be treated with an implanted feature or an independent sub-role of the CSP.

Table III.1 – Mapping of big data ecosystem roles and sub-roles of the CCRA user view

Big data ecosystem		User view of ITU-T Y.3502	Note
Data provider	Data supplier	CSN	For the cloud computing based big data environment, the new sub-role of the CSN for the data provider is required.
	Data broker	CSN	For the cloud computing based big data environment: (option 1) the extension of the activities of the CSN: Cloud service broker is required. (option 2) the new sub-role of the CSN for data brokerage is required. (option 3) adding the "brokerage" activity on the sub-role which corresponds with the data supplier is required.
Big data service customer		CSC	For the cloud-based big data service environment: (option 1) using the CSC is required. (option 2) the new role or sub-role of the CSC for the big data service customer is required.
Big data service provider		CSP	The big data service provider could be treated with an implemented feature. Nevertheless, to clarify the cloud-based big data service, an independent sub-role of the CSP for the big data service provider is required.

Bibliography

[b-ITU-T M.3030] Recommendation ITU-T M.3030 (2002), *Telecommunications Markup Language (tML) framework*.

[b-ITU-T Y.2201] Recommendation ITU-T Y.2201 (2011), *Requirements and capabilities for ITU-T NGN*.

[b-ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

[b-CRA-BDWP] *Challenges and Opportunities with Big Data*, Computing Research Association, November 2012. <http://cra.org/ccc/wp-content/uploads/sites/2/2015/05/bigdatawhitepaper.pdf>


END DEVICES
VELOCITY
CONSUMERS
VOLUME
BIG
DATA
VARIETY
STANDARDS
ANALYTICS
BUSINESS
SECURITY

Big data standardization roadmap

Supplement 40 to ITU-T Y.3600-series Recommendations

(07/2016)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Summary

Supplement 40 to ITU-T Y-series Recommendations provides the standardization roadmap for big data in the telecommunication sector. It describes the landscape and conceptual ecosystem of big data from an ITU-T perspective, related technical areas, activities in standards development organizations (SDOs) and gap analysis.

Keywords

Big data, big data ecosystem, data analytics, roadmap.

Table of Contents

1 Scope

This Supplement provides the standardization roadmap for big data area in the telecommunication sector. It addresses the following subjects:

- landscape of big data from an ITU-T perspective;
- related technical areas of big data;
- conceptual model of big data ecosystems;
- big data activities in standards development organizations (SDOs);
- standardization gap analysis.

2 References

[ITU-T Y.2060] Recommendation ITU-T Y.2060 (2013), *Overview of the Internet of things*.

[ITU-T Y.3300] Recommendation ITU-T Y.3300 (2014), *Framework of software-defined networking*.

[ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014), *Information technology – Cloud computing – Overview and vocabulary*.

[ITU-T Y.3600] Recommendation ITU-T Y.3600 (2015), *Big data – Cloud computing based requirements and capabilities*.

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following term defined elsewhere:

3.1.1 big data [ITU-T Y.3600]: A paradigm for enabling the collection, storage, management, analysis and visualization, potentially under real-time constraints, of extensive datasets with heterogeneous characteristics.

NOTE – Examples of datasets characteristics include high-volume, high-velocity, high-variety, etc.

3.2 Terms defined in this Supplement

None.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

AMQP Advanced Message Queuing Protocol
API Application Program Interface
BDaaS Big Data as a Service
BDC Big Data service Customer
bDDN big Data-Driven Networking
BDSP Big Data Service Provider
CSV Comma-Separated Values
DCAT Data Catalogue Vocabulary
DMG Data Ming Group
DPI Deep Packet Inspection
HTTP Hypertext Transfer Protocol
ICT Information and Communications Technology

IEC	International Engineering Consortium
IoT	Internet of Things
ISO	International Organization for Standardization
JSON	Java Script Object Notation
JTC 1	Joint Technical Committee 1
KVDB	Key-Value Database Application Interface
LDP	Linked Data Platform
M2M	Machine to Machine
MQTT	Message Queuing Telemetry Transport
PMML	Predictive Model Markup Language
RDF	Resource Description Framework
SC	Subcommittee
SDN	Software-defined Networking
SDO	Standards Development Organization
SG	Study Group
TC	Technical Committee
URL	Uniform Resource Locator
W3C	World Wide Web Consortium
WG	Working Group
XMILE	XML Interchange Language
XML	Extensible Markup Language

5 Conventions

None.

6 Landscape of big data from an ITU-T perspective

6.1 Characteristics and general concepts of big data

[ITU-T Y.3600] describes the characteristics and general concepts of the big data ecosystem.

With the rapid development of information and communications technology (ICT), Internet technologies and services, huge amount of data are generated, transmitted and stored with explosive growth. Data are generated by many sources and not only sensors, cameras, network devices, web pages, email systems, social networks and many other sources. Datasets are becoming so large and complex or are arriving so fast that traditional data processing methods and tools are inadequate. Efficient analytics of data within tolerable elapsed times becomes very challenging. The paradigm being developed to resolve the above issues are called big data [ITU-T Y.3600].

Within big data ecosystem, data types include structured, semi-structured and unstructured data. Structured data are often stored in databases which may be organized in different models, such as relational model, document model, key-value model, graph model etc. Semi-structured data does not conform to the formal structure of data models, but contain tags or markers to identify data. Unstructured data do not have a pre-defined data model and are not organized in any defined manner. Within all data types data can exist in formats, such as text, spreadsheet, video, audio, image, map, etc. [ITU-T Y.3600].

Big data is used in many fields, where data processing is characterized by scale (volume), diversity (variety), speed (velocity) and possibly others like credibility (veracity) or business value, if traditional methods and tools are not efficient. These characteristics, usually called v's, can be explained as following [ITU-T Y.3600]:

- **Volume**: refers to the amount of data collected, stored, analyzed and visualized, which big data technologies need to resolve;
- **Variety**: refers to different data types and data formats that are processed by big data technologies;
- **Velocity**: refers to both how fast the data is collected and how fast the data is processed by big data technologies to deliver expected results.

NOTE – Additionally, veracity refers to the uncertainty of data, and value refers to the business results from gaining new information using big data technologies. Other v's can be considered as well.

Taking into account the described above v's characteristics, big data technologies and services can resolve many new challenges, and can also create more new opportunities than ever before [ITU-T Y.3600]:

- **Heterogeneity and incompleteness**: data processed using big data can miss some attributes or introduce noise into data transmission. Even after data cleaning and error correction, some incompleteness and some errors in data are likely to remain. These challenges can be managed during data analysis [b-CRA].
- **Scale**: processing of large and rapidly increasing volumes of data is a challenging task. Using data processing technologies, the data scale challenge is mitigated by evolution of processing and storage resources. However, nowadays data volumes are scaling faster than resources are evolving. Technologies such as parallel databases, in-memory databases, non-SQL databases and analytical algorithms resolve this challenge.
- **Timeliness**: the acquisition rate and timeliness, to effectively find elements in a limited-time period that meet a specified criterion in a large dataset, are new challenges faced by data processing. Other new challenges are related to the types of criteria specified, and need to devise new index structures and responses to the queries having tight response-time limits.
- **Privacy**: data about human individuals, such as: demographic information, Internet activities, commutation patterns, social interactions, energy or water consumption, are being collected and analyzed for different purposes. Big data technologies and services are challenged to protect personal identities and sensitive attributes of data throughout the entire data processing process, while respecting applicable data retention policies.

Positive resolution of the above challenges opens new opportunities to discover new data relationships, hidden patterns or unknown dependencies [ITU-T Y.3600].

6.2 Benefits of big data

Big data technologies can provide many benefits such as data accessibility, productivity of business processes, and cost reduction to private via public sector.

Big data technology increases data accessibility by:

- Unlocking significant value by making information transparent;
- Creating and storing transactional data in digital form;
- Reducing time for finding/accessing the correct data.

Big data technology improves productivity by:

- Real-time monitoring and forecasting of events that impact either business performance or operations;
- Timely insights from the vast amount of data;
- Identifying significant information that can improve decision quality or minimize risks;
- Creating new service models using big data analytics.

Big data technology reduces cost by:

- Scale-out of data storage;
- Identifying and reducing inefficiencies.

7 Related technical areas of big data

7.1 Cloud computing

Cloud computing is a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand. Key characteristics of cloud computing are [ITU-T Y.3500]:

- **Broad network access**: a feature where physical and virtual resources are available over a network and accessed through standard mechanisms that promote use by heterogeneous client platforms;
- **Measured service**: a feature where the metered delivery of cloud services is such that usage can be monitored, controlled, reported, and billed. This is an important feature needed to optimize and validate the delivered cloud service;
- **Multi-tenancy**: a feature where physical or virtual resources are allocated in such a way that multiple tenants and their computations and data are isolated from, and inaccessible to, one another;
- **On-demand self-service**: a feature where a cloud service customer can provision computing capabilities, as needed, automatically or with minimal interaction with the cloud service provider;
- **Rapid elasticity and scalability**: a feature where physical or virtual resources can be rapidly and elastically adjusted, in some cases automatically, to quickly increase or decrease resources;
- **Resource pooling**: a feature where a cloud service provider's physical or virtual resources can be aggregated in order to serve one or more cloud service customers.

Big data needs on-demand high-performance data processing and distributed storage as well as a variety of tools required to accomplish activities of the big data ecosystem. The burst nature of workloads makes cloud computing more appropriate for big data challenges such as scalability and timeliness [ITU-T Y.3600].

The relationship of cloud computing and big data mainly concerns two aspects:

1) Cloud computing can support big data using cloud infrastructure and services;
2) Big data services can provide public cloud analysis services, such as big data as a service (BDaaS).

7.2 Internet of things

The Internet of things (IoT) is a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies [ITU-T Y.2060].

The IoT can be perceived as a far-reaching vision with technological and societal implications. From the perspective of technical standardization, the IoT can be viewed as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable ICT. Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of "things" to offer services to all kinds of applications, while ensuring that security and privacy requirements are fulfilled.

Big data in the context of IoT has some specific characteristics which do not necessarily pertain to big data in other technical areas. The prominent characteristics of big data in the context of IoT are: high variety (heterogeneity of data types and sources), high velocity (high frequency of data generation) and high volatility (data generated in a non-persistent stateless manner).

Some identified challenges concerning big data in the context of IoT are the following [b-Chen]:

- An increasing number of connected things generates huge amounts of data;
- The generated data are mainly semi-structured or even unstructured;
- The generated data may have different confidence and precision levels;
- The generated data are generally not useful until they are adequately "processed" (including pre-processing, analysis, etc.).

7.3 Security and privacy

Data security and privacy comprise the people, process and technology required to prevent destructive forces and unwanted actions [b-IBM]. From a big data perspective, security and privacy requirements are magnified by the characteristics of big data. Some identified challenges concerning big data in the context of security and privacy are the following [b-CSA]:

- Secure computations in distributed programing frameworks;
- Secure data storage and transactions logs;
- End-point input validation/filtering and data provenance;
- Real-time security/compliance monitoring;
- Scalable and composable privacy-preserving data mining and analytics;
- Anonymization and de-identification.

7.4 Software-defined networking

Software-defined networking (SDN) is a set of techniques that enables users to directly program, orchestrate, control and manage network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner [ITU-T Y.3300]. By abstracting the underlying infrastructure for applications and network services, SDN lets administrators dynamically adjust network-wide traffic flow to meet changing needs, while maintaining a global view of the network.

Big data processing requires agile, multi-domain, centrally managed architecture. SDN addresses the congestion and lack of scalability of current networks by [b-NEC]:

- Allowing for changing traffic patterns;
- Providing functionality to applications that access geographically distributed databases and servers through public and private clouds;
- Providing access to bandwidth on demand.

7.5 Deep packet inspection

Deep packet inspection (DPI) is a form of filtering used to inspect data packets sent from one computer to another over a network. Software-based DPI, provides advanced traffic analysis and multidimensional reporting, showing the possibility of making off-the-shelf hardware work at actual line rates. Software-based DPI can be pervasively deployed in the network, providing much better analysis capabilities, as well as simpler mechanisms for deployment, update, testing and scaling to changing workloads [b-ITU-T DPI].

7.6 Big data-driven networking

Big data-driven networking (bDDN) is a group of technologies and methods to facilitate network operation, administration, maintenance and optimization, etc., based on the big data generated by the network and a series of methods and tools. That is to say, big data generated by the network is used to serve the network and make the network better. bDDN solves this problem by introducing and applying the big data technology to the framework of future networks [b-ITU-T DDN].

7.7 Open data

Open data is accessible public data that people, companies, and organizations can use to launch new ventures, analyze patterns and trends, make data-driven decisions, and solve complex problems. Open data includes two basic features: the data must be publicly available for anyone to use, and it must be licensed in a way that allows for its reuse [b-theguardian]. Open data is more focused on a horizontal scaling of big data sources.

The main technical issues for open data are as follows:

- Data publication: metadata supporting machine readability, data format, and licenses;
- Data finding: data identification, data semantics, and data access;
- Data provenance: data quality, data lineage tracking, and data versioning.

7.8 Standardization areas of big data

This clause describes the potential areas of standardization for big data that may be of interest to ITU-T [b-ITU-T TSAG]:

- Common requirements and use cases;
- Definition, architecture, data model and application program interfaces (APIs);
- Network-driven data analytics;
- Personalized network experience;
- Security and data protection, anonymization and de-identification of personal data;
- Framework for data quality and veracity;
- Standards and guidelines to address issues surrounding legal implications of big data in the telecommunications sector (e.g., data ownership);
- Framework and related standards for telecom big data exchange.

8 Conceptual model of big data ecosystem

[ITU-T Y.3600] describes the roles and sub-roles of the big data ecosystem as shown in Figure 8-1.

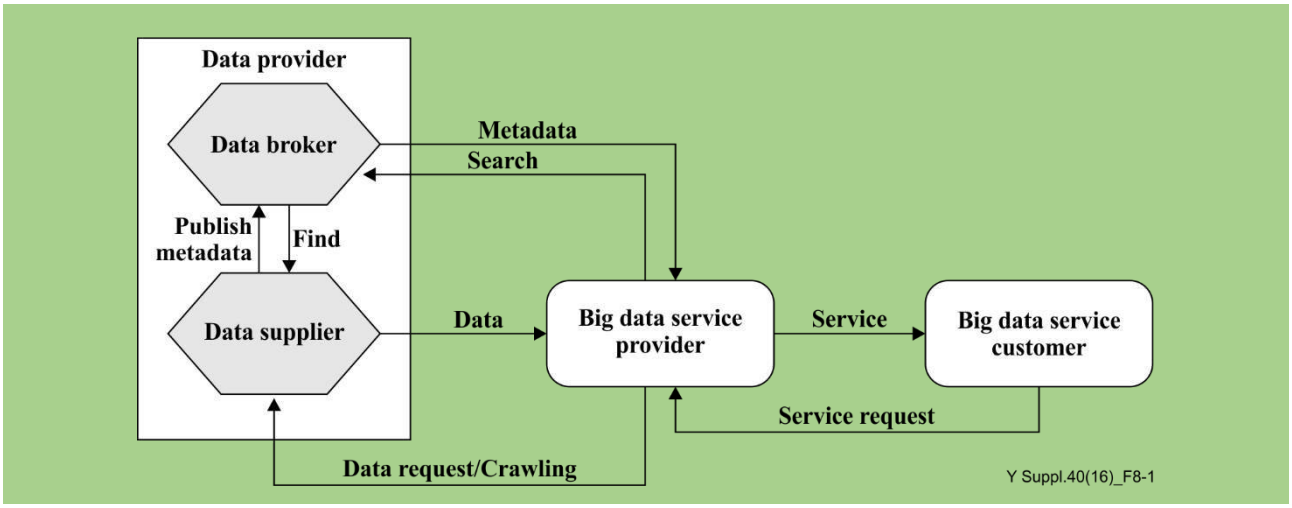


Figure 8-1 – Big data ecosystem (from [ITU-T Y.3600])

Data provider (DP) roles consists of two sub-roles:

- data supplier;
- data broker.

The data supplier provides data from different sources to the data broker, which can be accessed by the big data service provider (BDSP). The data supplier's activities include:

- generate data;
- create metadata information describing the data source(s) and relevant attributes;
- publish metadata information to access it.

The data broker serves as the connection between the data supplier and the BDSP. The data broker can act as a clearinghouse, open data mart, etc., and its activities include:

- providing a meta-information registry to data suppliers for publishing their data sources;
- finding on-line open-data sources and registering corresponding meta-information;
- providing a service catalogue to the BDSP for searching usable data.

The BDSP supports capabilities for big data analytics and infrastructure. The BDSP can act as a form of big data platform, extension of existing data analytics platform, etc. BDSP activities include:

- searching data sources (from data broker) and collecting data by requesting and crawling;
- storing data to a data repository;
- integrating data;
- providing tools for data analysis and visualization;
- supporting data management such as: data provenance, data privacy, data security, data retention policy, data ownership.

The big data service customer (BDC) is the end-user or a system, that uses the results or services from a BDSP. The BDC may produce new services or knowledge on consumer activities and furnish them outside of the big data ecosystem. BDC activities include:

- requesting big data services to the BDSP;
- using the outputs of big data services.

9 Big data SDO activities

This clause describes SDO's activities with big data in order to identify the current status of standardization.

NOTE – A summary of each standard item is described in Appendix I.

9.1 ITU-T

ITU-T Study Group 13 (SG13) has been studying requirements, capabilities and mechanisms of future networks.

- Q17/13 deals with cloud computing and big data. In November 2015, ITU-T SG13 published [ITU-T Y.3600], "Big data – Cloud computing based requirements and capabilities".
- Q18/13 deals with cloud functional architecture, infrastructure and networking; the draft Recommendation [ITU-T Y.BDaaS-arch] describes an architecture for BDaaS.
- Q7/13 has been studying DPI in support of service/application awareness in evolving networks, and initiated draft Recommendations about DPI and bDDN for supporting big data.

ITU-T SG 17 is responsible for building confidence and security in the use of ICTs, and deals with the security and privacy issues of cloud computing. These activities on cloud computing can be applied to the area of big data as well.

ITU-T SG 20 is responsible for IoT and its applications, with an initial focus on smart cities and communities (SC&C). In November 2015, Q2/20 initiated a draft Recommendation [ITU-T Y.IoT-BigData-reqts], "Specific requirements and capabilities of the Internet of Things for Big Data" which describes the characteristics of big data in the context of IoT. Table 9-1 lists the ITU-T deliverables and work items related to big data.

Table 9-1 – ITU-T deliverables and work items related to big data

Study group	Reference (Note)	Title	Status
SG 13	[ITU-T Y.3600]	Big data – Cloud computing based requirements and capabilities	Published 2015
SG 13	[ITU-T Y.BigDataEX-reqts]	Big data exchange framework and requirements	2Q 2017
SG 13	[ITU-T Y.BdaaS-arch]	Functional architecture of Big data as a Service	Dec. 2016
SG 13	[ITU-T Y.bDDN-req]	Requirement of big data-driven networking	Dec. 2018
SG 13	[ITU-T Y.bDDN-fr]	Framework of big data driven networking based on DPI	Jul. 2018
SG 13	[ITU-T Y.dsf-reqts]	Requirements and Capabilities for Data Storage Federation	2Q 2018
SG 13	[ITU-T Y.bDPI-Mec]	Mechanism of deep packet inspection applied in network big data context	Dec. 2018
SG 13	[ITU-T Y.SDN-ARCH]	Functional architecture of software-defined networking	Jul. 2017
SG13	[ITU-T Y.bdp-reqts]	Big data – Requirements for data provenance	4Q 2018
SG 17	[ITU-T X.1601]	Security framework for cloud computing	Published 2014
SG 17	[ITU-T X.CSCDataSec]	Guidelines for cloud service customer data security	Dec. 2016
SG 20	[ITU-T Y.IoT-BigData-reqts]	Specific requirements and capabilities of the Internet of Things for Big data	4Q 2016
NOTE – Clause I.1 contains a description of each cited reference.			

9.2 ISO/IEC JTC 1

In November 2014, the ISO/IEC joint technical committee 1 (JTC 1) established working group (WG) 9 [b-JTC 1] on big data to:

- Serve as the focus of, and proponent for, big data standardization;
- Develop foundational standards for big data – including reference architecture and vocabulary standards – for guiding big data efforts throughout JTC 1 upon which other standards can be developed;
- Develop other big data standards that build on the foundational standards when relevant JTC 1 subgroups, that could address these standards, do not exist or are unable to develop them.
- Identify gaps in big data standardization;
- Develop and maintain liaisons with all relevant JTC 1 entities as well as with any other JTC 1 subgroup that may propose work related to big data in the future;
- Identify JTC 1 (and other organization) entities that are developing standards and related material that contribute to big data, and where appropriate, investigate ongoing and potential new work that contributes to big data;
- Engage with the community outside of JTC 1 to grow the awareness of and encourage engagement in JTC 1 big data standardization efforts within JTC 1, forming liaisons as is needed.

JTC 1 subcommittee (SC) 27 has been developing standards for the protection of information and ICT, which include generic methods, techniques and guidelines to address aspects of both security and privacy. Security and privacy is one of the cross cutting aspect on ICT, and the activities of SC 27 can be applied to the area of big data as well.

JTC 1/SC 38 focuses on the area of "Cloud Computing and Distributed Platforms". JTC1/SC 38 is developing ISO/IEC 19944 which describes data and their flow across devices and cloud services. Table 9-2 lists the JTC 1 deliverables and work items related to big data.

Table 9-2 – JTC 1 deliverables and work items related to big data

Sub group	Reference (Note)	Name/Title	Status
WG 9	[ISO/IEC 20546]	Information technology – Big data – Overview and vocabulary	Aug. 2017
WG 9	[ISO/IEC 20547-1]	Information technology – Big data – Reference architecture – Part 1: Framework and Application Process	Apr. 2017
WG 9	[ISO/IEC 20547-2]	Information technology – Big data – Reference architecture – Part 2: Use Cases and Derived Requirements	Dec. 2016
WG 9	[ISO/IEC 20547-3]	Information technology – Big data – Reference architecture – Part 3: Reference architecture	Dec. 2017
WG 9	[ISO/IEC 20547-5]	Information technology – Big data – Reference architecture – Part 5: Standards roadmap	Apr 2017
SC 27	[ISO/IEC 20547-4]	Information technology – Big data – Reference architecture – Part 4: Security and privacy fabric	May 2018
SC 27	[ISO/IEC 27000]	Information technology – Security techniques – Information security manage systems – Overview and vocabulary	Published 2014
SC 27	[ISO/IEC 27001]	Information technology – Security techniques – Information security manage systems – Requirements	Published 2013
SC 27	[ISO/IEC 27002]	Information technology – Security techniques – Code of practice for information security controls	Published 2013
SC 27	[ISO/IEC 29100]	Information technology – Security techniques – Privacy framework	Published 2011
SC 38	[ISO/IEC 19944]	Information technology – Cloud computing – Data and their flow across devices and cloud services	Oct. 2017
NOTE – Clause I.2 contains a description of each cited reference.			

9.3 W3C

The World Wide Web Consortium (W3C) big data community explores emerging big data pipelines and discusses the potential for developing standard architectures, APIs, and languages that will improve interoperability, enable security, and lower the overall cost of big data solutions. In addition, this group will also develop tools and methods that will enable:

- Trust in big data solutions;
- Standard techniques for operating on big data; and
- Increased education and awareness of accuracy and uncertainties associated with – applying emerging techniques to big data [b-W3C-BDCG].

The W3C Open Government Community Group's mission is to discuss and prepare data and API specifications relating to open government information. This group defines various serializations of the specifications, including but not limited to resource description framework (RDF) and Java script object notation (JSON) [b-W3C-OGCG].

Furthermore, W3C has the following data activities related to big data:

- RDF WG;
- Linked data platform (LDP) WG;
- Data on the Web best practices WG;
- CSV (comma-separated values) on the Web WG.

Table 9-3 lists the W3C deliverables and work items related to big data.

Table 9-3 – W3C deliverables and work items related to big data

Sub group	Reference (Note)	Name/Title	Status
CSV on the Web WG	[W3C MVTD]	Metadata Vocabulary for Tabular Data	Published 2015
CSV on the Web WG	[W3C MTDM]	Model for Tabular Data and Metadata on the web	Published 2015
Government Linked Data WG	[W3C DCAT]	Data Catalog Vocabulary (DCAT)	Published 2014
Government Linked Data WG	[W3C OO]	The Organization Ontology	Published 2014
Linked Data Platform WG	[W3C LDP 1.0]	Linked Data Platform 1.0	Published 2015
RDF WG	JSON-LD 1.0	A JSON-based Serialization for Linked Data	Published 2014
RDF WG	RDF 1.1	RDF 1.1 Concepts and Abstract Syntax	Published 2014
NOTE – Clause I.3 contains a description of each cited reference.			

9.4 OASIS

The following Organization for the Advancement of Structured Information Standards (OASIS) technical committees (TCs) are relevant to big data [b-OASIS]:

- OASIS Advanced Message Queuing Protocol (AMQP) TC: defines a ubiquitous, secure, reliable and open Internet protocol for handling business messaging;
- OASIS Key-Value Database Application Interface (KVDB) TC: defines an open application programming interface for managing and accessing data from database systems based on a key-value model;
- OASIS Message Queuing Telemetry Transport (MQTT) TC: provides a lightweight publish/subscribe reliable messaging transport protocol suitable for communication in machine to machine (M2M) and IoT contexts where a small code footprint is required and/or network bandwidth is at a premium;
- OASIS XML Interchange Language (XMILE) for System Dynamics TC: defines an open XML protocol for sharing interoperable system dynamics models and simulations.

Table 9-4 lists the OASIS deliverables and work items related to big data.

Table 9-4 – OASIS deliverables and work items related to big data

Sub group	Reference (Note)	Name/Title	Status
AMQP TC	[OASIS AMQP 1.0]	Advanced Message Queuing Protocol Version 1.0	Published 2012
MQTT TC	[OASIS MQTT 3.1.1]	Message Queuing Telemetry Transport Version 3.1.1	Published 2014
NOTE – Clause I.4 contains a description of each cited reference.			

9.5 Data Mining Group

The Data Mining Group (DMG) is a vendor led consortium that develops data mining related standards. The DMG develops the Predictive Model Markup Language (PMML), which is an XML-based file format to provide a way for applications to describe and exchange models produced by data mining and machine learning algorithms. Table 9-5 lists the DMG deliverables and work items related to big data.

Table 9-5 – DMG deliverables and work items related to big data

Sub group	Reference (Note)	Name/Title	Status
–	[DMG PMML 4.2.1]	Predictive Model Markup Language 4.2.1	Published 2014
NOTE – Clause I.5 contains a description of each cited reference.			

9.6 TM Forum

The TM Forum (formerly TeleManagement Forum) is a global member association for digital business. The TM Forum published "Guide book for big data analytics" describing best practices on big data. Table 9-6 lists the TM Forum deliverables and work items related to big data.

Table 9-6 – TM Forum deliverables and work items related to big data

Sub group	Reference (Note)	Name/Title	Status
–	[TMF BDAG]	The Big Data Analytics Guidebook	Published 2015
NOTE – Clause I.6 contains a description of each cited reference.			

10 Gap analysis in big data standardization

This clause provides a matrix for gap analysis and the related standardization activities with big data in order to identify standardization gaps.

The matrix is composed of two axes. The horizontal axis describes document categories which cover the subject of applications as follows:

- **General, definition**: the standard which provides general descriptions or terms and definitions of the technology;
- **Common requirements, use cases**: the standard which provides use cases and derived general/functional requirements;

- **Architecture**: the standard which provides reference architecture;
- **API, interface, profile**: the standard which provides common interface, API and/or its profile;
- **Data model, format, schema**: the standard which provides data model or protocol including scheme and/or its encoding format;
- **Others** (e.g., guidelines, technical reports).

The vertical axis describes the related technologies for supporting big data as follows.

- **Fundamental**: concept of big data and its applications;
- **Data exchange**: for supporting big data publishing, sharing, transaction, etc.;
- **Data integration**: with heterogeneous data sources;
- **Analysis/visualization**: for mining model description, etc.;
- **Data provenance/metadata**: for data quality, history tracking, data management, etc.;
- **Security/privacy**: for big data, especially personal identification information;
- **Other**: big data related technologies which are not described above.

NOTE 1 – The items on the horizontal axis are not subordinated to the different technologies.

NOTE 2 – The items on the vertical axis can be modified with technology change.

NOTE 3 – A standard has more than one location on the matrix. In the case that one standard is included in multiple document categories (horizontal axis) or related technologies (vertical axis), it can be mapped several times.

Table 10-1 shows the standardization matrix related to big data.

Table 10-1 – Standardization matrix of big data

	General/ Definition	Common requirement/ Use case	Architecture	API, Interface and its profile	Data model, format, schema	Others (e.g., guideline)
Fundamental	**ITU-T Y.3600** ISO/IEC 20546 ISO/IEC 20547-1	**ITU-T Y.3600**	**ITU-T Y.BDaaS-arch** ISO/IEC 20547-3			
Data exchange	**ITU-T Y.BigDataEX-reqts**	**ITU-T Y.BigDataEX-reqts**			OASIS AMQP 1.0 OASIS MQTT 3.1.1	
Data integration					W3C DCAT W3C JSON-LD 1.0 W3C LDP 1.0 W3C RDF 1.1 W3C OO	
Analysis /Visualization					DMG PMML 4.2.1	TMF BDAG
Data Provenance /Metadata	**ITU-T Y.bdp-reats**	**ITU-T Y.bdp-reats**			W3C MVTD W3C MTDMW	
Security /Privacy	**ITU-T X.1601** ISO/IEC 27000 IEO/IEC 29100	ISO/IEC 20547-4			ISO/IEC 27002 ISO/IEC 27018	**ITU-T X.CSCDataSec** ISO/IEC 27001

Table 10-1 – Standardization matrix of big data

	General/ Definition	Common requirement/ Use case	Architecture	API, Interface and its profile	Data model, format, schema	Others (e.g., guideline)
Others	**ITU-T Y.bDPI-Mec** **ITU-T Y.bDDN-fr**	**ITU-T Y.IoT-BigData-reqts** **ITU-T Y.dsf-reqts** **ITU-T Y.bDDN-req** ISO/IEC 20547-2	**ITU-T Y.SDN-ARCH**			ISO/IEC 19944 ISO/IEC 20547-5

NOTE 4 – The bold letter items in Table 10-1 are ITU-T work in progress activities.

According to the gap analysis in Table 10-1:

- ITU-T has been focusing on 'general/definition', 'common requirement/use cases' with each technical area described in vertical axis;
- It is expected that standardization efforts of ITU-T will be moved to 'architecture' of each technical areas;
- Consideration on standardizing 'analysis/visualization' is needed;
- The entries under the column 'API, interface and its profile' of each of technical standardization areas are empty. These areas are being developed by open source projects, so ITU-T has to consider establishing relationships with them.

Appendix I

Summaries of referenced standardization work items

This appendix provides the summaries of the big data related SDO standardization items specified in clause 9.

NOTE – The summary text comes from the 'scope' or the corresponding part of each item such as 'overview', 'introduction', etc.

I.1 ITU-T references and associated summaries

[ITU-T Y.bDPI-Mec] Mechanism of deep packet inspection applied in network big data context

This proposed Recommendation specifies mechanism of DPI for network big data. The scope of this proposed Recommendation includes:

- overview of big data processing procedure;
- analysing role of DPI in big data processing procedure;
- data classification mechanism used for DPI for big data;
- data pre-processing mechanism used for DPI for big data;
- coordination processing mechanism of DPI in network big data context;
- interfaces between DPI and the upper-layer big data related method.

URL: http://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=10966

[ITU-T Y.bDDN-req] Requirement of big data-driven networking

This proposed Recommendation specifies the requirements of bDDN. bDDN, aims at solving the problem where the valuable information from the network can't effectively be used by the network, through making full use of big data generated by the network itself; this can provide the data intelligence to facilitate network management, operation, control, optimization and security, etc. The scope of this work includes:

- requirements for bDDN;
- requirements of big data plane for bDDN;
- requirements of network plane for bDDN;
- requirements of management plane for bDDN;
- interface requirements for bDDN;

URL: http://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=10967

[ITU-T Y.bDDN-fr] Framework of big data driven networking based on DPI

This proposed Recommendation specifies the framework of data-driven networking based on DPI.

URL: http://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=10629

[ITU-T Y.dsf-reqts] Requirements and Capabilities for Data Storage Federation

This proposed Recommendation specifies requirements and capabilities of data storage federation which is based on the collection of use cases within telecommunication ecosystem, analyses of gaps with different technologies and identification of related documents in cloud computing and big data area.

The scope of this proposed Recommendation includes:

- Overview of data storage federation;
- Requirements of data storage federation;
- Capabilities of data storage federation;
- Use cases of data storage federation.

URL: http://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=10972

[ITU-T Y.3600] Big data – Cloud computing based requirements and capabilities

This proposed Recommendation provides an approach to use cloud computing to meet existing challenges in the use of big data.

The scope of this proposed Recommendation includes:

Overview of big data:

– Cloud computing based big data system context and benefits;
– Cloud computing based big data requirements;
– Cloud computing based big data capabilities.

Overview of cloud computing based big data:

– Big data system context and its activities;
– Cloud computing based big data requirements;
– Cloud computing based big data capabilities;
– Cloud computing based big data use cases and scenarios.

URL: https://www.itu.int/rec/T-REC-Y.3600-201511-I/en

[ITU-T Y.BigDataEX-reqts] Big data exchange framework and requirements

This proposed Recommendation specifies the big data exchange framework and requirements, which is based on the collection of use cases and scenarios, analyses of gaps with different application areas and identification of functional requirements within telecommunication ecosystem.

The scope of this proposed Recommendation consists of:

– Overview of big data exchange;
– Framework of big data exchange;
– Functional requirements of big data exchange.

URL: http://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=10542

[ITU-T Y.BDaaS-arch] Cloud computing - Functional architecture of Big Data as a Service

This proposed Recommendation specifies the functionalities, functional components, functional architecture, and reference points of BDaaS.

The scope of this proposed Recommendation includes:

– Overview of BDaaS functional architecture;
– Functional components of BDaaS;
– Functional architecture of BDaaS;
– Reference points of BDaaS functional architecture.

URL: http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=10548

[ITU-T X.1601] Security framework for cloud computing

This Recommendation analyses security threats and challenges in the cloud computing environment, and describes security capabilities that could mitigate these threats and address security challenges. A framework methodology is provided for determining which of these security capabilities will require specification for mitigating security threats and addressing security challenges for cloud computing.

URL: https://www.itu.int/rec/T-REC-X.1601-201510-I

[ITU-T X.CSCDataSec] Guidelines for cloud service customer data security

This proposed Recommendation provides guidelines for cloud service customer data security in cloud computing, for those cases where the cloud service provider (CSP) is responsible for ensuring that the data is handled with proper security.

This proposed Recommendation, also, identifies security controls for cloud service customer data that can be used in different stages of the full data lifecycle.

URL: http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=10273

[ITU-T Y.IoT-BigData-reqts] Specific requirements and capabilities of the IoT for Big Data

Building on the identified specific requirements of the IoT for big data, the capabilities of the IoT for big data are specified.

The scope of this proposed Recommendation includes:

– Overview of big data in the IoT;
– Requirements of the IoT for big data;
– Capabilities of the IoT for big data.

URL: http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=10258

ITU-T Y.SDN-ARCH Functional architecture of software-defined networking

This proposed Recommendation describes the functional architecture SDN by providing components of the architecture and appropriate interfaces

URL: http://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=10233

[ITU-T Y.bdp-reqts] Big data – Requirements for data provenance

This proposed Recommendation specifies the overview and requirements of big data provenance.

The scope of this proposed Recommendation includes:

– Overview of big data provenance concept including characteristics, application area, and functional framework;
– Requirements of big data provenance;
– Use cases of big data provenance.

I.2 ISO/IEC JTC 1 References and associated summaries

[ISO/IEC WD 20546] Information technology – Big Data – Definition and Vocabulary

This International Standard (under development) provides an overview of big data, along with a set of terms and definitions. It provides a terminological foundation for big data-related standards.

URL: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=68305

[ISO/IEC 20547-1] Information technology – Big data reference architecture – Part 1: Framework and application process

This technical report (under development) describes the framework of the big data reference architecture and the process for how a user of the standard can apply it to their particular problem domain.

[ISO/IEC 20547-2] Information technology – Big data reference architecture – Part 2: Use cases and derived requirements

This technical report (under development) would decompose a set of contributed use cases into general big data reference architecture requirements.

[ISO/IEC 20547-3] Information technology – Big data reference architecture – Part 3: Reference architecture

This International Standard (under development) specifies the big data reference architecture. The reference architecture includes the big data roles, activities, and functional components and their relationships.

[ISO/IEC 20547-4] Information technology – Big data reference architecture – Part 4: Security and privacy fabric

This International Standard (under development) specifies the underlying Security and Privacy fabric that applies to all aspects of the big data reference architecture including the big data roles, activities, and functional components.

[ISO/IEC 20547-5] Information technology – Big data reference architecture – Part 5: Standards roadmap

This technical report provides big data relevant standards, both in existence and under development, along with priorities for future big data standards development based on gap analysis.

[ISO/IEC 19944] Information technology – Cloud computing – Cloud services and devices: data flow, data categories and data use

Establish common and functional ways of understanding and describing the breadth of the cloud service ecosystem.

Enumerate and define the types of connections that can exist between cloud services and customers where their devices are mobile.

Provide foundational concepts necessary to enable others to provide guidance concerning data locality, mobile ecosystem issues, and identity issues.

Identify the types of data that flow across the customers and cloud services ecosystem and that can help cloud customers'

URL: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=66674

[ISO/IEC 27000] Information technology – Security techniques – Information security manage systems – Overview and vocabulary

This International Standard provides the overview of information security management systems, and terms and definitions commonly used in the ISMS family of standards. This International Standard is applicable to all types and sizes of organization (e.g., commercial enterprises, government agencies, not-for-profit organizations).

URL: http://www.iso.org/iso/catalogue_detail?csnumber=63411

[ISO/IEC 27001] Information technology – Security techniques – Information security manage systems – Requirements

This International Standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. This International Standard also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in this International Standard are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

[ISO/IEC 27002] Information technology – Security techniques – Code of practice for information security controls

This International Standard gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

URL: http://www.iso.org/iso/catalogue_detail?csnumber=54533

[ISO/IEC 29100] Information technology – Security techniques – Privacy framework

This International Standard provides a privacy framework which:

– specifies a common privacy terminology;
– defines the actors and their roles in processing personally identifiable information (PII);
– describes privacy safeguarding considerations; and
– provides references to known privacy principles for information technology.

URL: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45123

I.3 W3C references and associated summaries

[W3C DCAT] Data Catalog Vocabulary (DCAT)

The DCAT is an RDF vocabulary designed to facilitate interoperability between data catalogs published on the Web. This document defines the schema and provides examples for its use.

By using DCAT to describe datasets in data catalogs, publishers increase discoverability and enable applications easily to consume metadata from multiple catalogs. It further enables decentralized publishing of catalogs and facilitates federated dataset search across sites. Aggregated DCAT metadata can serve as a manifest file to facilitate digital preservation.

URL: http://www.w3.org/TR/vocab-dcat/

[W3C LDP 1.0] Linked Data Platform 1.0

LDP defines a set of rules for Hypertext Transfer Protocol (HTTP) operations on web resources, some based on RDF, to provide an architecture for read-write Linked Data on the web.

URL: http://www.w3.org/TR/ldp/

[W3C OO] The Organization Ontology

This document describes a core ontology for organizational structures, aimed at supporting linked data publishing of organizational information across a number of domains. It is designed to allow domain-specific extensions to add classification of organizations and roles, as well as extensions to support neighboring information such as organizational activities.

URL: http://www.w3.org/TR/vocab-org/

[W3C MVTD] Metadata Vocabulary for Tabular Data

Validation, conversion, display, and search of tabular data on the web requires additional metadata that describes how the data should be interpreted. This document defines a vocabulary for metadata that annotates tabular data. This can be used to provide metadata at various levels, from groups of tables and how they relate to each other down to individual cells within a table.

URL: http://www.w3.org/TR/tabular-metadata/

[W3C MTDM] Model for Tabular Data and Metadata on the web

This document outlines a data model, or infoset, for tabular data and metadata about that tabular data that can be used as a basis for validation, display, or creating other formats. It also contains some non-normative guidance for publishing tabular data as CSV and how that maps into the tabular data model.

URL: http://www.w3.org/TR/2015/REC-tabular-data-model-20151217/

I.4 OASIS references and associated summaries

[OASIS AMQP 1.0] Advanced Message Queuing Protocol Version 1.0

The AMQP is an open Internet protocol for business messaging. It defines a binary wire-level protocol that allows for the reliable exchange of business messages between two parties. AMQP has a layered architecture and the specification is organized as a set of parts that reflects that architecture.

URL: http://docs.oasis-open.org/amqp/core/v1.0/os/amqp-core-overview-v1.0-os.html

[OASIS MQTT 3.1.1] Message Queuing Telemetry Transport Version 3.1.1

MQTT is a client server publish/subscribe messaging transport protocol. It is light weight, open, simple, and designed so as to be easy to implement. These characteristics make it ideal for use in many situations, including constrained environments such as for communication in M2M and IoT contexts where a small code footprint is required and/or network bandwidth is at a premium.

URL: http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html

I.5 Data Mining Group references and associated summaries

[DMG PMML 4.2.1] Predictive Model Markup Language 4.2.1

PMML is XML-based file format to provide a way for applications to describe and exchange models produced by data mining and machine learning algorithms. It supports common models such as logistic regression and feed forward neural networks.

URL: http://www.dmg.org/v4-2-1/GeneralStructure.html

I.6 TM Forum references and associated summaries

[TMF BDAG] The Big Data Analytics Guidebook

The guidebook provides guidance to a communication service provider on the major components that are needed for the implementation of real-life big data analytics use cases. It defines a reference model, use cases, business value roadmap, building blocks and the analytics big data repository for big data analytics. It also includes addendums, which are;

– Big data analytics use cases – Best practice;
– Big data analytics building blocks – Best practice;
– Big data analytics privacy risk score details – Best practice;
– Big data analytics big data repository – Best practice.

URL: https://www.tmforum.org/resources/collection/gb979-big-data-analytics-solution-suite-r15-5-1/

Bibliography

[b-ITU-T DDN] ITU-T Study Group 13 work in progress Y.bDDN-req, *Requirements of big data-driven networking*. <http://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=10967>

[b-ITU-T DPI] ITU-T Study Group 13 work in progress Y.DPI-ReqFN, *Functional Requirements of Deep Packet Inspection for Future Networks*. <http://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=10546>

[b-ITU-T TSAG] ITU-T Telecommunication Standardization Advisory Group, *Outcome of the workshop session on big data in telecommunications sector*. <http://www.itu.int/en/ITU-T/Workshops-and-Seminars/bigdata/Documents/workshop%20outcome.pdf>

[b-ITU-T TWR] ITU-T Technology Watch Report, November 2013, http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000220001PDFE.pdf *Big data: Big today, normal tomorrow*. <http://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=10546>

[b-Chen] Min Chen, Shiwen Mao, Ying Zhang, *et al.* (2014), *Big Data: Related Technologies, Challenges and Future Prospects*, Springer.

[b-CRA] Challenges and Opportunities with Big Data (2012), *Computing Research Association*, November.

[b-CSA] Cloud Security Alliance (2012), *Top Ten Big Data Security and Privacy Challenges*.

[b-IBM] IBM Data Security and Protection, *What are data security and data privacy?* <http://www-01.ibm.com/software/data/security-privacy/>

[b-JTC 1] ISO/IEC JTC 1 N12395 (2014), *Resolution Adopted at the 29th Meeting of ISO/IEC JTC 1 15-20 November 2014 in Abu Dhabi*.

[b-NEC] NEC (2015), *Software Defined Networking Goes Big: What Big Data Means for SDN*. <http://www.nec.com/en/global/ad/insite/article/bigdata02.html>

[b-OASIS] OASIS Committee Categories: *Big Data*. <https://www.oasis-open.org/committees/tc_cat.php?cat=bigdata>

[b-theguardian] The Guardian, *Big data and open data: what's what and why does it matter?* <http://www.theguardian.com/public-leaders-network/2014/apr/15/big-data-open-data-transform-government>

[b-W3C-BDCG] W3C, *Big Data Community Group*. <http://www.w3.org/community/bigdata/>

[b-W3C-OGCG] W3C, *Open Government Community Group*. <http://www.w3.org/community/opengov/>


STANDARDS

Cloud computing standardization roadmap

Supplement 49 to ITU-T Y.3500-series Recommendation

(11/2018)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Summary

Supplement 49 to ITU-T Y-series Recommendations is provides a summary of the cloud-computing-related deliverables of ITU-T study groups and other standards development organizations (SDOs). For this purpose, the Supplement collects all the information from ITU and other SDOs on their work and understanding related to cloud computing.

Keywords

Analysis matrix, cloud computing, Recommendation, roadmap, standard.

Table of Contents

1 Scope

This Supplement provides a summary of cloud-computing-related deliverables in ITU-T study groups (SGs) and other standards development organisations (SDOs). Also, this supplement provides a common matrix for mapping these deliverables to different cloud-related categories. With the common matrix, this supplement provides analysis for cloud-computing-related deliverables in ITU-T SGs and other SDOs.

2 References

[ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014), *Cloud computing – Overview and vocabulary.*

[ITU-T Y.3501] Recommendation ITU-T Y.3501 (2016), *Cloud computing – Framework and high-level requirements.*

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), Information technology – *Cloud computing – Reference architecture.*

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following terms defined elsewhere:

3.1.1 cloud computing [ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

3.1.2 cloud service [ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.3 cloud service category [ITU-T Y.3500]: Group of cloud services that possess some common set of qualities.

3.1.4 cloud service customer [ITU-T Y.3500]: Party which is engaged in support of, or auxiliary to, activities of either the cloud service provider, or the cloud service customer, or both.

3.1.5 cloud service provider [ITU-T Y.3500]: Party which makes cloud services available.

3.2 Terms defined in this Supplement

None.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

AC Alternating Current

API Application Programming Interface

ATIS Alliance for Telecommunications Industry Solution

BBF Broadband Forum

C&I Conformance and Interoperability

CADF Cloud Auditing Data Federation

CCF Cloud Computing Fundamentals

CCRA Cloud Computing Reference Architecture

CDN Content Distribution Network

CIM Cloud Infrastructure Management

CIMI	Cloud Infrastructure Management Interface
CMP	Cloud Management Platform
CO	Central Office
CP	Cloud Provider
CSA	Cloud Service Agreement
CSB	Cloud Services Brokerage
CSC	Cloud Service Customer
CSDL	Common Schema Description Language
CSN	Cloud Service Partner
CSP	Cloud Service Provider
CSU	Cloud Service User
DaaS	Desktop as a Service
DC	Direct Current
DMTF	Distributed Management Task Force
DSF	Data Storage Federation
EMF	Metro Ethernet Forum
ETSI	European Telecommunications Standards Institute
FCAPS	Fault, Configuration, Accounting, Performance, Security
FN	Future Network
GHG	Greenhouse Gas
GNS	Goods, Networks and Services
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
ICP	Internet Content Provider
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IoT	Internet of Things
IPTV	Internet Protocol Television
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
LCA	Life Cycle Assessment
MIB	Management Information Base
NaaS	Network as a Service
NERG	Network Enhanced Residential Gateway
NFV	Network Function Virtualization
NFVI	Network Function Virtualization Infrastructure

NGN	Next Generation Network
NNI	Network-Network Interconnect
OB	Open Broadband
OBL	Open Broadband Laboratories
OS	Operating System
OVF	Open Virtualization Format
PaaS	Platform as a Service
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PNF	Physical Network Function
REST	Representational State Transfer
RFID	Radio Frequency Identification
RG	Residential Gateway
SaaS	Software as a Service
SDF	Service Delivery Framework
SDN	Software-Defined Networking
SDO	Standards Development Organization
SLA	Service Level Agreement
SLO	Service Level Objective
SMASH	System Management Architecture for Server Hardware
SMI	Service Management Interface
SNMP	Simple Network Management Protocol
SPMF	Scalable Platform Management Forum
SQO	Service Qualitative Objective
UPS	Uninterruptible Power Supply
ViLTE	Video over Long-Term Evolution
VM	Virtual Machine
VNF	Virtualized Network Function
VoLTE	Voice over Long-Term Evolution
XML	Extensible Markup Language

5 Conventions

None.

6 Landscape of cloud computing from ITU-T perspective

Cloud computing is a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on demand.

Below arethe key characteristics of cloud computing described in [ITU-T Y.3500]:

- **Broad network access**: a feature where the physical and virtual resources are available over a network and accessed through standard mechanisms that promote use by heterogeneous client platforms. The focus of this key characteristic is that cloud computing offers an increased level of convenience in that users can access physical and virtual resources from wherever they need to work, as long as it is network accessible, using a wide variety of clients including devices such as mobile phones, tablets, laptops and workstations.
- **Measured service**: a feature where the metered delivery of cloud services is such that usage can be monitored, controlled, reported and billed. This is an important feature needed to optimize and validate the delivered cloud service. The focus of this key characteristic is that the customer may only pay for the resources that they use. From the customers' perspective, cloud computing offers the users value by enabling a switch from a low efficiency and asset utilization business model to a high efficiency one.
- **Multi-tenancy**: a feature where physical or virtual resources are allocated in such a way that multiple tenants and their computations and data are isolated from and inaccessible to one another. Typically, and within the context of multi-tenancy, the group of cloud service users that form a tenant will all belong to the same cloud service customer organization. There might be cases where the group of cloud service users involves users from multiple different cloud service customers, particularly in the case of public cloud and community cloud deployments. However, a given cloud service customer organization might have many different tenancies with a single cloud service provider representing different groups within the organization.
- **On-demand self-service**: a feature where a cloud service customer can provision computing capabilities, as needed, automatically or with minimal interaction with the cloud service provider. The focus of this key characteristic is that cloud computing offers users a relative reduction in the costs, time and effort needed to take an action, since it grants the user the ability to do what they need, when they need it, without requiring additional human user interactions or overheads.
- **Rapid elasticity and scalability**: a feature where physical or virtual resources can be rapidly and elastically adjusted, in some cases automatically, to quickly increase or decrease resources. For the cloud service customer, the physical or virtual resources available for provisioning often appear to be unlimited and can be purchased in any quantity at any time automatically, subject to the constraints of service agreements. Therefore, the focus of this key characteristic is that cloud computing means that customers no longer need to worry about limited resources and might not need to worry about capacity planning.
- **Resource pooling**: a feature where a cloud service provider's physical or virtual resources can be aggregated in order to serve one or more cloud service customers. The focus of this key characteristic is that cloud service providers can support multi-tenancy while at the same time using abstraction to mask the complexity of the process from the customer. From the customer's perspective, all they know is that the service works, while they generally have no control or knowledge over how the resources are being provided or where the resources are located. This offloads some of the customer's original workload, such as maintenance requirements, to the provider. Even with this level of abstraction, it should be pointed out that users might still be able to specify locations at a higher level of abstraction (e.g., country, state, or data centre).

The general requirements for cloud computing described in [ITU-T Y.3501] are as follows:

- **Service life-cycle management**: It is required that the cloud service provider (CSP) supports automated service provisioning, modification and termination during the service life-cycle.
- **Regulatory**: It is required that all applicable laws and regulations be respected, including those related to the protection of personally identifiable information (PII).
- **Security**: It is required that the cloud computing systems provided by a CSP be appropriately secured to protect the interests of all involved parties (e.g., persons and organizations).

– **Accounting and charging**: It is recommended that the cloud services provided by a CSP support various accounting and charging models and policies.
– **Efficient service deployment**: It is recommended that the cloud services provided by a CSP enable the efficient use of resources for service deployment.
– **Interoperability**: It is recommended that the cloud services provided by a CSP comply with appropriate specifications and/or standards for allowing these systems to work together.
– **Portability**: It is recommended that the cloud services provided by a CSP support the portability of software assets and data of cloud service customers (CSCs) with minimum disruption.
– **Service access**: A CSP is recommended to provide CSCs with access to cloud services from a variety of user devices. It is recommended that CSCs be provided with a consistent experience when accessing cloud services from different devices.
– **Service availability, service reliability and quality assurance**: It is recommended that the CSP provides end-to-end quality of service assurance, high levels of reliability and continued availability of cloud services according to the service level agreement (SLA) with the CSC.

7 Overview of cloud computing standard roadmap

7.1 Introduction to standards development organizations (SDOs) for cloud computing

7.1.1 ITU-T SG13

Study Group 13 is responsible for studies relating to the requirements, architectures, capabilities and mechanisms of future networks including studies relating to service awareness, data awareness, environmental awareness and socio-economic awareness of future networks. It is responsible for studies relating to cloud-computing technologies, big data, virtualization, resource management, reliability and security aspects of the considered network architectures.

– Q17/13 (Requirements, ecosystem, and general capabilities for cloud computing and big data)

  The primary focus of this Question is to provide the necessary overall frameworks, definitions and ecosystems, including requirements and capabilities, related to the integration or support of cloud computing and big data models and technologies in telecommunication ecosystems. Also the relationship between cloud computing and big data is developed. This Question is intended to develop new Recommendations for:

  • cloud computing and big data definitions, overview, ecosystem and use cases;
  • cloud computing and big data requirements and capabilities;
  • requirements for interoperability data portability and exchange information in cloud computing and big data;
  • relationship between cloud computing and big data;

– Q18/13 (Cloud functional architecture, infrastructure and networking)

  The main focus of this Question is to provide cloud computing architectures, cloud computing infrastructure and cloud networking views related to the integration and support of the cloud computing paradigm and technologies in telecommunication ecosystems. Another focus of this Question is to provide big data architectures related to the integration and support of the big data paradigm and technologies in telecommunication ecosystems.

  This Question is intended to develop new Recommendations for:

  • cloud computing functional architectures supporting cloud service categories (e.g., NaaS, IaaS, PaaS, BDaaS and XaaS);
  • cloud computing functional architectures of inter-cloud;
  • cloud computing infrastructure including cloud networking aspects (e.g., for the support of network slicing);
  • big data functional architectures including big data exchange functional architecture and cloud-computing-based big data architecture.

– Q19/13 (End-to-end cloud computing management and security)

The primary focus of this Question is cloud service and infrastructure management and the management of composite cloud services and components that use a variety of telecommunication and IT infrastructure resources. These cloud services are typically composed of individual service elements that may be acquired from or exposed to third parties. This is a very complex management environment and requires the study of standards that provide the means to enable consistent end-to-end, multi-cloud management and monitoring of services exposed by and across different service providers' domains and technologies. This Question also includes the study of security mechanisms and methods to streamline and manage service delivery mechanisms across service life cycles so that services can be created and delivered efficiently. The second focus of this Question is big data governance including data management, data preservation, as well as life-cycle management of big data to provide the necessary overall frameworks, definitions and ecosystems including requirements, capabilities related to the integration or support of the big data model and technologies in telecommunication ecosystems.

7.1.2 ITU-T SG17

ITU-T Study Group 17 (SG17) coordinates security-related work across all ITU-T Study Groups. Often working in cooperation with other standards development organizations (SDOs) and various ICT industry consortia, SG17 deals with a broad range of standardization issues.

To give a few examples, SG17 is currently working on cybersecurity; security management; security architectures and frameworks; countering spam; identity management; the protection of personally identifiable information; and the security of applications and services for the Internet of Things (IoT), smart grids, smartphones, software-defined networking (SDN), web services, big data analytics, social networks, cloud computing, mobile financial systems, IPTV and telebiometrics.

One key reference for security standards in use today is Recommendation ITU-T X.509 for electronic authentication over public networks. Recommendation ITU-T X.509, a cornerstone in designing applications relating to public key infrastructure (PKI), is used in a wide range of applications; from securing the connection between a browser and a server on the web, to providing digital signatures that enable e-commerce transactions to be conducted with the same confidence as in a traditional system. Without wide acceptance of the standard, the rise of e-business would have been impossible.

Cybersecurity remains high on SG17's agenda. Additionally, SG17 is coordinating security standardization work covering combating counterfeit and mobile device theft, IMT-2020, cloud-based event data technology, e-health, open identity trust framework, radio frequency identification (RFID), and child online protection.

7.1.3 ITU-T SG5

ITU-T Study Group 5 (SG5) is responsible for studies on methodologies for evaluating ICT effects on climate change and publishing guidelines for using ICTs in an eco-friendly way. Under its environmental mandate, SG5 is also responsible for studying design methodologies to reduce ICTs and e-waste's adverse environmental effects, for example, through the recycling of ICT facilities and equipment.

In addition to its climate-focused activities, the ITU-T Recommendations, Handbooks and other publications produced by SG5 have four main objectives. The first is to protect telecommunication equipment and installations against damage and malfunction due to electromagnetic disturbances, such as those from lightning. In this field, SG5 is one of the world's most experienced and respected standardization bodies.

The second is to ensure the safety of personnel and users of networks against current and voltages used in telecommunication networks. The third is to avoid health risks from electromagnetic fields (EMFs) produced by telecommunication devices and installations. The fourth is to guarantee a good quality of service (QoS) for high-speed data services by providing requirements on characteristics of copper cables and on the coexistence of services delivered by different providers.

7.1.4 ITU-T SG11

Study Group 11 is responsible for developing test specifications for testing conformance and interoperability (C&I) for all types of networks, technologies and services, a testing methodology and test suites for standardized network parameters in relation to the framework for Internet-related performance measurement, as well as for existing technologies (e.g., NGN) and emerging technologies (e.g., FN, cloud, SDN, NFV, IoT, VoLTE/ViLTE, IMT-2020 technologies, flying ad hoc networks, tactile Internet, augmented reality, etc.).

SG11 has been designated Lead study group for establishing test specifications, conformance and interoperability testing for all types of networks, technologies and services that are the subject of study and standardization by all ITU‑T study groups.

7.1.5 ITU-T SG16

ITU-T SG16 is advancing in its IPTV Recommendations, which have been successfully deployed in various countries. However, bearing in mind that the business ecosystem is continuously changing and video-oriented services became prosperous also out of an IPTV domain, SG16 pursues more dynamic and adaptable features for IPTV specifications.

7.1.6 ITU-T SG20

ITU-T SG20 does not have any ongoing work item directly related to "Cloud Computing" at this stage. However, SG20's activities may be linked to the activities in the area of cloud computing in the context of IoT and smart cities and communities. As an example, Q4/20 "*e/Smart services, applications and supporting platforms*" activities on supporting platform technologies for e/Smart services, applications are related to cloud computing.

7.1.7 ITU-T SG2

One of the mandates of ITU-T SG2 is "operational and management aspects of networks, including network traffic management, designations and transport-related operations procedures". ITU-T SG2 is also developing cloud-computing-management-related Recommendations. ITU-T SG2 has developed "Overview of end-to-end cloud computing management" and "Requirements for service management in cloud-aware telecommunication management system" Recommendations. Currently ITU-T SG2 is developing "Requirements for resource management in cloud-aware telecommunication management system" and "Cloud-based network management functional architecture".

7.1.8 JTC 1 SC 38 (Cloud Computing and Distributed Platforms)

SC 38 is a standardization subcommittee in ISO/IEC JTC 1 of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Currently, there are two working groups under SC 38, listed below [b-JTC 1 SC 38].

– WG 3 (Cloud Computing Fundamentals (CCF))
  - Projects related to cloud computing service agreements;
  - projects related to fundamental concepts, terminology and definitions for cloud computing;
  - projects related to guidance on use of international standards in the development of policies that govern or regulate cloud service providers and cloud services, and policies that govern the use of cloud services in enterprise organizations;
  - establish liaisons and collaborate with other entities within JTC 1, SDOs and consortia performing work related to cloud computing.

– WG 5 (Data in cloud computing and related technologies)
  - Standardization in the area of data in cloud computing, distributed platforms, connected devices and related technologies;
  - establish liaisons and collaborate with other entities within and external to JTC 1 as appropriate.

7.1.9 DMTF (Distributed Management Task Force)

The DMTF is an industry standards organization working to simplify the manageability of network-accessible technologies through open and collaborative efforts by leading technology companies. DMTF creates and drives the international adoption of interoperable management standards, supporting implementations that enable the management of diverse traditional and emerging technologies including cloud, virtualization, network and infrastructure [b-DMTF].

The DMTF working groups that deliver standards used in cloud computing are [b-DMGF-WG]:

– Cloud Management Working Group (CMWG)
– Cloud Auditing Data Federation Working Group (CADF)

The DMTF working groups that deliver standards which may be used in cloud data centres are:

– CIM Profile for Platforms and Service Working Group (CPPSWG)
– Open Virtualization Format Working Group (OVF)
– Scalable Platform Management Forum (SPMF)
– Virtualization Management Working Group

7.1.10 TM Forum

TM Forum is the global member association for digital business. It provides a platform for hundreds of global members across a wide range of industries: communications, technology, cities and municipal government, finance, healthcare and so on, to collaborate and partner to co-create, prototype, deliver, and monetize innovative digital services for their billions of customers [b-TMF].

7.1.11 ATIS

ATIS is where leading ICT companies come for solutions when seeking industry alignment to advance their most critical priorities [b-ATIS].

7.1.12 Broadband Forum

The Broadband Forum, a non-profit industry organization, is focused on engineering smarter and faster broadband networks. Their work defines best practices for global networks, enables service and content delivery, establishes technology migration strategies, engineers critical device and service management tools, and is key to redefining broadband. Free technical reports and white papers can be found at broadband-forum.org [b-Broadband].

The Cloud-based Central Office (CloudCO) project is the core of a number of BBF activities applying the design principles of software-defined networking (SDN) and network functions virtualization (NFV) techniques enabling the decentralization of what has traditionally been monolithic networking elements. CloudCO enables dramatically faster and more efficient provisioning of new, cloud-based services.

For management in an SDN&NFV architecture, NETCONF/YANG is expected to play a key role. The CloudCO project is leveraging the work done by the Broadband Forum Common YANG Work Area, which defines the YANG models required for the management of ultrafast broadband networks based on copper and fibre access.

The Open Broadband (OB) programme is a collaborative space for integration, interop, testing of open source, vendor and standards-based implementations. The migration to cloud-based, programmed, virtualized systems and coexistence with existing infrastructure drove OB. OB provides alignment with open source techniques and focus on interoperability to mitigate deployment risks. It provides value to service providers, integrators and suppliers.

Open Broadband Laboratories (OBL) is a collaborative resource for the integration, staging and testing of open source, commercial software, standards-based and vendor implementations where suppliers, integrators and operators can work together on new and coexisting solutions for CloudCO. OBLs are a common hardware and software platform with regional laboratories in Asia, Europe and USA that are open to members and non-members.

7.2 Analysis of deliverable to provide its category

For the analysis of deliverables from clause 7, this supplement provides an analysis template in the form of a matrix table (see Table 7-1).

Table 7-1 – Matrix for analysis of deliverables

	General, definition	Requirements use cases	Architecture	API, interface, profile	Data model, format, schema	Others
Fundamental						
Cloud service category						
Security						
Management						
Inter-cloud, CSB						
SLA, metering						
Testing						
Others						

The vertical axis describes the sub- or related technology. The horizontal axis describes the document category which covers the following applicable subjects:

– General, definition: the standard which provides a general description or terms and definitions of the technology;

– Requirements, use cases: the standard which provides use cases and derived general/functional requirements;

– Architecture: the standard which provides reference architecture;

– API, interface, profile: the standard which provides a common interface, API and/or its profile;

– Data model, format, schema: the standard which provides a data model or protocol including scheme and/or its encoding format;

– Others (e.g., guidelines, technical reports, etc.).

NOTE 1 – The items on the horizontal axis are not subordinate to the different technologies.

NOTE 2 – The items of vertical axis can be modified with technology changes.

NOTE 3 – A standard has more than one location on a matrix. If a standard includes multiple document (horizontal axis) categories or related technologies (vertical axis), it should be mapped multiple times.

8 ITU-T SG13

8.1 Q17

Table 8-1 provides a list of ITU-T Q17/ SG13 deliverables associated with cloud computing.

Table 8-1 – ITU-T Q17/13 deliverables

Title of deliverable	Current status	Starting date	Target date
ITU-T Y.3500|ISO/IEC 17788 Information technology – Cloud computing – Overview and vocabulary	Recommendation | IS	09/2012	08/2014
ITU-T Y.3501, Cloud computing – Framework and high-level requirements	Recommendation 2nd Edition Recommendation	06/2012 05/2015	05/2013 06/2016
ITU-T Y.3503, Requirement for desktop as a service	Recommendation	06/2012	05/2014
ITU-T Y.3600, Big data – cloud computing based requirements and capabilities	Recommendation	06/2013	11/2015
ITU-T Y.3504, Functional architecture for Desktop as a Service	Recommendation	07/2014	06/2016
ITU-T Y.cccm-reqts, Cloud Computing – Requirements for Containers and Micro-services	Draft Recommendation	05/2016	2019-Q4
ITU-T Y.3505, Cloud computing – Overview and functional requirements for data storage federation	Recommendation	05/2016	05/2018
ITU-T Y.ccdc-reqts, Distributed cloud overview and high-level requirements	Draft Recommendation	10/2016	2019-Q2
ITU-T Y.3507, Cloud computing – Functional requirements of physical machine	Recommendation	10/2016	11/2018
ITU-T Y.3506, Cloud computing – Functional requirements for cloud service brokerage	Recommendation	10/2016	05/2018
ITU-T Y.MLaaS-reqts, Cloud computing – Functional requirements for machine learning as a service	Draft Recommendation	01/2018	12/2020
ITU-T Y.BaaS-reqts, Cloud computing – Functional requirements for blockchain as a service	Draft Recommendation	11/2017	12/2020

- **ITU-T Y.3500 | ISO/IEC 17788**: This Recommendation | International Standard provides an overview of cloud computing along with a set of terms, definitions and concepts. It is a terminology foundation for the cloud computing standardization work. This Recommendation | International Standard is applicable to all types of organizations (e.g., commercial enterprises, government agencies, not-for-profit organizations).

  URI: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12210

- **ITU-T Y.3501**: This Recommendation provides a cloud computing framework by identifying high-level requirements for cloud computing. The Recommendation addresses the general requirements and use cases for:
  - cloud computing;
  - Infrastructure as a Service (IaaS), Network as a Service (NaaS), and Desktop as a Service (DaaS) cloud services;
  - inter-cloud, end-to-end resource management, and cloud infrastructure.

  The first release of this Recommendation addresses a set of use cases and related requirements which are included in Appendix I. The second release of this Recommendation provides an update of this set of use cases and requirements. The release concept is described in Appendix II.

  URI: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11917

- **ITU-T Y.3503**: This Recommendation provides use cases, general requirements and functional requirements for Desktop as a Service (DaaS).

  URI: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12167

- **ITU-T Y.3600**: This Recommendation provides an approach to use cloud computing to meet the challenges which exist in the use of big data. It addresses the following subjects:
  - overview of big data;
    - introduction to big data;
    - big data ecosystem and roles;
  - relationship between cloud computing and big data;
  - cloud-computing-based big data system context and benefits;
  - cloud-computing-based big data requirements;
  - cloud-computing-based big data capabilities.

  URI: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12584
- **ITU-T Y.3504**: This Recommendation provides the functional architecture for Desktop as a Service (DaaS) to specify the detailed functional components and their relationships based on the general and functional requirements of [ITU-T Y.3503]. It addresses the following subjects:
  - DaaS functionalities related with DaaS components;
  - DaaS functional architecture;
  - mapping DaaS functional architecture to the cloud computing reference architecture.

  URI: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12889
- **ITU-T Y.cccm-reqts**: This Recommendation provides an overview of the container concept describing its main characteristics and their support of micro-services. The document also identifies typical use cases related to the usage of containers and micro-services in cloud computing identifying use cases related to the support of the Containers as a Service cloud service category by the CSP. Based on the identified use cases, requirements and capabilities are derived regarding the support of the Containers as a Service category. This Recommendation will consider the work as an open source activity initiated by Linux Foundation projects (Open Container Initiative, and Cloud Native Computing Foundation), and ETSI NFV. The scope of this Recommendation consists of:
  - overview of the containers concept;
  - requirements of containers and micro-services;
  - use cases of containers and micro-services.

  URI: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=13641
- **ITU-T Y.3505**: This Recommendation provides an overview and functional requirements of data storage federation. Data storage federation provides a single virtual volume from multiple data sources in heterogeneous storage. In this Recommendation, configuration for logical components, and ecosystem of data storage federation as well as cloud-computing-based data storage federation are introduced for data storage federation. Functional requirements are derived from use cases.

  URI: https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13616
- **ITU-T Y.ccdc-reqts**: This Recommendation provides an overview of the distributed cloud with the main objective of highlighting this important area for future standardization.
  - More specifically, this Recommendation covers the following:
  - definition of distributed cloud;
  - concept and scope of distributed cloud;
  - characteristics of distributed cloud;
  - high-level requirements of distributed cloud;
  - distributed cloud use cases is provided in Appendix I.

  URI: http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=13649

- **ITU-T Y.3507**: This Recommendation provides the functional requirements of the physical machine for cloud computing based on cloud computing infrastructure requirements in [ITU-T Y.3510]. It addresses the following subjects: (i) overview of the physical machine; (ii) functional requirements of the physical machine. The functional requirements provided in this Recommendation are derived from use cases.

  URI: http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=13652

- **ITU-T Y.3506**: Cloud service brokerage is a service that arbitrates, delivers and manages cloud services provided by cloud service providers for cloud service customers. This Recommendation provides the functional requirements of cloud service brokerage. To provide functional requirements for cloud service brokerage, this Recommendation specifies an overview and includes a service model and configuration of cloud service brokerage. Various use cases are also identified to derive the functional requirements.

  URI: https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13612

- **ITU-T Y.MLaaS-reqts**: This Recommendation provides cloud computing requirements for machine learning as a service, which addresses capabilities, and requirements from use cases. Machine learning as a service (MLaaS) is a cloud service category to support the development and applications of machine learning in the cloud computing environments. On the perspective of cloud computing service provisioning, this Recommendation defines the capabilities and functional requirements for MLaaS to identify functionalities such as data gathering, machine learning modelling and computing resources, etc. This is fundamentally aligned with the cloud computing reference architecture of [ITU-T Y.3502].

  NOTE – Developments of machine learning algorithms and methodology are out of the scope of this Recommendation.

  URI: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14484

– **ITU-T Y.BaaS-reqts**: Recommendation ITU-T Y. BaaS-reqts provides the functional requirements for blockchain as a service (BaaS) in the cloud computing environment. Blockchain technologies use decentralized, shared, immutable ledgers to store data and record transactions history, by which the trust, accountability, transparency and efficiency can be achieved. Blockchain technologies include p2p networking, consensus mechanism, smart contract and cipher algorithms, which are now driving various emerging applications across a wide range, such as digital cryptocurrency, finance, insurance, banking, healthcare, government, manufacturing, retail, legal, media and entertainment, supply chain and logistics, accounting, notarization and certification.

  URI: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14485

8.2 Q18

Table 8-2 provides a list of ITU-T Q18/ SG13 deliverables associated with cloud computing.

Table 8-2 – ITU-T Q18/13 deliverables

Title of deliverable	Current status	Starting date	Target date
ITU-T Y.3502 | ISO/IEC 17789 Information technology – Cloud computing – Reference architecture	Recommendation | IS	09/2012	08/2014
ITU-T Y.3510, Cloud computing infrastructure requirements	Recommendation 2nd Edition	06/2012 05/2015	05/2013 02/2016
ITU-T Y.3511, Framework of inter-cloud computing	Recommendation	06/2012	03/2014
ITU-T Y.3512, Cloud computing – Functional requirements of Network as a Service	Recommendation	06/2012	06/2013

Table 8-2 – ITU-T Q18/13 deliverables

Title of deliverable	Current status	Starting date	Target date
ITU-T Y.3513, Cloud computing – Functional requirements of Infrastructure as a Service	Recommendation	02/2013	08/2014
ITU-T Y.3515, Cloud computing – Functional Architecture of Network as a Service	Recommendation	07/2014	02/2017
ITU-T Y.3516, Cloud computing – Functional Architecture of inter-cloud computing	Recommendation	05/2015	07/2017
ITU-T Y.3519, Cloud computing – Functional architecture of Big Data as a Service	Recommendation	05/2015	11/2018
ITU-T Y.dsf-arch, Cloud computing – Functional architecture for data storage federation	Draft Recommendation	05/2018	12/2019

- **ITU-T Y.3502 | ISO/IEC 17789**: This Recommendation | International Standard specifies the cloud computing reference architecture (CCRA). The reference architecture includes the cloud computing roles, cloud computing activities, as well as the cloud computing functional components and their relationships.

  URI: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12209

- **ITU-T Y.3510**: This Recommendation identifies requirements for cloud infrastructure capabilities to support cloud services. The scope of this Recommendation includes:
  - overview of cloud infrastructure;
  - requirements for compute resources;
  - requirements for network resources;
  - requirements for storage resources;
  - requirements for resource abstraction and control.

  URI: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12713

- **ITU-T Y.3511**: This Recommendation describes the framework for interactions of multiple cloud service providers (CSPs) that is referred to as inter-cloud computing. Based on several use cases and consideration of different types of service offerings, this Recommendation describes the possible relationship between multiple CSPs, which are peering, federation and intermediary. By introducing the concept of the primary CSP and /secondary CSPs, the Recommendation further describes CSP interactions in the cases of federation and intermediary patterns. The Recommendation also considers the network significance and its issues. Finally, relevant functional requirements are derived.

  URI: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12078

- **ITU-T Y.3512**: This Recommendation provides use cases and functional requirements of Network as a Service (NaaS), one of the representative cloud service categories. This Recommendation covers the following:
  - high-level concept of NaaS;
  - functional requirements of NaaS;
  - typical NaaS use cases.
  - This Recommendation provides use cases and functional requirements of NaaS application, NaaS platform and NaaS connectivity.

  URI: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12285

- **ITU-T Y.3513**: This Recommendation provides the functional requirements and use cases of Infrastructure as a Service (IaaS), one of the representative cloud service categories. This Recommendation covers the following:
  - general description of IaaS;
  - functional requirements of IaaS;
  - typical IaaS use cases.

  URI: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12286
- **ITU-T Y.3515**: This Recommendation specifies NaaS functional architecture, including functionalities, functional components as well as reference points and procedures, based on the functional requirements specified in [ITU-T Y.3512]. The scope of this Recommendation consists of:
  - overview of NaaS functional architecture;
  - functionalities of NaaS;
  - functional components of NaaS;
  - reference points between functional components of NaaS;
  - procedures for typical NaaS use cases.

  URI: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13255
- **ITU-T Y.3516**: This Recommendation specifies inter-cloud computing functional architecture, including functions and functional components, based on the inter-cloud computing framework specified in [ITU-T Y.3511]. The Recommendation builds upon the functional view of the cloud computing reference architecture [ITU-T Y.3502] and makes extensions to functional components with inter-cloud functions. This Recommendation also describes the mapping between functions and functional requirements of inter-cloud computing and examples of inter-cloud related reference points.

  URI: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13352
- **ITU-T Y.3519**: This Recommendation provides an overview of the big data as a service (BDaaS) functional architecture and defines the BDaaS functional architecture and its cross-cutting aspects by specifying the functional components for the support of BDaaS.

  URI: https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=13627
- **ITU-T Y.dsf-arch**: This Recommendation describes the functional architecture for data storage federation (DSF). The DSF functions based on DSF logical components identified in Y.35XX (ex Y.dsf-reqts) are introduced. The DSF functional architecture, including DSF functions and DSF functional components, is specified. This Recommendation also provides the relationship between the DSF functional architecture and the cloud computing reference architecture.

  URI: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14623

8.3 Q19

Table 8-3 provides a list of ITU-T Q19/ SG13 deliverables associated with cloud computing.

Table 8-3 – ITU-T Q19/13 deliverables

Title of deliverable	Current status	Starting date	Target date
ITU-T Y.3520, Cloud computing framework for end to end resource management	Recommendation 2nd Edition Recommendation	06/2012 05/2015	06/2013 09/2015
ITU-T Y. 3514, Cloud computing – Trusted inter-cloud computing framework and requirements	Recommendation	05/2015	05/2017

Table 8-3 – ITU-T Q19/13 deliverables

Title of deliverable	Current status	Starting date	Target date
ITU-T Y.3518, Cloud computing – Functional requirements of inter-cloud data management	Recommendation	07/2016	11/2018
ITU-T Y.3517, Cloud computing – Overview of inter-cloud trust management	Recommendation	07/2016	11/2018
ITU-T Y.cccsdaom-reqts, Cloud computing – Requirements of cloud service development and operation management	Draft Recommendation	08/2018	09/2020
ITU-T Y.ccm-reqts, Cloud computing maturity requirements and framework	Draft Recommendation	01/2018	12/2019
ITU-T Y.cslm-metadata, Metadata framework for cloud service life-cycle management	Draft Recommendation	03/2017	01/2019
ITU-T Y.e2efapm, Cloud Computing – End-to-end fault and performance management framework of virtual network services in inter-cloud	Draft Recommendation	08/2018	09/2020

- **ITU-T Y.3520**: This Recommendation provides a framework for end-to-end cloud computing resource management. This Recommendation includes:
  - general concepts of end-to-end cloud computing resource management;
  - a vision for adoption of cloud computing resource management in a telecommunication rich environment;
  - end-to-end management of cloud resource and services across multiple platforms, i.e., management of any hardware and software used in support of the delivery of cloud services.

  URI: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12585
- **ITU-T Y.3514**: This Recommendation specifies the framework of trusted inter-cloud computing and relevant use cases, based on the framework specified in [ITU-T Y.3511]. The scope of this Recommendation includes:
  - objectives of trusted inter-cloud computing;
  - requirements for security of trusted inter-cloud;
  - requirements for governance of trusted inter-cloud;
  - requirements for resiliency of trusted inter-cloud.

  URI: https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13254
- **ITU-T Y.3518**: This Recommendation specifies the functional requirements for inter-cloud data management. It provides an overview of inter-cloud data management and inter-cloud data classification in aspects of categories, identification qualifiers and dependency. This Recommendation proposes a set of requirements for inter-cloud data annotation, processing and usage to enable the justification of use of network data plane mechanisms for data protection and traffic isolation. The scope of this Recommendation includes:
  - overview of inter-cloud data management;
  - inter-cloud data classification;
  - requirements for inter-cloud data annotation, processing and usage;
  - requirements for inter-cloud data isolation and protection;
  - requirements for inter-cloud data management.

  URI: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=13645

- **ITU-T Y.3517**: This Recommendation specifies a global overview of inter-cloud trust management including an inter-cloud trust management model and functionalities for managing isolation and security mechanisms needed to guarantee both trust management and/or isolation in an inter-cloud environment. The scope of this Recommendation includes:
  - overview of inter-cloud trust management;
  - inter-cloud trust management model;
  - functionalities for managing isolation and security mechanism;
  - inter-cloud trust management requirements and use cases.

  URI: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=13644
- **ITU-T Y.cccsdaom-reqts**: This proposed draft Recommendation aims to provide the functional requirements of cloud service development and operation management. It covers the following aspects:
  - overview of cloud service development and operation management;
  - functional requirements of cloud service development and operation management;
  - typical use cases of cloud service development and operation management.

  URI: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14746
- **ITU-T Y.ccm-reqts**: This Recommendation specifies cloud computing maturity requirements and framework and relevant use cases. The scope of this Recommendation includes:
  - overview of cloud computing maturity;
  - cloud computing maturity requirements;
  - cloud computing maturity framework;
  - relationship with cloud computing reference architecture;
  - typical use cases of cloud computing maturity.

  URI: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14486
- **ITU-T Y.cslm-metadata**: This Recommendation specifies the metadata framework for cloud service life-cycle management in the closed-loop automation environment.

  URI: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14077
- **ITU-T Y.e2efapm**: This Recommendation specifies an end-to-end fault and performance management framework and relevant use cases of virtual network services in inter-cloud computing. The scope of this Recommendation includes:
  - overview of end-to-end fault and performance management of virtual network services;
  - functional requirements of end-to-end fault and performance management of virtual network services;
  - use cases relevant to end-to-end fault and performance management of virtual network services.

  URI: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14745

8.4 Analysis of ITU-T SG13 deliverables

Table 8-4 gives an analysis of ITU-T SG13 deliverables.

Table 8-4 – Analysis of ITU-T SG13 deliverables

	General, definition	Requirements use cases	Architecture	API, interface, profile	Data model, format, schema	Others
Fundamental	ITU-T Y.3500 | ISO/IEC 17788	ITU-T Y.3501, ITU-T Y.3510, ITU-T Y.3600	ITU-T Y.3502 | ISO/IEC 17789			
Cloud service category		ITU-T Y.3503, ITU-T Y.cccm-reqts, ITU-T Y.3512, ITU-T Y.3513, ITU-T Y.MLaaS-reqts, ITU-T Y.BaaS-reqts, ITU-T Y.ccdc-reqts, ITU-T Y.3507, ITU-T Y.3505	ITU-T Y.3504, ITU-T Y.3515, ITU-T Y.3509, ITU-T Y.dsf-arch			
Security						
Management	ITU-T Y.3520, ITU-T Y.cslm-metadata	ITU-T Y.cccsdaom-reqts, ITU-T Y.ccm-reqts, ITU-T Y.e2efapm				
Inter-cloud, CSB		ITU-T Y.3506, ITU-T Y.3511, ITU-T Y.3514, ITU-T Y.3518, ITU-T Y.3517	ITU-T Y.3516			
SLA, metering						
Testing						
Others						

9 ITU-T JRG-CCM (Joint Rapporteur Group on Cloud Computing Management) of ITU-T SG13 and ITU-T SG2

Table 9-1 provides a list of ITU-T JRG-CCM deliverables associated with cloud computing.

Table 9-1 – ITU-T JRG-CCM deliverables

Title of deliverable	Current status	Starting date	Target date
ITU-T Y.3521/M.3070, Overview of end-to-end cloud computing management	Recommendation	02/2013	03/2016
ITU-T Y.3522, End-to-end cloud service lifecycle management requirements	Recommendation	06/2013	09/2016
ITU-T M.3371, Requirements for service management in cloud-aware telecommunication management system	Recommendation	01/2013	09/2016

- **ITU-T Y.3521/M.3070**: Recommendation ITU-T Y.3521 presents the conceptual view and the common model of end-to-end (E2E) cloud computing management based on the service management interface (SMI) and cloud computing reference architecture, from the perspective of the telecommunications industry.

  URI: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12714

- **ITU-T Y.3522**: This Recommendation specifies the functional requirements of end-to-end (E2E) cloud service life cycle management. This Recommendation consists of the following:
  - cloud service life cycle metadata;
  - cloud service life cycle management framework;
  - cloud service life cycle management stages;
  - relationship with cloud computing reference architecture;
  - functional requirements and typical use cases of cloud service life cycle management.

  URI: https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13020
- **ITU-T M.3371**: This Recommendation defines the general and functional management requirements that support the service management in cloud-aware telecommunication management systems, see [ITU-T M.3070], and provides a functional framework for services management in cloud-aware telecommunication management systems.

  URI: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13064

Table 9-2 provides an analysis of ITU-T JRG-CCM deliverables.

Table 9-2 – Analysis of ITU-T JRG-CCM deliverables

	General, definition	Requirements use cases	Architecture	API, interface, profile	Data model, format, schema	Others
Fundamental						
Cloud service category						
Security						
Management	ITU-T M.3070/ Y.3521	ITU-T M.3371, ITU-T Y.3522				
Inter-cloud, CSB						
SLA, metering						
Testing						
Others						

10 ITU-T SG17

Table 10-1 provides a list of ITU-T SG17 deliverables associated with cloud computing.

Table 10-1– ITU-T SG17 deliverables

Title of deliverable	Current status	Starting date	Target date
ITU-T X.1601, Security framework for cloud computing	Recommendation	04/2010	10/2015
ITU-T X.1631 | ISO/IEC 27017, Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services	Recommendation	05/2013	07/2015
ITU-T X.1642, Guidelines of operational security for cloud computing	Recommendation	03/2012	03/2016

Table 10-1– ITU-T SG17 deliverables

Title of deliverable	Current status	Starting date	Target date
ITU-T X.1602, Security requirements for software as a service application environments	Recommendation	04/2011	03/2016
ITU-T X.1641, Guidelines for cloud service customer data security	Recommendation	09/2014	09/2016
ITU-T X.1603, Data security requirements for the monitoring service of cloud computing	Recommendation	09/2015	03/2018
ITU-T X.SRIaaS, Security requirements of public infrastructure as a service (IaaS) in cloud computing	Draft Recommendation	03/2016	09/2019
ITU-T X.SRNaaS, Security requirements of Network as a Service (NaaS) in cloud computing	Draft Recommendation	09/2016	09/2019
ITU-T X.SRCaaS, Security requirements for Communication as a Service application environments	Draft Recommendation	09/2016	109/2019
ITU-T X.GSBDaaS, Guidelines on security of Big Data as a Service	Draft Recommendation	09/2016	09/2019
ITU-T X.sgcc, Security guidelines for container in cloud computing environment	Draft Recommendation	09/2018	Q4/2020

- **ITU-T X.1601**: This Recommendation provides guidelines for cloud service customer data security in cloud computing, for those cases where the cloud service provider (CSP) is responsible for ensuring that the data is handled with proper security. This is not always the case, since for some cloud services the security of the data will be the responsibility of the cloud service customers (CSCs) themselves. In other cases, the responsibility may be mixed.

  For example, in some cases the CSP may be responsible for restricting access to the data, while the CSC remains responsible for deciding which cloud service users (CSUs) should have access to it, and the behaviour of any scripts or applications with which the CSU processes the data.

  This Recommendation identifies security controls for cloud service customer data that can be used in different stages of the full data life cycle. These security controls may differ when the security level of the cloud service customer data changes. Therefore, the Recommendation provides guidelines on when each control should be used for best security practice.

  URI: http://www.itu.int/ITU-T/recommendations/rec.aspx?id=12613

- **ITU-T X.1631 | ISO/IEC 27017**: Recommendation ITU-T X.1631 | ISO/IEC 27017 provides guidelines for information security controls applicable to the provision and use of cloud services by providing:
  - additional implementation guidance for relevant controls specified in ISO/IEC 27002;
  - additional controls with implementation guidance that specifically relate to cloud services.

  This Recommendation | International Standard provides controls and implementation guidance for both cloud service providers and cloud service customers.

  URI: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12490

- **ITU-T X.1642**: This Recommendation provides guideline of operational security for cloud computing, which includes guidance on service level agreements (SLAs) and daily security maintenance for cloud computing. The target audiences of this Recommendation are cloud service providers, such as traditional telecommunication operators, ISPs and ICPs.

  URI: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12616

- **ITU-T X.1602**: This Recommendation provides a generic functional description for a secure service oriented Software as a Service (SaaS) application environment that is independent of network types, operating systems, middleware, vendor specific products or solutions. In addition, this

Recommendation is independent of any service or scenarios-specific model (e.g., web services, Parlay X or REST), assumptions or solutions. This Recommendation describes a structured approach for defining, designing and implementing secure and manageable service-oriented capabilities in telecommunication cloud computing environments.

URI: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12615

- **ITU-T X.1641**: This Recommendation provides generic security guidelines for cloud service customer (CSC) data in cloud computing. It analyses the CSC data security life cycle and proposes security requirements at each stage of the data life cycle. Furthermore, the Recommendation provides guidelines on when each control should be used for best security practice.

  URI: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12853

- **ITU-T X.1603**: Recommendation ITU-T X.1603 analyses data security requirements for the monitoring service of cloud computing which includes monitoring data scope requirements, monitoring data life cycles, security requirements of monitoring data acquisition and security requirements of monitoring data storage. Monitoring data scope requirements include the necessary monitoring scope that CSPs should provide to maintain cloud security and the biggest monitoring scope of CSPs. Monitoring data life cycles includes data creation, data store, data use, data migrate, data present, data destroy and data backup. Monitoring acquisition determines the security requirements of the acquisition techniques of a monitoring service. Monitoring data storage determines the security requirements for CSPs to store the monitoring data.

  URI: https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=13562

- **ITU-T X.SRIaaS**: Infrastructure as a Service (IaaS) is one of the representative categories of cloud services, in which the cloud capabilities service provided to the CSC is an infrastructure capabilities type. IaaS environments and virtualized services are facing more challenges and threats than traditional information technology infrastructure and applications. Platforms that share computing, storage and network services need protections specific to the threats in the IaaS environment. If these threats are not carefully addressed, it will have very negative impacts on the development of IaaS services. This Recommendation aims to document the security requirements of public IaaS. This will be helpful for IaaS CSPs to improve the overall security level throughout the planning, constructing and operating stages of IaaS platform and services. This work also complements the security standardization activity related to software-defined networks, especially X.sdnsec.

  URI: https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=13578

- **ITU-T X.SRNaaS**: Network as a Service (NaaS) is one of the representative cloud service categories, in which the capability provided to the cloud service customer (CSC) is transport connectivity and related network capabilities. NaaS services can provide any of three cloud capabilities: NaaS application service, NaaS platform service and NaaS connectivity service. All three kinds of NaaS service face particular security challenges such as application security vulnerabilities, security risks of network virtualization, eavesdropping, etc. Recommendation ITU-T X.SRNaaS analyses the security challenges and security requirements of NaaS application, NaaS platform and NaaS connectivity. This Recommendation could help NaaS service providers to address security issues. The capabilities provided by this Recommendation will take into account the national legal and regulatory obligations in individual Member States in which the NaaS services operate. The methodology of this proposal would follow the recommendations of clause 10 in Recommendation ITU-T X.1601.

  URI: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=13590

- **ITU-T X.SRCaaS**: Recommendation ITU-T X.SRCaaS recommends the security requirements of communication as a service (CaaS) application environments with the identification of the risks. The Recommendation describes the scenarios and the features of CaaS, into which multi-communication capabilities are plugged. Moreover, some special /unique risks are identified, which are caused by the unique features of CaaS. The corresponding security requirements are recommended for the following aspects: identity fraud, orchestration security, multi-device security, countering spam, privacy protection, infrastructure attack, attack from infrastructure, Intranet attack and so on. The

Recommendation refers to the common security requirements of Recommendation ITU-T X.1602 to avoid duplicated work. These measures in the requirements take into account the national legal and regulatory obligations in individual Member States in which the platforms operate. The work applies the methodology standardized in clause 10 of Recommendation ITU-T X.1601.

URI: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=13589

- **ITU-T X.GSDBaaS**: The Recommendation analyzes security challenges faced by Big Data as a Service, and provides the componentized security framework of big data platform services, specifies that security protection measures should be satisfied for the activities/components related to BDaaS and roles participated in the big data activities, etc.

  URI: http://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=13591

- **ITU-T X.sgcc**: This Recommendation analyses security threats and challenges on containers in the cloud computing environment, and provides the security guidelines and reference security framework for containers in cloud.

  URI: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14788

Table 10-2 provides an analysis of ITU-T SG17 deliverables.

Table 10-2 – Analysis of ITU-T SG17 deliverables

	General, definition	Requirements use cases	Architec-ture	API, interface, profile	Data model, format, schema	Others
Fundamental						
Cloud service category						
Security	ITU-T X.1601	ITU-T X.1602, ITU-T X.1603, ITU-T X.SRIaaS, ITU-T X.SRNaaS, ITU-T X.SRCaaS,				ITU-T X.1642, ITU-T X.1631, ITU-T X.1641, ITU-T X.GSBDBaaS, ITU-T X.sgcc
Management						
Inter-cloud, CSB						
SLA, metering						
Testing						
Others						

11 ITU-T SG5

Table 11-1 provides a list of ITU-T SG5 deliverables associated with cloud computing.

Table 11-1– ITU-T SG5 deliverables

Title of deliverable	Current status	Starting date	Target date
ITU-T L.1200, Direct current power feeding interface up to 400V at the input to telecommunication and ICT equipment	Recommendation	10/2010	05/2012
ITU-T L.1300, Best practices for green data centres	Recommendation		06/2014

Table 11-1– ITU-T SG5 deliverables

Title of deliverable	Current status	Starting date	Target date
ITU-T L.1410, Methodology for the assessment of the environmental impact of information and communication technology goods, networks and services	Recommendation		12/2014
ITU-T L.1301, Minimum data set and communication interface requirements for data centre energy management	Recommendation		05/2015
ITU-T L.1201, Architecture of power feeding systems of up to 400 VDC	Recommendation		03/2014
ITU-T L.1202, Methodologies for evaluating the performance of an up to 400 VDC power feeding system and its environmental impact	Recommendation		04/2015
ITU-T L.1420, Methodology for energy consumption and greenhouse gas emissions impact assessment of information and communication technologies in organizations	Recommendation		02/2012
ITU-T L.1430, Methodology for assessment of the environmental impact of information and communication technology greenhouse gas and energy projects	Recommendation		12/2013
ITU-T L.1302, Assessment of energy efficiency on infrastructure in data centres and telecommunication centres	Recommendation		11/2015
ITU-T L.1320, Energy efficiency metrics and measurement for power and cooling equipment for telecommunications and data centres	Recommendation		03/2014
ITU-T L.1205, Interfacing of renewable energy or distributed power sources to up to 400 VDC power feeding systems	Recommendation	12/2013	12/2016
ITU-T L.green_mgm_DC, Functionality requirements and framework of green data centre energy-saving management system	WI approved	12/2014	2018
ITU-T L.1440, Methodology for environmental impact assessment of information and communication technologies at city level	Recommendation		10/2015
ITU-T L.1204, Extended architecture of power feeding systems of up to 400 VDC	Recommendation		06/2016
ITU-T L.1220, Innovative energy storage technology for stationary use – Part 1: Overview of energy storage	Recommendation		05/2017
ITU-T L.1206, Impact on ICT equipment architecture of multiple AC, –48 VDC or up to 400 VDC power input	Recommendation		05/2017
L.se_DC, smart energy solutions for data centre and telecommunication centre	Draft Recommendation	05/2017	12/2018

- **ITU-T L.1200**: This Recommendation specifies the direct current (DC) interface between the power feeding system and ICT equipment connected to it. It also describes normal and abnormal voltage ranges, and immunity test levels for ICT equipment to maintain the stability of telecommunication and data communication services. The specified interface is operated from a DC power source of up

to 400 V to allow increased power consumption and equipment power density, in order to obtain higher energy efficiency and reliability with less material usage than using a lower voltage such as –48 VDC or AC UPS power feeding solutions.

URI: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11638

- **ITU-T L.1300**: This Recommendation specifies best practices aimed at developing green data centres. A green data centre can be defined as a repository for the storage, management and dissemination of data in which the mechanical, lighting, electrical and computer systems are designed for maximum energy efficiency and minimum environmental impact. The construction and operation of a green data centre includes advanced technologies and strategies. The Recommendation provides a set of rules to be referred to when undertaking improvement of existing data centres, or when planning, designing or constructing new ones.

  URI: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12204

- **ITU-T L.1410**: Recommendation ITU-T L.1410 deals with environmental life cycle assessments (LCAs) of information and communication technology (ICT) goods, networks and services. It is organized in two parts:

  – Part I: ICT life cycle assessment: framework and guidance
  – Part II: Comparative analysis between ICT and reference product system (Baseline scenario); framework and guidance.

  Part I deals with the life cycle assessment (LCA) methodology applied to ICT goods, networks and services. Part II deals with comparative analysis based on LCA results of an ICT goods, networks and services product system, and a reference product system.

  URI: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12207

- **ITU-T L.1301**: Recommendation ITU-T L.1301 establishes a minimum data set necessary to manage data centres and telecommunication rooms in an environmentally responsible manner.

  The Recommendation specifies the communication interface and defines the parameters to be communicated depending on the equipment used in data centres, such as power systems (alternating current (AC)/direct current (DC) and uninterruptible power supply (UPS) and energy distribution), cooling systems and information and communication technology (ICT) equipment.

  URI: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12428

- **ITU-T L.1201**: Recommendation ITU-T L.1201 describes the architecture of power feeding systems of up to 400 VDC for information and communication technology (ICT) equipment in telecommunication centres, data centres and customer premises. It describes aspects such as configuration, redundancy, power distribution and monitoring, in order to construct safe, reliable and manageable power feeding systems. It can be used also as an architecture reference model for further Recommendations e.g., on the performance of DC power feeding systems.

  URI: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12135

- **ITU-T L.1202**: Recommendation ITU-T L.1202 is provided as a complement to Recommendation ITU-T L.1201, which describes the architecture of direct current (DC) power systems with an up to 400 VDC information and communication technology (ICT) equipment interface. The up to 400 VDC ICT equipment interface is described in Recommendation ITU-T L.1200.

  Recommendation ITU-T L.1202 provides a framework for assessing performances of up to 400 VDC power feeding systems and the savings incurred when compared to other power feeding systems such as the −48 VDC power system and the AC uninterruptable power system (UPS) commonly used in information and communication technology (ICT) sites.

  This Recommendation deals with performance factors such as efficiency, reliability/availability and environmental impact.

  URI: http://www.itu.int/ITU-T/recommendations/rec.aspx?id=12427

- **ITU-T L.1420**: Recommendation ITU-T L.1420 presents the methodology to be followed if an organization intends to claim compliance with this Recommendation when assessing its information and communication technology (ICT) related energy consumption and/or greenhouse gas (GHG) emissions.

  This Recommendation can be used to assess energy consumption and GHG emissions generated over a defined period of time for the following purposes: for assessment of related impact from ICT organizations or for assessment of impact from ICT related activities within non-ICT organizations.

  URI: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11431

- **ITU-T L.1430**: Recommendation ITU-T L.1430 is intended as a complement to ISO standard ISO 14064-2 and the Project Protocol of the Greenhouse Gas Protocol (GHG Protocol).

  This Recommendation provides guidance for the application of a specific methodology to assess the environmental impact of information and communication technology (ICT) greenhouse gas (GHG) and energy projects. This assessment methodology is specifically directed at quantifying and reporting GHG emission reductions, GHG removal enhancements, energy consumption reductions, and enhancement of energy generation and storage in ICT GHG and energy projects.

  An ICT GHG project uses mainly ICT goods, networks and services (GNS) and is designed to reduce GHG emissions or increase GHG removals that are quantified by comparison between the environmental impact of a project activity and a corresponding baseline scenario.

  An ICT energy project uses mainly ICT goods, networks and services to reduce energy consumption and improve energy efficiency.

  From the ICT perspective, this Recommendation takes into account considerations based on existing project quantification guidelines and aims at covering ICT GHG and energy project activities within both the ICT and non-ICT sectors.

  This Recommendation recognizes the importance of project validation and verification for the credibility of project results but does not enforce the validation and verification procedures to be applied. It is expected that such procedures will be determined by the selected GHG programme, national regulations, the project proponent's internal policy or the intended user's request.

  URI: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11904

- **ITU-T L.1302**: Recommendation ITU-T L.1302 contains the energy efficiency assessment methodology for data and telecommunication centres, test equipment accuracy requirements, assessment periods, assessment conditions and calculation methods.

  For data and telecommunication centres, the document was divided into assessment methods for whole data centre /telecommunication centre efficiency and for partial data centre/telecommunication centre efficiency.

  As the main energy consuming infrastructure in data centres/telecommunication centres are power feeding systems (power supply system) and cooling systems, both system energy efficiency measurement methodologies are covered in this Recommendation.

  It takes advantage of methodologies and best practices currently in use or in development in networks and data centres/telecommunication centres.

  This Recommendation aims to reduce the negative impact of data and telecommunication centres through providing the methodologies of energy efficiency assessments. It is commonly recognized that data and telecommunication centres will have an ever-increasing impact on the environment in the future. The application of the assessment methods defined in this Recommendation can help owners and managers to build future data centres/telecommunication centres, or improve existing ones, to operate in an environmentally responsible manner.

  URI: http://www.itu.int/itu-t/recommendations/rec.aspx?rec=12630

- **ITU-T L.1320**: Recommendation ITU-T L.1320 contains the general definition of metrics, test procedures, methodologies and measurement profiles required to assess the energy efficiency of power and cooling equipment for telecommunication and data centres. More detailed measurement procedures and specifications can be developed in future related ITU-T Recommendations.

  Metrics and measurement methods are defined for power equipment, alternating current (AC) power feeding equipment (such as AC uninterruptible power supply (UPS), direct current (DC/AC) inverters), DC power feeding equipment (such as AC/DC rectifiers, DC/DC converters), solar equipment, wind turbine equipment and fuel cell equipment.

  In addition, metrics and measurement methods are defined for cooling equipment such as air conditioning equipment, outdoor air cooling equipment and heat exchanging cooling equipment.

  URI: http://www.itu.int/ITU-T/recommendations/rec.aspx?id=12136

- **ITU-T L.renewable**: This draft document defines the interface and architecture for injecting renewable energy and distributed power sources into an up to 400 V power system as defined in Recommendation ITU-T L.1201.

  URL: http://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=10018

- **ITU-T L.green_mgm_DC**: This Recommendation describes the functionality requirements and framework of green data centre energy-saving management systems. The energy saving will be realized through performance to increase the energy efficiency of data centres. The scope of this Recommendation includes:

  – characteristics and operation flow of green data centre energy-saving management systems;

  – functionality requirements of green data centre energy-saving management systems (e.g., real-time energy consumption data acquisition; energy consumption data analysis and chart show; energy consumption data query; energy consumption monitoring and early warning; strategy optimization, etc.);

  – capability needs of green data centre energy-saving management systems (e.g., collect data from different communication interfaces; secure storage; control management, etc.)

  – framework of green data centre energy-saving management systems.

  Sensor definition, interface and protocol are not included in the scope of this Recommendation.

  URL: http://web.itu.int/ITU-T/workprog/wp_item.aspx?isn=10367

- **ITU-T L.1440**: Recommendation ITU-T L.1440 gives general guidance for city-level environmental assessments related to ICTs, and provides a description of methodologies to be used for the assessment of the environmental impact of ICTs in cities.

  In this first edition of this Recommendation, the assessment is limited to energy consumption and GHG emissions.

  The Recommendation is divided in two parts.

  – Part I relates to the first order effects from the use of ICT goods and networks in a city's organizations and households.

  – Part II relates to the first and second order effects from ICT projects and services applied in the city.

  This Recommendation provides specific guidance in setting the city boundaries, preparing and performing the assessment of ICT-related GHG emissions and energy consumption at the city level.

  URI: http://www.itu.int/ITU-T/recommendations/rec.aspx?id=12431

- **ITU-T L.1204**: Recommendation ITU-T L.1204 describes the extended architecture of power feeding systems of up to 400 volts DC (VDC) for information and communication technology (ICT) equipment in telecommunication centres, data centres and customer premises. It describes aspects such as configuration, redundancy, power distribution and monitoring, in order to construct safe, reliable and manageable power feeding systems. This Recommendation can be used also as an architecture

reference model for future Recommendations, e.g., on the performance of DC power feeding systems. This Recommendation describes extended power feeding architectures using up to 400 VDC, e.g., hybrid redundant DC and AC power feeding based on Recommendation ITU-T L.1201.

URI: http://www.itu.int/itu-t/recommendations/rec.aspx?rec=12882

- **ITU-T L.1220**: This Recommendation provides an overview of evolution of energy storage for stationary use for ICT/telecommunication equipment. Global results of investigations from laboratory and field tests of solutions for site, network, data centre and CPE resilience in smart sustainable cities. Mobile and portable batteries are out of the scope of this Recommendation.

  URI: http://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=10713

  ITU-T L.1206: The document discusses multiple power interfaces to ICT equipment operated by standardized –48V direct current, alternating current source and direct current source up to 400 V in line with the interfaces, operational voltage and characteristics detailed within ITU-T Recommendation and ETSI relevant standards. It also includes some details on the power architecture within the ICT equipment between the ICT power interface and the ICT end load.

  URI: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=13938

  ITU-T L.se_DC: Recommendation "smart energy solutions for data centre and telecommunication centre" defines established clear requirements on data centre and telecommunication centre smart energy system performance, safety, energy efficiency and environmental impacts.

  URI: https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14153

Table 11-2 provides an analysis of ITU-T SG5 deliverables.

Table 11-2 – Analysis of ITU-T SG5 deliverables

	General, definition	Requirements use cases	Architecture	API, interface, profile	Data model, format, schema	Others
Fundamental						
Cloud service category						
Security						
Management		ITU-T L.1301, ITU-T L.green_mgm_DC				ITU-T L.1410
Inter-cloud, CSB						
SLA, metering						
Testing						ITU-T L.1202, ITU-T L.1420, ITU-T L.1430, ITU-T L.1302, ITU-T L.1320, ITU-T L.1440
Others			ITU-T L.1201, ITU-T L.1204	ITU-T L.renewable		ITU-T L.1200, ITU-T L.1300, ITU-T L.1220, ITU-T L.1206, L.se_DC

12 ITU-T SG11

Table 12-1 provides a list of ITU-T SG11 deliverables associated with cloud computing.

Table 12-1– ITU-T SG11 deliverables

Title of deliverable	Current status	Starting date	Target date
ITU-T Q.4040, The framework and overview of cloud computing interoperability testing	Recommendation	02/2013	02/2016
ITU-T Q.4041.1, Cloud computing infrastructure capabilities interoperability testing – part 1: Interoperability testing between the CSC and CSP	Recommendation	04/2015	11/2017
ITU-T Q.4042.1, Cloud interoperability testing for web applications	Recommendation	04/2016	03/2018
ITU-T Q.3914, Set of parameters of cloud computing for monitoring	Recommendation	07/2014	11/2017

- **ITU-T Q.4040**: This Recommendation describes the framework and provides an overview of cloud computing interoperability testing. According to the identified target areas of testing, the framework Recommendation includes overview of cloud computing interoperability testing with common confirmed items, infrastructure capabilities type, platform capabilities type and application capabilities type interoperability testing.

  URI: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12703
- **ITU-T Q.4041.1**: This Recommendation specifies the cloud computing infrastructure capabilities type interoperability testing between the CSC and CSP, including interoperability testing of computing services, storage services, network services and related management functions based on the functional requirements specified in Recommendation ITU-T Y.3513. The test cases of cloud computing infrastructure capabilities type interoperability testing between the CSC and CSP have also been introduced.

  URI: https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13492&lang=en
- **ITU-T Q.4042.1**: This document focuses on the cloud interoperability testing for web applications.

  URI: http://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=13839
- **ITU-T Q.3914**: This Recommendation provides a set of parameters that indicate the status and event of a cloud computing system, including resource layer, service layer and access layer.

  URI: https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13487

Table 12-2 provides an analysis of ITU-T SG11 deliverables.

Table 12-2 – Analysis of ITU-T SG11 deliverables

	General, definition	Requirements use cases	Architec-ture	API, interface, profile	Data model, format, schema	Others
Fundamental						
Cloud service category						
Security						
Management						
Inter-cloud, CSB						
SLA, metering						

Table 12-2 – Analysis of ITU-T SG11 deliverables

	General, definition	Requirements use cases	Architec-ture	API, interface, profile	Data model, format, schema	Others
Testing	ITU-T Q.4040					ITU-T Q.4041.1, ITU-T Q.4042.1, ITU-T Q.3914
Others						

13 ITU-T SG16

Table 13-1 provides a list of ITU-T SG16 deliverables associated with cloud computing.

Table 13-1– ITU-T SG16 deliverables

Title of deliverable	Current status	Starting date	Target date
ITU-T H.248.CLOUD, Gateway control protocol: Cloudification of packet gateways	Draft Recommendation	07/2014	12/2018
ITU-T F.743.2, Requirements for cloud storage in visual surveillance	Recommendation	03/2015	07/2016
ITU-T H.626.2, Architecture for cloud storage in video surveillance	Recommendation	12/2015	12/2017

- **ITU-T H.248.CLOUD**: This Recommendation does not define any new signalling extensions for the ITU-T H.248 gateway control protocol. The purpose of this Recommendation is to provide some kind of guidance to the specification of ITU-T H.248 profiles for ITU-T H.248 gateways in cloud-based network solutions.

  URI: http://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=13278

- **ITU-T F.743.2**: The purpose of this Recommendation is to define the cloud storage service requirements in visual surveillance. Cloud storage enables the service users to have ubiquitous, convenient and on-demand network access to a shared pool of configurable storage resources, which can be rapidly provisioned and released with minimal management effort or service-provider interaction. Cloud storage can realize flexible and reliable data storage for large-scale visual surveillance, and its components are modularized and allocated dynamically based on real usage. This Recommendation provides the application scenarios and the requirements for cloud storage in visual surveillance.

  URI: http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12895

- **ITU-T H.626.2**: This Recommendation defines a cloud storage architecture in visual surveillance. Cloud storage enables the service users to have ubiquitous, convenient and on-demand network access to a shared pool of configurable storage resources, which can be rapidly provisioned and released with minimal management effort or service-provider interaction. Cloud storage can realize flexible and reliable data storage for large-scale visual surveillance, and its components are modularized and allocated dynamically based on real usage. This Recommendation provides the architecture, entities, reference points and service control flow for cloud storage in visual surveillance.

  URI: https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13436

Table 13-2 provides an analysis of ITU-T SG16 deliverables.

Table 13-2 – Analysis of ITU-T SG16 deliverables

	General, definition	Requirements use cases	Architecture	API, interface, profile	Data model, format, schema	Others
Fundamental						
Cloud service category		ITU-T F.743.2	ITU-T H.626.2			
Security						
Management				ITU-T H.248.CLOUD		
Inter-cloud, CSB						
SLA, metering						
Testing						
Others						

14 ITU-T SG2

Table 14-1 below provides a list of ITU-T SG2 deliverables associated with cloud computing.

Table 14-1 – ITU-T SG2 deliverables

Title of deliverable	Current status	Starting date	Target date
ITU-T M.3071, Cloud-based network management functional architecture	Recommendation	04/2016	12/2017
ITU-T M.3372, Requirements for resource management in cloud-aware telecommunication management systems	Recommendation	04/2017	12/2018

- **ITU-T M.3071**: This Recommendation introduces a new network management functional architecture with cloud-computing technology. In this Recommendation, the background and basic concept of cloud-based network management are provided. This Recommendation also provides details of a cloud-based network management functional architecture, including its basic components, functionalities and the relationship between its components.

  URI: https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13479

- **ITU-T M.3372**: This document provides the functional framework and functional requirements for resource management in cloud-aware telecommunication management systems, describes the composition of a functional framework and explains the functions of each component in the framework.

  URI: http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14193

Table 14-2 provides an analysis of ITU-T SG2 deliverables.

Table 14-2 – Analysis of ITU-T SG2 deliverables

	General, definition	Requirements use cases	Architecture	API, interface, profile	Data model, format, schema	Others
Fundamental						
Cloud service category						
Security						
Management		ITU-T M.3372	ITU-T M.3071			
Inter-cloud, CSB						
SLA, metering						
Testing						
Others						

15 ISO/IEC JTC 1 SC 38

Table 15-1 provides a list of ISO/IEC JTC 1 SC 38 deliverables associated with cloud computing.

Table 15-1 – ISO/IEC JTC 1 SC 38 deliverables

Title of deliverable	Current status	Starting date	Target date
ITU-T Y.3500|ISO/IEC 17788, Information technology – Cloud computing – Overview and vocabulary	Recommendation | IS	09/2012	08/2014
ITU-T Y.3502|ISO/IEC 17789, Information technology – Cloud computing – Reference architecture	Recommendation | IS	09/2012	08/2014
ISO/IEC 19086-1, Cloud Computing – Service Level Agreement (SLA) Framework – Part 1 : Overview and Concepts	IS	02/2013	09/2016
ISO/IEC 19086-2, Information Technology – Cloud Computing – Service Level Agreement (SLA) Framework – Part 2 : Metric Model	DIS	10/2014	10/2017
ISO/IEC 19086-3, Information Technology – Cloud Computing – Service Level Agreement (SLA) Framework – Part 3 : Core Conformance Requirements	IS	10/2014	07/2017
ISO/IEC 19086-4, Information Technology – Cloud Computing – Service Level Agreement (SLA) Framework – Part 4 : Security and Privacy	IS	10/2014	01/2018
ISO/IEC 19941, Information Technology – Cloud Computing – Interoperability and Portability	IS	10/2014	10/2017
ISO/IEC 19944, Information Technology – Cloud Computing - Cloud services and devices: data flow,data categories and data use	IS	10/2014	10/2017
ISO/IEC 22123, Information Technology – Cloud Computing – Concepts and terminology	WD	01/2017	01/2020

Table 15-1 – ISO/IEC JTC 1 SC 38 deliverables

Title of deliverable	Current status	Starting date	Target date
ISO/IEC 22624, Information Technology – Cloud Computing - Taxonomy based data handling for cloud services	WD	10/2017	ongoing
ISO/IEC TR 22678, Information Technologies – Cloud Computing – Guidance for Policy Development	WD	04/2017	ongoing
ISO/IEC TR 23186, Information Technologies – Cloud Computing – Framework of trust for processing of multi-sourced data	WD	04/2017	ongoing
ISO/IEC TR 23187, Information technology – Cloud computing – Interacting with cloud service partners (CSNs)	WD	10/2017	ongoing
ISO/IEC TR 23188, Information technology – Cloud computing – Edge computing landscape	WD	10/2017	ongoing
ISO/IEC TS 23167, Information technology – Cloud computing – Common Technologies and Techniques	WD	12/2017	ongoing

- **ITU-T Y.3500|ISO/IEC 17788**: This Recommendation | International Standard provides an overview of cloud computing along with a set of terms, definitions and concepts. It is a terminology foundation for the cloud computing standardization work.

  This Recommendation | International Standard is applicable to all types of organizations (e.g., commercial enterprises, government agencies, not-for-profit organizations).

  URI: https://www.iso.org/standard/60544.html
- **ITU-T Y.3502|ISO/IEC 17789**: This Recommendation | International Standard specifies the cloud computing reference architecture (CCRA). The reference architecture includes the cloud computing roles, cloud computing activities, as well as the cloud computing functional components and their relationships.

  URI: https://www.iso.org/standard/60545.html
- **ISO/IEC 19086-1**: This document seeks to establish a set of common cloud SLA building blocks (concepts, terms, definitions, contexts) that can be used to create cloud service level agreements (SLAs). This document specifies: a) an overview of cloud SLAs; b) identification of the relationship between the cloud service agreement and the cloud SLA; c) concepts that can be used to build cloud SLAs; and d) terms commonly used in cloud SLAs. This document is for the benefit and use of both cloud service providers and cloud service customers. The aim is to avoid confusion and facilitate a common understanding between cloud service providers and cloud service customers. Cloud service agreements and their associated cloud SLAs vary between cloud service providers, and in some cases different cloud service customers can negotiate different contract terms with the same cloud service provider for the same cloud service. This document aims to assist cloud service customers when they compare cloud services from different cloud service providers. This document does not provide a standard structure that can be used for a cloud SLA or a standard set of cloud service level objectives (SLOs) and cloud service qualitative objectives (SQOs) that will apply to all cloud services or all cloud service providers. This approach provides flexibility for cloud service providers in tailoring their cloud SLAs to the particular characteristics of the offered cloud services. This document does not supersede any legal requirement.

  URI: https://www.iso.org/standard/67545.html

- **ISO/IEC 19086-2**: This part of ISO/IEC 19086 defines a model for specifying metrics for cloud service level agreements (SLAs) and includes applications of the model with examples. This part of ISO/IEC 19086 establishes a common terminology and approach for specifying metrics.

  This standard is for the benefit and use of both cloud service providers and cloud service customers.

  This standard is intended to complement ISO/IEC 19086-1, ISO/IEC 19086-3 and ISO/IEC 19086-4.

  This part of ISO/IEC 19086 does not mandate the use of a specific set of metrics for cloud SLAs.

  This part of ISO/IEC 19086 does not supersede any legal requirement.

  URI: https://www.iso.org/standard/67546.html

- **ISO/IEC 19086-3**: This international standard specifies core conformance requirements for service level agreements (SLAs) for cloud services for ISO/IEC 19086. This standard is for the benefit and use for providers and customers.

  This standard does not provide a standard structure that would be used for cloud SLA contracts.

  This document does not supersede any legal requirement.

  URI: https://www.iso.org/standard/67547.html

- **ISO/IEC 19086-4**: This document specifies security and protection of personally identifiable information components, SLOs and SQOs for cloud service level agreements (cloud SLAs) including requirements and guidance. This document is for the benefit and use of both CSPs and CSCs.

  NOTE – ISO/IEC 19086-4 is initiated in JTC 1/SC 38 and transferred to JTC 1/SC 27.

  URI: https://www.iso.org/standard/68242.html

- **ISO/IEC 19941**: This document specifies cloud computing interoperability and portability types, the relationship and interactions between these two cross-cutting aspects of cloud computing, and common terminology and concepts used to discuss interoperability and portability and particularly relating to cloud services. This document is related to other standards namely ISO/IEC 17788, ISO/IEC 17789, ISO/IEC 19086-1, ISO/IEC 19944, and in particular references the cross-cutting aspects and components identified in ISO/IEC 17788 and ISO/IEC 17789 respectively. The goal of this document is to ensure that all parties involved in cloud computing, particularly CSCs, CSPs and CSNs acting as cloud service developers, have a common understanding of interoperability and portability for their specific needs. This common understanding helps to achieve interoperability and portability in cloud computing by establishing common terminology and concepts.

  URI: https://www.iso.org/standard/66639.html

- **ISO/IEC 19944**: This document extends the existing cloud computing vocabulary and reference architecture in ISO/IEC 17788 and ISO/IEC 17789 to describe an ecosystem involving devices consuming cloud services, describes the various types of data flowing within the devices and cloud computing ecosystem, describes the impact of connected devices on the data that flows within the cloud computing ecosystem, describes flows of data between cloud services, cloud service customers and cloud service users, provides foundational concepts, including a data taxonomy, identifies the categories of data that flow across the cloud service customer devices and cloud services. This document is applicable primarily to cloud service providers, cloud service customers and cloud service 56 users, but also to any person or organization involved in legal, policy, technical or other implications of data 57 flows between devices and cloud services.

  URI: https://www.iso.org/standard/66674.html

- **ISO/IEC 22123**: This document provides a consolidated set of terms and definitions extracted from the ISO/IEC cloud computing standards, including, but not limited to, ISO/IEC 17788, ISO/IEC 17789, ISO/IEC 19086, ISO/IEC 19941 and ISO/IEC 19944. In addition, relevant and stable terminology from non-cloud computing ISO sources (e.g., Information technology – Security techniques) and external organization are also included. This document also contains terms and definitions that are not necessarily contained in other works. This document also addresses discrepancies and inconsistencies that have been identified in the consolidated terms and definitions to further enhance the usability of the ISO cloud computing terminology. This document includes additional descriptions and clarifications of cloud computing vocabulary terms, concepts and their inter-relationships.

  URI: https://www.iso.org/standard/72627.html

- **ISO/IEC 22624**: This document:

– describes a framework for the structured expression of data-related policies and practices in the cloud computing environment, based on the data taxonomy in ISO/IEC 19944;

– covers expression of data-related policies and practices including, but not limited to, the following:
  - data geolocation: location of data in various jurisdictions, as it applies to data at rest;
  - cross-border control of data: control of data that resides in different jurisdictions or under different sovereign control depending on their data categorization (ISO/IEC 19944), and/or classification hierarchy and data use statement structure (ISO/IEC 19944);
  - cross-border flow of data: flow of data across borders and in general across various jurisdictions;
  - data portability: portability requirements of data in the cloud computing environment;
  - data classification: policies and practices which vary depending on the classification of the data;
  - data processing: processing of the data either by the CSP or by a 3rd party;
  - data management: management of the data either by the CSP or by a 3rd party;
  - data governance: governance of the data;

– describes how the framework can be used in code(s) of conduct for practices regarding data at rest and in transit, including cross-border transfer of data, as well as remote access to data;

– provides guiding principles on application of the taxonomy for the handling of data based on data subcategory and classification, including the processes that are needed for data in different levels of categorization and classification;

– provides use cases for data sovereignty challenges, i.e. control, access and location of data according to data categories just in-time elevations in data access for people in various roles (e.g., data centre operators and administrators, and other roles in cloud computing).

  This document is applicable primarily to cloud service providers, cloud service customers and cloud service users, but also to any person or organization involved in legal, policy, technical or other implications of taxonomybased data management in cloud services.

  URI: https://www.iso.org/standard/73614.html

- **ISO/IEC TR 22678**: This document provides guidance on the use of international standards as a tool in the development of those policies that govern or regulate cloud service providers (CSPs) and cloud services, and those policies and practices that govern the use of cloud services in enterprise organisations. This includes material that explains cloud computing concepts and the role of cloud computing international standards in formulating policies and practices. The document makes reference to various international standards. Where possible, these standards are ISO/IEC documents. Where a suitable ISO/IEC standard is not available, references are made to documents published by other WTO-registered standards bodies. As explained in the WTO "Technical Barriers to Trade" (TBT) Agreement, standards play a vital role in supporting technical regulations and conformity assessment, however this document does not cover matters of trade.

  URI: https://www.iso.org/standard/73642.html

- **ISO/IEC TR 23186**: This document describes a framework of trust for the processing of multi-sourced data that includes data use obligations and controls, data provenance, chain of custody, security and immutable proof of compliance as elements of the framework.

  URI: https://www.iso.org/standard/74844.html

- **ISO/IEC TR 23187**: This document provides an overview and discussion of interactions between cloud service partners (CSNs), specifically cloud service brokers, cloud service developers and cloud service auditors, and other cloud service entities. In addition, the document describes how cloud service agreements (CSAs) and cloud service level agreements (SLAs) should be used to address those interactions including the following:
  - define terms and concepts and provide an overview for interactions between cloud service partners (CSNs) and cloud service customers (CSCs) and cloud service providers (CSPs);
  - description of types of CSN interactions;
  - description of interactions between CSNs and CSCs;
  - description of interactions between CSNs and CSPs;
  - elements of CSAs and cloud SLAs for CSN interactions, both with CSPs and with CSCs.

  URI: https://www.iso.org/standard/74845.html

- **ISO/IEC TR 23188**: The scope of this technical report is to investigate and report on the concept of edge computing, its relationship to cloud computing and IoT, and the technologies that are key to the implementation of edge computing. This report will explore the following topics with respect to edge computing:
  - concept of edge computing systems;
  - architectural foundation of edge computing;
  - edge computing terminology;
  - software classifications in edge computing – for example: firmware, services, applications;
  - supporting technologies such as containers, serverless, microservices;
  - networking for edge systems, including virtual networks;
  - data – data flow, data storage, data processing in edge computing;
  - management – of software, of data and of networks, resources, quality of service;
  - virtual placement of software and data, and metadata;
  - security and privacy;
  - real time;
  - mobile edge computing, mobile devices.

  URI: https://www.iso.org/standard/74846.html

- **ISO/IEC TR 23167**: This document describes a series of technologies and techniques commonly used to build applications and systems using cloud computing. These include:
  - virtual machines (VMs) and hypervisors;
  - containers and container management systems;
  - "Serverless" computing;
  - Microservices architecture and automation;
  - platform as a service systems and their architecture;
  - storage services;
  - security, scalability and networking as applied to the above cloud computing technologies.

  URI: https://www.iso.org/standard/74845.html

Table 15-2 provides an analysis of JTC 1 SC 38 deliverables.

Table 15-2 – Analysis of JTC 1 SC 38 deliverables

	General, definition	Requirements use cases	Architecture	API, interface, profile	Data model, format, schema	Others
Fundamental	ISO/IEC 17788, ISO/IEC 22123		ISO/IEC 17789			
Cloud service category						
Security	ISO/IEC 19086-4					
Management						
Inter-cloud, CSB	ISO/IEC TR 23187					
SLA, metering	ISO/IEC 19086-1	ISO/IEC 19086-3				ISO/IEC 19086-2
Testing						
Others	ISO/IEC 19941, ISO/IEC 19944		ISO/IEC 22624 ISO/IEC TR 23186			ISO/IEC TR 23188 ISO/IEC TS 23167

16 DMTF

Table 16-1 provides a list of DMTF deliverables associated with cloud computing.

Table 16-1 – DMTF deliverables

Title of deliverable	Current status	Starting date	Target date
DSP0217, System Management Architecture for Server Hardware (SMASH) Implementation Requirements Version 2.1.0	DMTF Standard		12/2014
DSP0243, Open Virtualization Format Specification – Version 1.1.0	DMTF Standard (INCITS & ISO)		08/2015
DSP0243, Open Virtualization Format Specification – Version 2.1.1	DMTF Standard (INCITS)		08/2015
DSP0262, Cloud Auditing Data Federation (CADF) Data Format and Interface Definitions Specification Version 1.0.0	DMTF Standard		07/2014
DSP0263, Cloud Infrastructure Management Interface (CIMI) Model and REST Interface over HTTP e Version 2.0.0	DMTF Standard (ISO) [Chinese]		08/2016

Title of deliverable	Current status	Starting date	Target date
DSP0264, Cloud Infrastructure Management Interface – Common Information Model (CIMI-CIM) Version 1.0.0	DMTF Standard [Chinese]		01/2013
DSP0266, Redfish Scalable Platform Management API Specification Version 1.1.0	DMTF Standard [Chinese]		01/2017
DSP0270, Redfish Host Interface Specification Version 1.0.0	DMTF Standard		01/2017
DSP8009, CIMI XML Schema	DMTF Standard		02/2014
DSP8010, Redfish Schema	DMTF Standard		01/2017
DSP8023, Open Virtualization Format XSD	DMTF Standard		01/2013

- **DSP0217**: The "System Management Architecture for Server Hardware (SMASH) Implementation Requirements" specifies the CIM profile implementation requirements needed for conformance with SMASH 2.0.

  URI: http://dmtf.org/sites/default/files/standards/documents/DSP0217_2.1.0.pdf

- **DSP0243**: The "Open Virtualization Format (OVF) Specification" describes an open, secure, portable and extensible format for the packaging and distribution of software for execution in virtual machines across multiple virtualization platforms. This specification is recognized by INCITS (469-2010) and ISO/IEC (17203:2011).

  URI: http://dmtf.org/sites/default/files/standards/documents/DSP0243_1.1.0.pdf

  Version 2.1.1 of this document extends the format definition to support network ports, scaling at deployment time, basic placement policies, encryption of OVF packages, runtime disk sharing, advanced boot order, advanced data transfer to Guest OS, improved Internationalization – I18N, improved HASH and CIM schema.

  URI: http://dmtf.org/sites/default/files/standards/documents/DSP0243_2.1.1.pdf

- **DSP0262**: The "Cloud Auditing Data Federation (CADF) Data Format and Interface Definitions Specification" document specifies a data model and associated schema definitions to format event records, logs and reports that can be federated and are suitable for audit purposes.

  URI: http://dmtf.org/sites/default/files/standards/documents/DSP0262_1.0.0.pdf

- **DSP0263**: The "Cloud Infrastructure Management Interface (CIMI) Model and REST Interface over HTTP" specifies the model and protocol for management interactions between the provider of a cloud infrastructure as a service (IaaS) and a consumer of that service. The model includes machines, storage and networks within the IaaS provider which the IaaS consumer can perform life cycle management.

  URI: http://dmtf.org/sites/default/files/standards/documents/DSP0263_1.0.1.pdf

- **DSP0264**: The "Cloud Infrastructure Management Interface - Common Information Model" specifies a CIM representation for the logical model contained in the "Cloud Infrastructure Management Interface" document (DSP0263).

  URI: http://dmtf.org/sites/default/files/standards/documents/DSP0264_1.0.0.pdf

- **DSP0266**: The "Redfish Scalable Platform Management API Specification" document specifies RESTful interface semantics to access the data defined in model format to perform out-of-band systems management. It is suitable for a wide range of servers, from standalone servers to rack mount and bladed environments but scales equally well for large-scale cloud environments.

  URI: http://www.dmtf.org/sites/default/files/standards/documents/DSP0266_1.1.0.pdf

- **DSP0270**: The "Redfish Host Interface Specification" document specifies the functional requirements for Redfish host interfaces. The term "host interface" refers to interfaces that can be used by software running on a computer system to access the Redfish Service that is used to manage that computer system.

  URI: http://www.dmtf.org/sites/default/files/standards/documents/DSP0270_1.0.0.pdf
- **DSP8009**: The "CIMI XML Schema" contains the XML schema for representing CIMI interface. (DSP0263).

  URI: http://schemas.dmtf.org/ovf/envelope/2/dsp8009_1.0.2.xsd
- **DSP8010**: The "Redfish Schema' document contain the schema definitions for managing compute platforms. The schema are provided in two formats: json-schema format and OData CSDL (Common Schema Description Language) format.

  URI: http://www.dmtf.org/sites/default/files/standards/documents/DSP8010_2016.3.zip
- **DSP8023**: The "Open Virtualization Format XSD" contains the XML schema for representing DMTF OVF files (DSP0243).

  URI: http://schemas.dmtf.org/ovf/envelope/2/dsp8023_2.0.0.xsd

Table 16-2 provides an analysis of DMTF deliverables.

Table 16-2 – Analysis of DMTF deliverables

	General, definition	Requirements use cases	Architecture	API, interface, profile	Data model, format, schema	Others
Fundamental						
Cloud service category						
Security					DSP0262	
Management				DSP0217, DSP0263, DSP0264, DSP0266, DSP0270	DSP8009, DSP8010, DSP8023	
Inter-cloud, CSB						
SLA, metering						
Testing						
Others						

17 TM Forum

Table 17-1 lists a TM Forum deliverable associated with cloud computing.

Table 17-1 – TM Forum deliverables

Title of deliverable	Current status	Starting date	Target date
TMF061 Release 1.0, Service Delivery Framework (SDF) Reference Architecture, Release 1.0	Published		07/2009

- **TMF061 Release 1.0**: The SDF RA Release 1 defines the scope and characteristics of the essential elements which constitute the patterns that the SDF architecture must support.

  URI: http://www.tmforum.org/TechnicalSpecifications/TMF061ServiceDelivery/39341/article.html

Table 17-2 provides an analysis of ITU-T SG11 deliverables.

Table 17-2 – Analysis of TM Forum deliverables

	General, definition	Requirements use cases	Architecture	API, interface, profile	Data model, format, schema	Others
Fundamental						
Cloud service category						
Security						
Management						
Inter-cloud, CSB						
SLA, metering						
Testing						
Others			TMF061 Release 1.0			

18 ATIS

Table 18-1 provides a list of ATIS deliverables associated with cloud computing.

Table 18-1 – ATIS deliverables

Title of deliverable	Current status	Starting date	Target date
ATIS-0200005, Cloud Framework for Telepresence Service	Published		02/2012
ATIS-0200008, Trusted Information Exchange (TIE)	Published		10/2012
ATIS-0200009, Cloud Service Lifecycle Checklist	Published		11/2012
ATIS-0200006, Virtual Desktop Requirements	Published		05/2012
ATIS-0200010, CDN Interconnection Use Cases and Requirements in a Multi-Party Federation Environment	Published		12/2012
ATIS-0200011, Multicast Delivery of Content to Mobile End User Devices	Approved		02/2014

- **ATIS-0200005**: This specification establishes a foundation for continuing ATIS work efforts on unified visual communications. The specification explores a provider-agnostic and product-agnostic implementation. It will consider two primary aspects of the telepresence service. The first is use cases such as immersive telepresence that are deployed today. The second are future cases resulting from the application of the cloud and service evolution in the future.

  URI: http://www.atis.org/docstore/product.aspx?id=26079

- **ATIS-0200008**: This document describes the Trusted Information Exchange as an aggregated service and lists the high level requirements.

  URI: http://www.atis.org/docstore/product.aspx?id=26798

- **ATIS-0200009**: The cloud service life cycle checklist establishes a baseline of expectations between providers who are interoperating cloud services. The document will also be referenced in cloud service standards to provide a reference model for requirements development. Each enterprise has an existing governance model. The life-cycle checklist provides a way to extend the process model between participating companies.

  URI: http://www.atis.org/docstore/product.aspx?id=27854

- **ATIS-0200006**: This document addresses hosted virtual desktop services for medium and large enterprises. It specifies a federation framework to allow service providers to support high-performance virtual desktops beyond their normal coverage areas. The document also identifies an initial set of infrastructure-service interfaces and related requirements. This is a logical basis for the work on cloud infrastructure federation.

  URI: http://www.atis.org/docstore/product.aspx?id=26147

- **ATIS-0200010**: ATIS Standard ATIS-0200003 provided initial use cases and requirements for content distribution network (CDN) interconnection between two CDN providers via cache-based unicast delivery method. ATIS Standard ATIS-0200004 developed use cases and requirements for content distribution via multicast-based delivery. This standard, ATIS-0200005, extends the use cases and requirements for an environment involving multiple CDN providers joining together to form a CDN federation. The interconnection life-cycle use cases and requirements developed in the previous two ATIS standards are re-examined for the impact arising from a federation of multiple CDN providers. Additional emphasis is placed on the interconnection domain functionality such that guidance on the eventual development of network-network interconnect (NNI) architectures and supporting protocol requirements can be derived.

  URI: http://www.atis.org/docstore/product.aspx?id=27860

- **ATIS-0200011**: This document extends previous ATIS work on multicast-based content delivery methods to mobile end user devices. Three use cases describe potential situations where such devices can receive multicast-based broadcasts of specific live events/video content via the 3GPP Evolved Multimedia Broadcast Multicast System (eMBMS). Delivery processes, assumptions, content delivery network interconnection implications and supporting requirements are also provided.

  URI: https://www.atis.org/docstore/product.aspx?id=28155

Table 18-2 provides an analysis of ITU-T SG11 deliverables.

Table 18-2 – Analysis of ATIS deliverables

	General, definition	Requirements use cases	Architecture	API, interface, profile	Data model, format, schema	Others
Fundamental						
Cloud service category	ATIS-0200005	ATIS-0200006				
Security						
Management		ATIS-0200008				
Inter-cloud, CSB						ATIS-0200009
SLA, metering						
Testing						
Others		ATIS-0200010, ATIS-0200011				

19 Broadband Forum

Table 19-1 provides a list of Broadband Forum deliverables associated with cloud computing.

Table 19-1 – Broadband Forum deliverables

Title of deliverable	Current status	Starting date	Target date
TR-317, Network Enhanced Residential Gateway (NERG)	Published		06/2016
TR-328, Virtual Business Gateway	Published	09/2013	06/2017
TR-345, Broadband Network Gateway and Network Function Virtualization	Published		10/2016
WT-359, A Framework for Virtualization	Published		10/2016
TR-384, Cloud based Central Office Architectural Framework (CloudCO)	Published	09/2016	01/2018
WT-411, Functional module Interface definitions	Draft	09/2017	03/2019
WT-412, Test cases and application notes for Cloud CO system (collaborating with Open Broadband)	Draft	05/2017	05/2018
WT-413, SDN Management and Control Interfaces for CloudCO Network Functions	Draft	09/2017	05/2018
TR-416, CloudCO: Use Cases and Scenarios	Published	09/2016	05/2018

- **TR-317**: Network Enhanced Residential Gateway. This document specifies the network enhanced residential gateway (NERG) architecture. NERG consists in shifting some of the functionality of a residential gateway (RG), as defined in TR-124 to the operator's network.

  URI: https://www.broadband-forum.org/technical/download/TR-317.pdf

- **TR-328**: Virtual Business Gateway. This technical report specifies architecture and requirements for the virtual business gateway. The virtual business gateway architecture supports the migration of functionalities running on a business gateway to the network service provider's infrastructure to enable network-based features and services. Such migration is expected to simplify the deployment and management of the network and business services.

  URI: https://www.broadband-forum.org/technical/download/TR-328.pdf

- **TR-345**: This technical report describes how virtualized network functions (VNFs) and their supporting network function virtualization infrastructure (NFVI) can be integrated with these Broadband Forum architectures. This includes scenarios where NFVI is connected directly to a TR-101 access network and also where VNFs are deployed behind an MS-BNG as part of a service graph.

  URI: https://www.broadband-forum.org/technical/download/TR-345.pdf

- **TR-359**: A Framework for Virtualization. This document significantly enhances the architectural modelling of the management and control of the multi-service broadband network (MSBN). This document combined with TR-384 provides foundational underpinning of BBF work.

  URI: https://www.broadband-forum.org/technical/download/TR-359.pdf

- **TR-384**: Cloud-based Central Office (CloudCO) Reference Architectural Framework. This document specifies the recasting of a central office hosting infrastructure utilizing SDN, NFV and cloud technologies and aligned with the Forum’s Open Broadband (OB) vision. CloudCO enables significantly faster and more efficient provisioning of new cloud-based services to provide rapid availability of new revenue generating services. Collectively the transformational nature of the CloudCO structure and defined functions facilitate choice, adaptability, migration/coexistence and implementation with 'Open Source' to enable agility and a differentiation at the functional level.

  URI: https://www.broadband-forum.org/technical/download/TR-384.pdf

- **WT-411**: Definition of interfaces between Cloud CO functional modules. It defines the interfaces between the functional modules in the Cloud CO architectural framework, as well as the Cloud CO northbound API. Network transport protocols, the data models, schemas or APIs that are signalled across them will be defined as well. Existing open interface works, as described in standards and open source work is being leveraged as much as possible.
- **WT-412**: Test Cases for Cloud CO Applications. This work defines test cases for Cloud CO applications. Cloud CO scenarios are described in Cloud CO application notes. The Cloud CO application notes will detail how a certain service is instantiated, maintained and consumed across the Cloud CO architecture. The test cases will be consumed by the Open Broadband Labs, effectively validating the Cloud CO application note.
- **WT-413**: SDN Management and Control Interfaces for CloudCO Network Functions. This work primarily enables the migration from SNMP/MIB towards NETCONF/YANG interfaces and potentially other protocols to exercise not only traditional FCAPS management functions but also fine grained flow control across VNFs and physical network functions (PNFs) network service graphs. This is an essential step towards software networking introduction, automation and orchestration of PNFs and VNFs in a Cloud CO type of architecture. The development of this Working Text shall also shape the thinking on the way Cloud CO interfaces, especially for VNFs, are modelled and the opportunity to reuse/extend existing YANG work for that.
- **WT-416**: CloudCO Use Cases and Scenarios. This Working Text complements the CloudCO architectural framework specified in TR-384 by describing existing broadband service scenarios supported by the CloudCO architectural framework as well the use cases that can be established using this CloudCO architectural framework.

Table 19-2 provides an analysis of Broadband Forum deliverables.

Table 19-2 – Analysis of Broadband Forum deliverables

	General, definition	Requirements use cases	Architecture	API, interface, profile	Data model, format, schema	Others
Fundamental	TR-359	TR-317, TR-328				
Cloud service category		WT-416	TR-384	WT-411		
Security						
Management				WT-413		
Inter-cloud, CSB						
SLA, metering						
Testing		WT-412				
Others			TR-345			

20 Metro Ethernet Forum

Table 20-1 provides a list of Metro Ethernet Forum deliverables associated with cloud computing.

Table 20-1 – Metro Ethernet Forum deliverables

Title of deliverable	Current status	Starting date	Target date
Carrier Ethernet Services for Cloud Use Cases	Working Drafts	03/2012	04/2014
Carrier Ethernet Services for Cloud Management Interface Profile	Working Drafts	03/2012	04/2014

- **Carrier Ethernet Services for Cloud Use Cases**:
  - includes both single and multiple Ethernet cloud carrier domain cases;
  - Part1: for Cloud Provider Interconnect (CP to CP);
  - Part2: for Enterprise Access to CP.
- **Carrier Ethernet Services for Cloud Management Interface Profile**:
  - identify relevant Protocol Neutral MEF 7.x objects (and attributes);
  - operational use cases and information requirements for CP to ECC management interface;
  - focus on reconfiguration of specific service attributes (e.g., CIR);
  - Phase 1 approach: changes to service attributes occur only when EVC/OVC is inactive or during a maintenance interval;
  - explore scheduled reconfiguration and configuration durations;
  - provide interface operational requirements: number of changes allowed over time (how long change should last); lead time for request fulfilment;
  - describe SLSs for management interactions (performance metrics).

Table 20-2 provides an analysis of Metro Ethernet Forum deliverables.

Table 20-2 – Analysis of Metro Ethernet Forum deliverables

	General, definition	Requirements use cases	Architecture	API, interface, profile	Data model, format, schema	Others
Fundamental						
Cloud service category		Carrier Ethernet Services for Cloud Use Cases				
Security						
Management				Carrier Ethernet Services for Cloud Management Interface Profile		
Inter-cloud, CSB						
SLA, metering						
Testing						
Others						

Bibliography

[b-ATIS] Overview of ATIS. http://www.atis.org/01_about/

[b-Broadband] Mission, Vision of broadband Forum. http://www.broadband-forum.org/about-the-broadband-forum/about-the-forum/mission-and-vision

[b-DMGF-WG] DMTF Working Groups and Committees. https://www.dmtf.org/about/working-groups

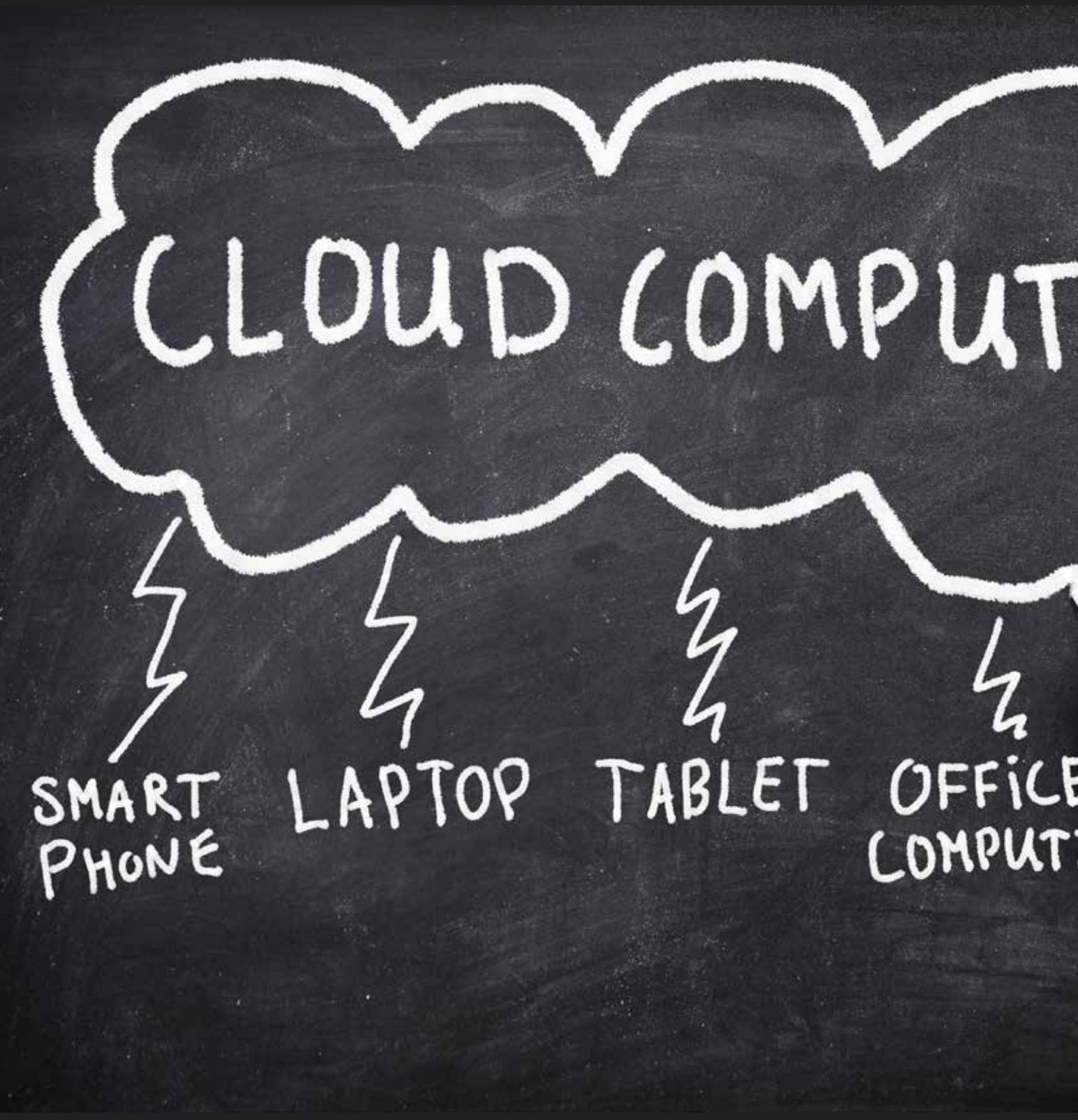
[b-DMTF] DMTF introduction. https://www.dmtf.org/about

[b-JTC 1 SC 38] ISO/IEC Cloud Computing and Distributed Platforms' scope and study groups. https://www.iso.org/isoiec_jtc1sc38.html

[b-TMF] TM Forum's vision. https://www.tmforum.org/

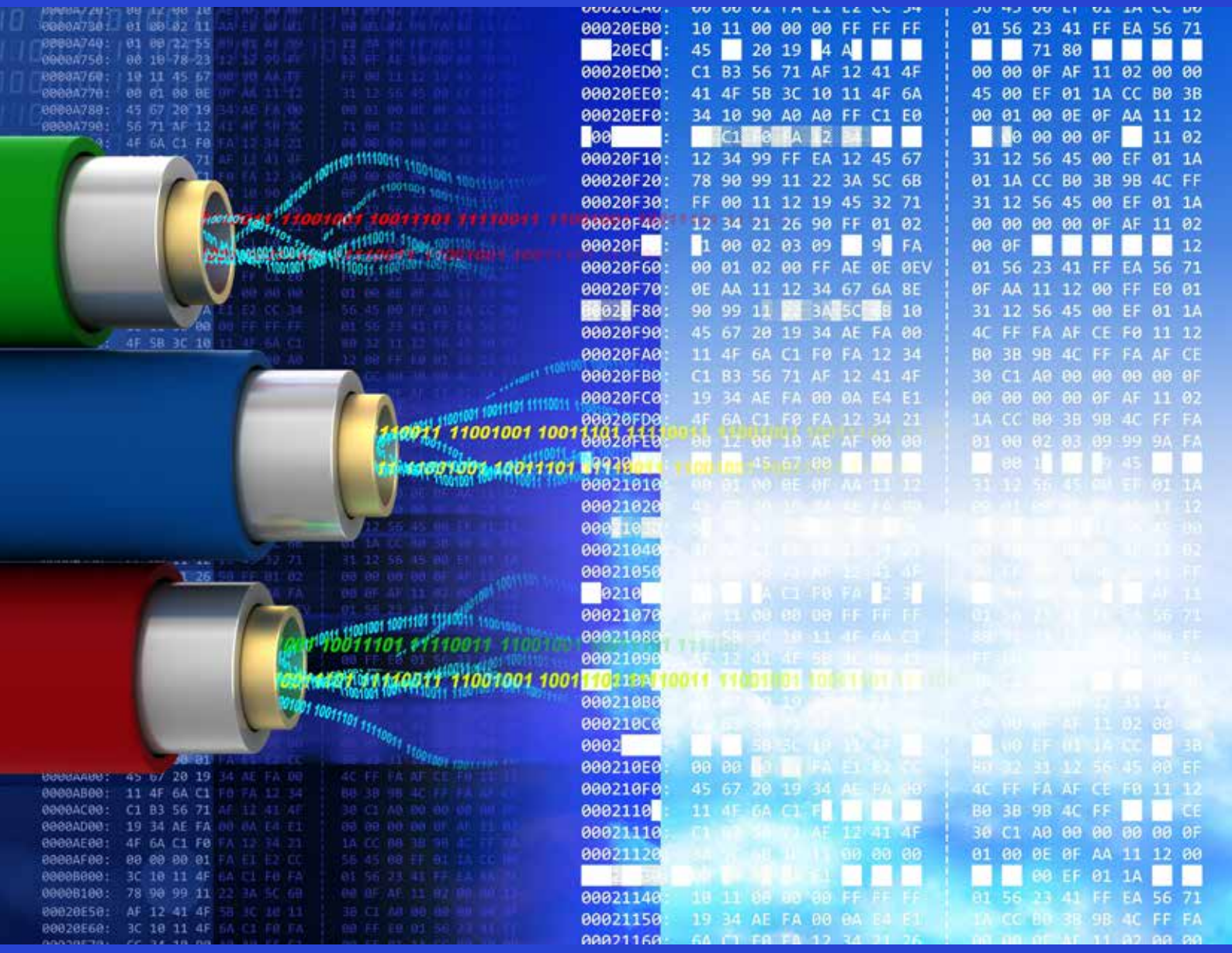
ITU Technology Watch Report

ITU Technology Watch Report (March 2009) "Distributed computing: utilities, grids & clouds" https://www.itu.int/oth/T2301000009/en


CLOUD COMPUT
SMART PHONE
LAPTOP
TABLET
OFFICE COMPUT

2.

Cloud Computing management



Overview of end-to-end cloud computing management

Recommendation ITU-T Y.3521/M.3070

(03/2016)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

SERIES M: TELECOMMUNICATION MANAGEMENT, INCLUDING TMN AND NETWORK MAINTENANCE

Summary

Recommendation ITU-T Y.3521/M.3070 presents a conceptual view and the common model of end to-end (E2E) cloud computing management based on the service management interface (SMI) and cloud computing reference architecture, from the perspective of the telecommunications industry.

Keywords

Cloud computing management, end-to-end, model, multi-cloud, service management interface.

Table of Contents

1 Scope

This Recommendation provides an overview of end-to-end (E2E) cloud computing management.

This Recommendation covers the following:

- cloud computing management objectives from telecommunication industry's perspective;
- conceptual view and management layering;
- common model for multi-cloud environment management;
- cloud computing management functionalities.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing*.

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), *Information technology – Cloud computing – Reference architecture*.

[ITU-T Y.3510] Recommendation ITU-T Y.3510 (2016), *Cloud computing infrastructure requirements*.

[ITU-T Y.3511] Recommendation ITU-T Y.3511 (2014), *Framework of inter-cloud computing*.

[ITU-T Y.3512] Recommendation ITU-T Y.3512 (2014), *Cloud computing – Functional requirements of Network as a Service*.

[ITU-T Y.3520] Recommendation ITU-T Y.3520 (2015), *Cloud computing framework for end to end resource management*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 cloud computing [b-ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

3.1.2 cloud service [b-ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.3 cloud service customer [b-ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

NOTE – A business relationship does not necessarily imply financial agreements.

3.1.4 cloud service provider [b-ITU-T Y.3500]: Party which makes cloud services available.

3.1.5 cloud service user [b-ITU-T Y.3500]: Natural person, or entity acting on their behalf, associated with a cloud service customer that uses cloud services.

NOTE – Examples of such entities include devices and applications.

3.1.6 inter-cloud computing [ITU-T Y.3511]: The paradigm for enabling the interworking between two or more cloud service providers.

NOTE – Inter-cloud computing is also referred as inter-cloud.

3.1.7 management system [b-ITU-T M.60]: A system with the capability and authority to exercise control over and/or collect management information from another system.

3.1.8 service level agreement (SLA) [b-ITU-T Y.3500]: Documented agreement between the service provider and customer that identifies services and service targets.

NOTE 1 – A service level agreement can also be established between the service provider and a supplier, an internal group or a customer acting as a supplier.

NOTE 2 – A service level agreement can be included in a contract or another type of documented agreement.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 service management interface (SMI): Interface that provides a set of management capabilities exposed by a cloud service through which the cloud service can be managed.

NOTE – For additional details of SMI concepts, see [ITU-T Y.3520] and [b-TMF TR198].

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

BSS	Business Support System
CSC	Cloud Service Customer
CSP	Cloud Service Provider
CSU	Cloud Service User
CT	Communication Technology
E2E	End-to-End
EMS	Element Management System
eTOM	Enhanced Telecom Operations Map
IaaS	Infrastructure as a Service
IT	Information Technology
KQI	Key Quality Indicator
NaaS	Network as a Service
NMS	Network Management System
OSS	Operational Support System
PaaS	Platform as a Service
SaaS	Software as a Service
SLA	Service Level Agreement
SLO	Service Level Objective
SMI	Service Management Interface
TMN	Telecommunications Management Network
VM	Virtual Machine

5 Conventions

None.

6 Introduction

In both telecommunication and cloud computing environments, management refers to the ability of maintaining visibility and control of all the managed resources in delivering a service to the customer and satisfying the negotiated service level agreement (SLA). However, until now, these approaches have been different.

For the management of telecommunication services and networks, telecommunication operators (as well as other stakeholders in the telecommunication industry) have applied the mature telecommunications management network (TMN) principles and enhanced telecom operations map (eTOM) as a standard framework and technologies. This has led to the construction of a set of management systems (e.g., element management system (EMS), network management system (NMS), business support system (BSS) or operational support system (OSS)) to realize the required telecommunication management functions.

With the convergence of information technology (IT) and communications technology (CT) industries, cloud computing is being adopted in telecommunication infrastructures. Telecommunication operators are now delivering various cloud services to their users in addition to applying cloud computing technologies for the optimization of their telecommunication service platforms and telecommunication support systems.

Cloud computing has a different management approach in that it does not expose individual elements of itself to the telecommunications management system. Rather, a cloud computing system incorporates its own sophisticated management functionality, which is able to manage the cloud computing system in a coherent manner. Therefore, cloud computing does not distinguish between management operations carried out on behalf of the customer, and identical management operations carried out on behalf of the network operator. Rather, cloud computing defines the role of cloud service customer (CSC) and sub-role of cloud service user (CSU), both of which can be performed by end-customers and telecommunication operators alike.

This Recommendation addresses the need to bring these two very different approaches together.

It is important to note that the creation and use of many cloud-based virtual resources and services are no longer treated as traditional "management" activities, but by the nature of cloud computing are regularly performed in an on-demand self-service manner by CSCs who do not require "management" credentials for this task. As an analogy, many of these tasks are therefore closer to placing telephone calls than to managing telephony equipment.

Many cloud computing use cases extend across multiple cloud service providers (CSPs) and multiple services. CSPs engaged in such a multiple cloud ecosystem therefore, are required to implement appropriate management capabilities on the inter-cloud interfaces [ITU-T Y.3511] to other CSPs. In such a scenario, a single company may be simultaneously acting as a CSP for its own customers, as a CSC for the services provided by another CSP, and as a CSC of its own CSP services.

In a virtualized environment, a CSP focuses on monitoring E2E network and application performance and needs the ability to dynamically add or remove resources when performance requirements change. Considering the addition of multiple technology domains involved, E2E management must cover both virtualized and physical infrastructures across potentially multiple CSPs.

In a multiple cloud environment, the E2E management means composition of:

a) service and resource management chains across:
   i) layers;
   ii) multiple CSPs.

b) service and resource management chains which may include:
   i) the CSC;

ii) one or more CSPs providing the cloud service;

iii) non-cloud-based telecommunications facilities.

See [ITU-T Y.3520] for further information.

Platforms on which the virtual resources are hosted are typically managed within a cloud computing management system, and might not be exposed directly to the telecommunications management system.

Therefore, the introduction of cloud computing brings new aspects to management for telecommunication operators:

- cloud computing roles and sub-roles, see clause 7.2.2 of [ITU-T Y.3502];
- cloud computing multi-layer functions, see clause 7.3.3 of [ITU-T Y.3502], including development environment, test environment, and the cloud computing BSS/OSS functions;
- cloud services, see clause 9.2.3 of [ITU-T Y.3502];
- cloud computing resources, see clause 9.2.4 of [ITU-T Y.3502].

7 Objectives

From the perspective of the telecommunication industry, the following management objectives regarding cloud computing should be considered:

- fulfil the holistic management of cloud computing resources and services together with the existing telecommunications management framework. For the purpose of providing cloud services effectively, both the telecommunication BSS/OSS and the cloud BSS/OSS should collaborate properly to support the holistic management of cloud computing resources and services, together with telecommunication networks;
- fulfil the network management needs of cloud computing. As defined in [ITU-T Y.3510] and [ITU-T Y.3512], network resources (e.g., bandwidth, switching and routing, network addresses) will need to be scalable, and adapt dynamically to the traffic generated. Telecommunication operators will need to provision self-managed and on-demand network capability to meet various requirements from the cloud service, and to apply dynamic control and adapt its configuration (including network bandwidth, protocols, codecs, security mechanisms, etc.) over the telecommunication network on the direct request of cloud services or CSCs;
- realize E2E service quality management. E2E service quality management is vital for telecommunication services which are deployed using cloud computing resources and services. Telecommunication services demand high availability, high security, and excellent service experience (e.g., short response times, high service success rate). Telecommunication operators need to be able to control and manage the cloud computing resources and services for the purpose of ensuring E2E telecommunication service quality and CSC experience.

8 Conceptual view and management layering

This clause defines the conceptual view of cloud computing management based on the cloud computing reference architecture [ITU-T Y.3502], cloud computing management layers and the service management interface (SMI) approach.

8.1 Cloud computing management layering

Figure 8-1 presents a comprehensive view of cloud computing management. It shows the management layers of a cloud computing system:

- customer management;
- product management;
- service management;
- resource management.

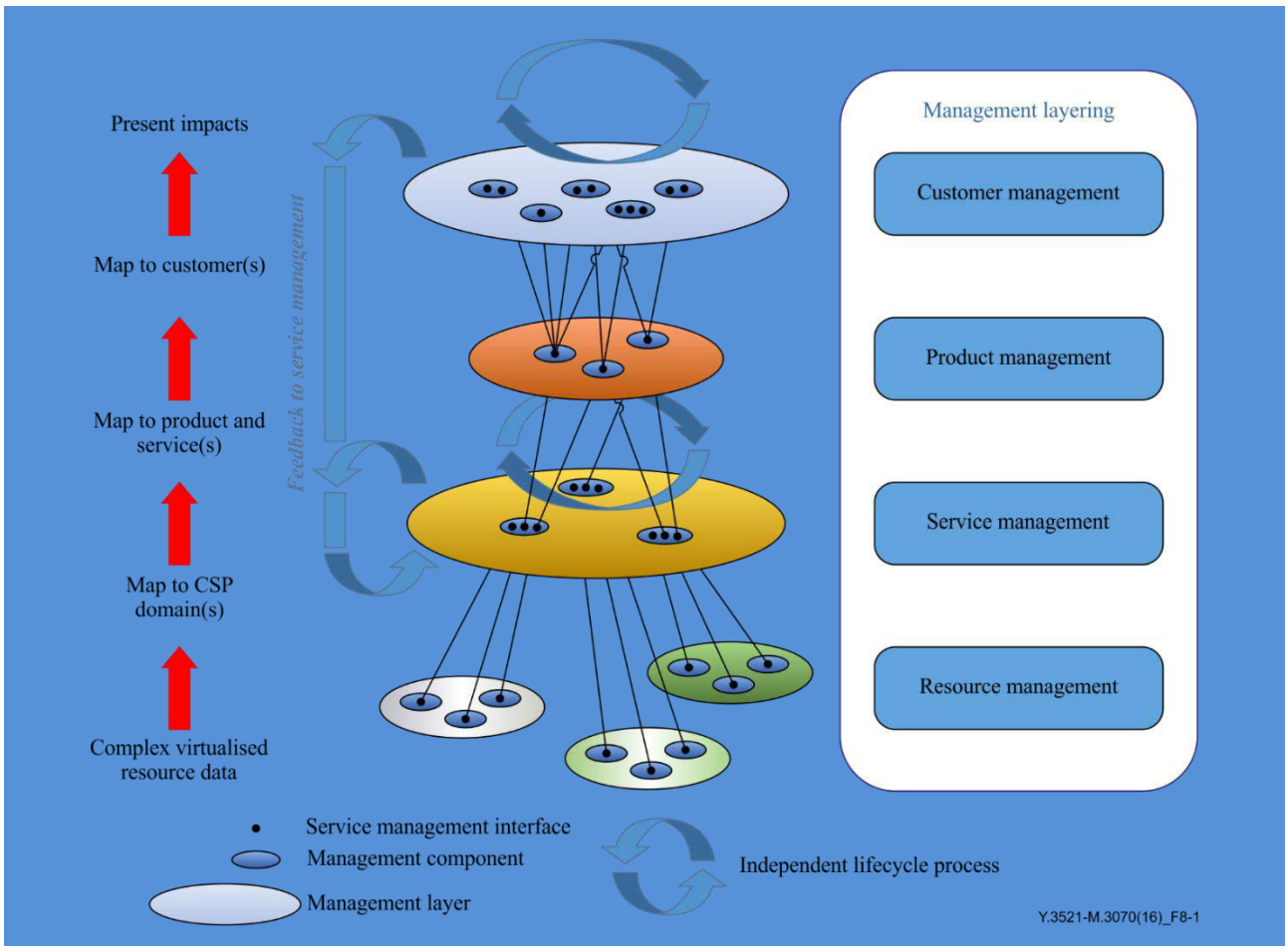


Figure 8-1 – Comprehensive view of cloud computing management

As shown in Figure 8-1, cloud computing management is realized based on SMIs, which correlate layers determined in the reference architecture of cloud computing [ITU-T Y.3502] to offer complete E2E management service chains (see clause 6).

A management layer represents a level of abstraction within the management system, such that higher layers do not need to interact directly with low-level managed elements or components.

A management component as represented here refers to a collection of management functionality that has responsibility for a specific area within a management layer.

The SMIs allow elements, components, and layers to expose management information and telemetry in a consistent matter that can be rolled up into a comprehensive diagnostics and management service.

See Appendix I for a complex scenario example of the use of this concept.

The purposes of the management layers are described below.

8.1.1 Customer management layer

The customer management layer considers the fundamental knowledge of customers' needs and includes all functionalities necessary for the acquisition, enhancement and retention of a relationship with a customer.

For details of the functionalities present in the customer management layer, see clause 10.1.

8.1.2 Product management layer

The product management layer includes the necessary management functions for maintaining the existing product catalogue and providing necessary functions for products sale.

For details of the functionalities present in the product management layer, see clause 10.2.

8.1.3 Service management layer

The service management layer focuses on the knowledge of cloud services and includes all functionalities necessary for the management and operations of cloud services required by or proposed to customers. The focus is on cloud service delivery and management as opposed to the management of the underlying resources.

This layer is accountable for cloud service delivery such as service instance management, and cloud service operation such as service monitoring and problem handling and the assurance of the service quality.

For details of the functionalities present in the service management layer, see clause 10.3.

8.1.4 Resource management layer

The resource management layer is responsible for maintaining knowledge of resources (application, computing and network infrastructures) and for managing all these resources (e.g., networks, IT systems, servers, routers) utilized to deliver and support cloud services required by or proposed to customers.

For details of the functionalities present in the resource management layer, see clause 10.4.

8.2 Service management interface

The SMI-based approach provides a means to allow consistent E2E management of cloud computing services exposed by, and across, different domains of CSPs thus unifying the traditional telecommunication environment and the cloud computing environment.

The SMI capabilities include the following:

- activation of a cloud service, i.e., making a cloud service available for a particular context (deploying a cloud service instance);
- provisioning of a cloud service, i.e., configuring the settings of a cloud service instance;
- status monitoring of a cloud service instance, i.e., querying the history and current status in terms of lifecycle management for a specific cloud service instance;
- usage monitoring of a cloud service instance, i.e., querying for usage metrics from a cloud service instance or listening for usage metrics reports or alarms (e.g., if metrics conditions imply notifications);
- health monitoring of a cloud service instance, i.e., querying for health metrics from a cloud service instance;
- update of a cloud service instance, i.e., modification of the setting or lifecycle management status of a cloud service instance;
- de-activation of a cloud service, i.e., making a cloud service unavailable.

A further description of how the SMI-based model can be used across various cloud computing reference architecture layers can be found in Annex A.

8.3 Relationship with the cloud computing reference architecture

Figure 8-2 illustrates the relationship between the management layers described in clause 8.1 and the BSS and OSS components of the cloud computing reference architecture as defined in [ITU-T Y.3502].

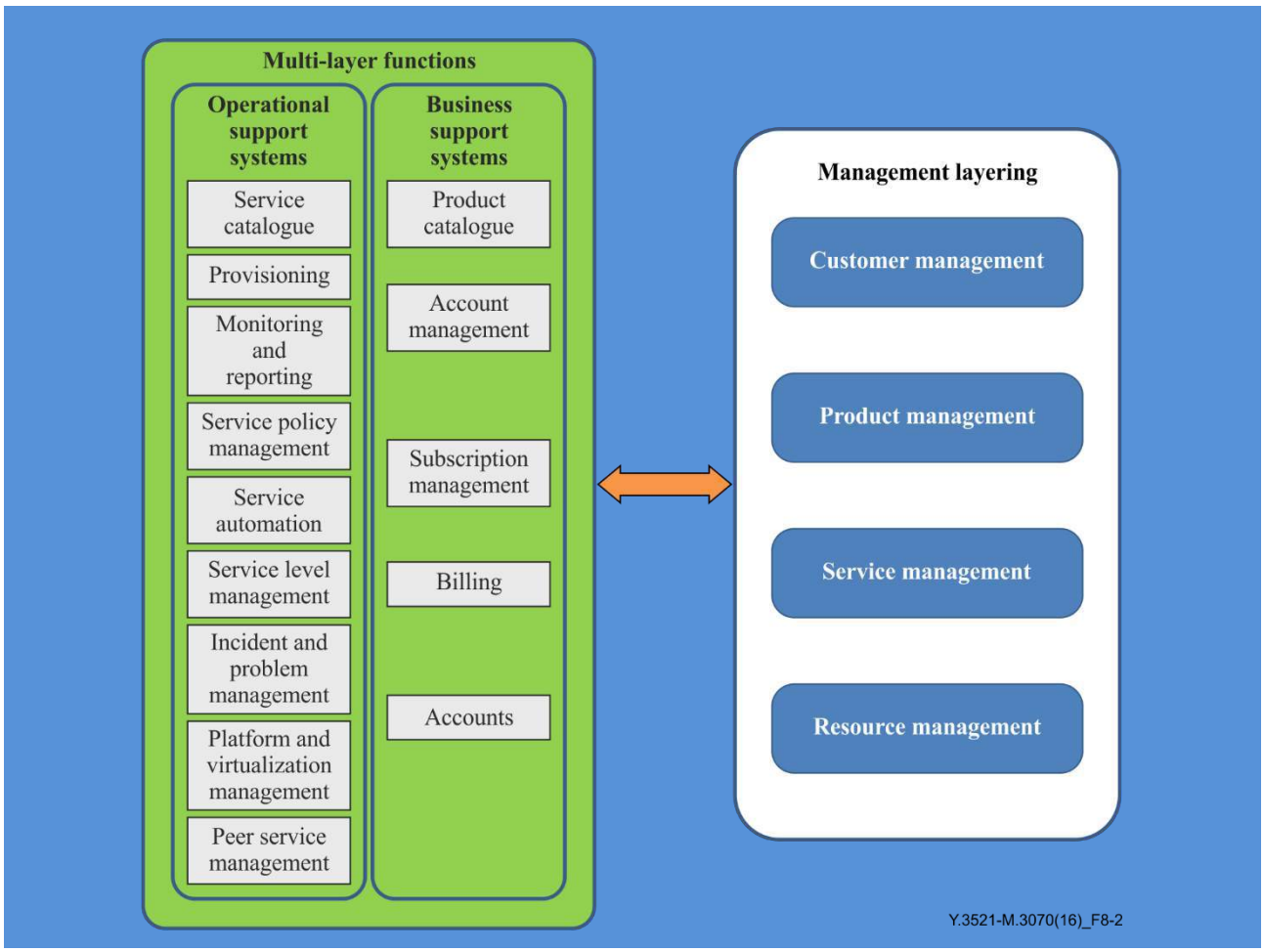


Figure 8-2 – Relationship of BSS/OSS components and the management layering

The cloud computing management layers support the management requirements of cloud computing to provision, operate and administer cloud computing resources and services, and consists of: customer management, product management, service management and resource management.

The OSS functional components encompass the set of operational related management capabilities that are required in order to manage and control the cloud services offered to customers (see clause 9.2.5.3 of [ITU-T Y.3502]). The BSS functional components encompass the set of business-related management capabilities dealing with customers and supporting processes (see clause 9.2.5.4 of [ITU-T Y.3502]).

Figure 8-3 shows how the OSS and BSS components of the cloud computing reference architecture are further split according to the different management layers based on the conceptual view of cloud computing management provided in clause 8.

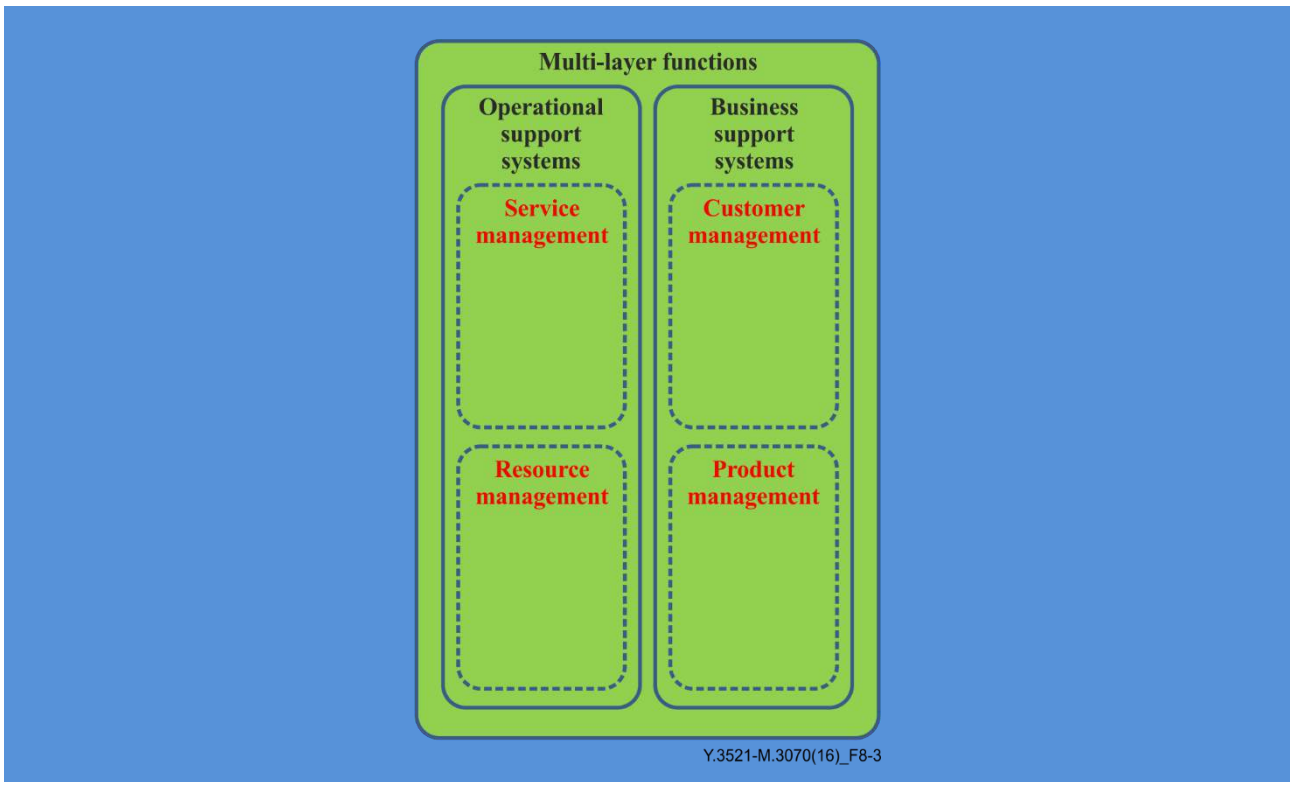


Figure 8-3 – Split of OSS/BSS components according to management layers

9 Common model for E2E cloud computing management

This clause describes a common management model, based on SMIs, for all layers of the cloud computing reference architecture. This allows management of E2E cloud computing applications and solutions in a multi-cloud computing environment, independently from the choice of technology, run-time, programming language or tools made to develop the solutions. This common management model also shows the concept of E2E cloud integrated telecommunications management.

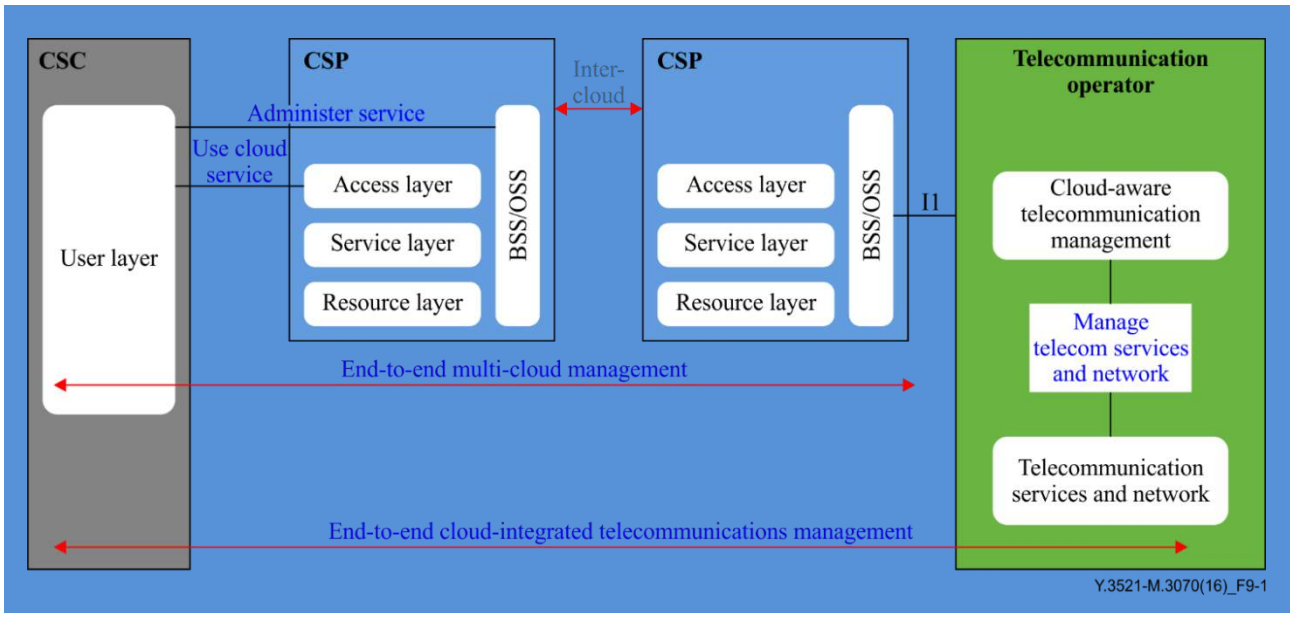


Figure 9-1 – Common model for E2E cloud computing management

Figure 9-1 is based on service and resource management chains including the CSC, one or more CSPs, and a telecommunication operator. The squared boxes with a black outline represent different parties involved in the common model for E2E cloud computing management.

The term "inter-cloud" is used in accordance with [ITU-T Y.3511] and covers the integration of cloud services from two or more CSPs.

The term "multi-cloud", as used in this Recommendation, includes holistic E2E management of one or more cloud service providers providing a given cloud service (see [ITU-T Y.3502], [ITU-T Y.3520], [ITU-T X.1601]).

The term "cloud-aware" is used here to describe the requirement of telecommunication management that are able to manage cloud-based facilities. This ability could be realized through the use of management interface "I1" which provides necessary information from the CSP's BSS/OSS to the cloud-aware telecommunication management system. The management interface "I1" can correspond to a set of SMIs as described in this Recommendation.

Note that the telecommunication operator may also act as a cloud service provider, see Figure 9-2.

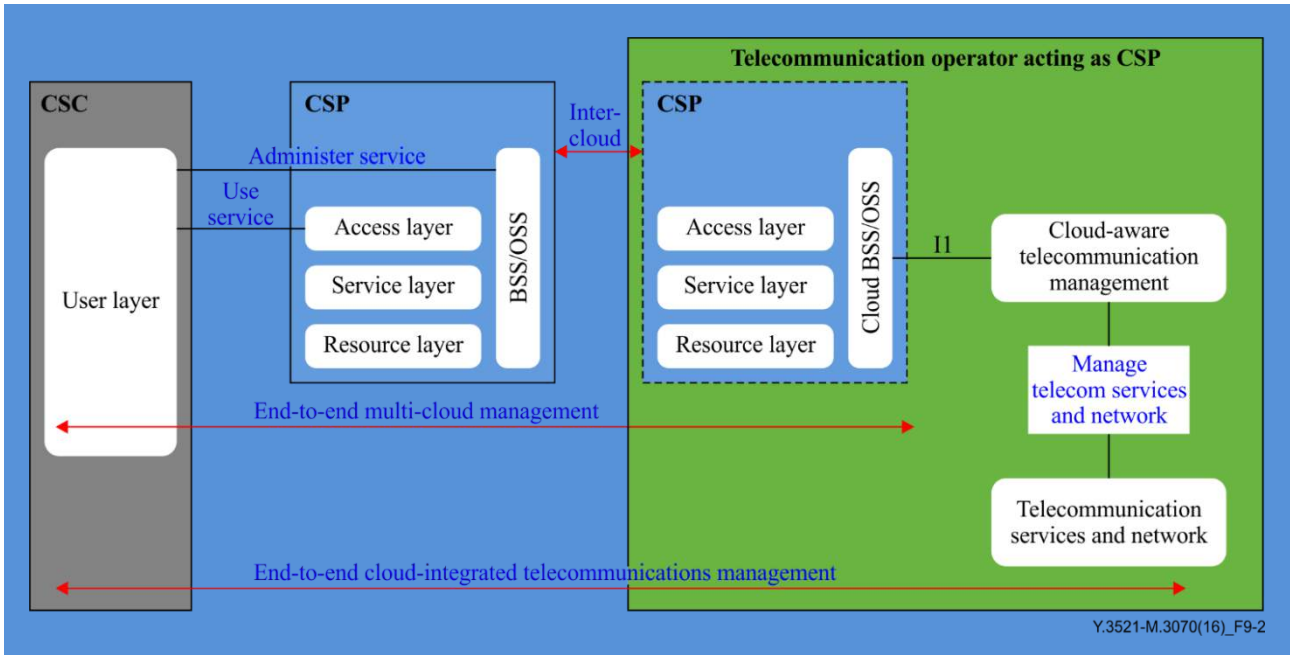


Figure 9-2 – Common model for E2E cloud computing management, with telecommunication operator acting as a CSP

In this case, the "I1" interface resides within the telecommunication operator.

The common model for E2E cloud computing management does not imply any particular arrangement of inter-cloud connectivity. For example, the telecommunication operator acting as a CSP could be acting as an intermediary CSP between the CSC and other cloud services, or in any other inter-cloud role described in [ITU-T Y.3511]. The management architecture is unaffected by this.

10 Cloud computing management functionalities

This clause identifies functionalities for cloud computing management. The high-level organization of cloud computing management functionalities presented in Figure 10-1 is based on the management layering described in clause 8.1 covering customer management, product management, service management, and resource management.

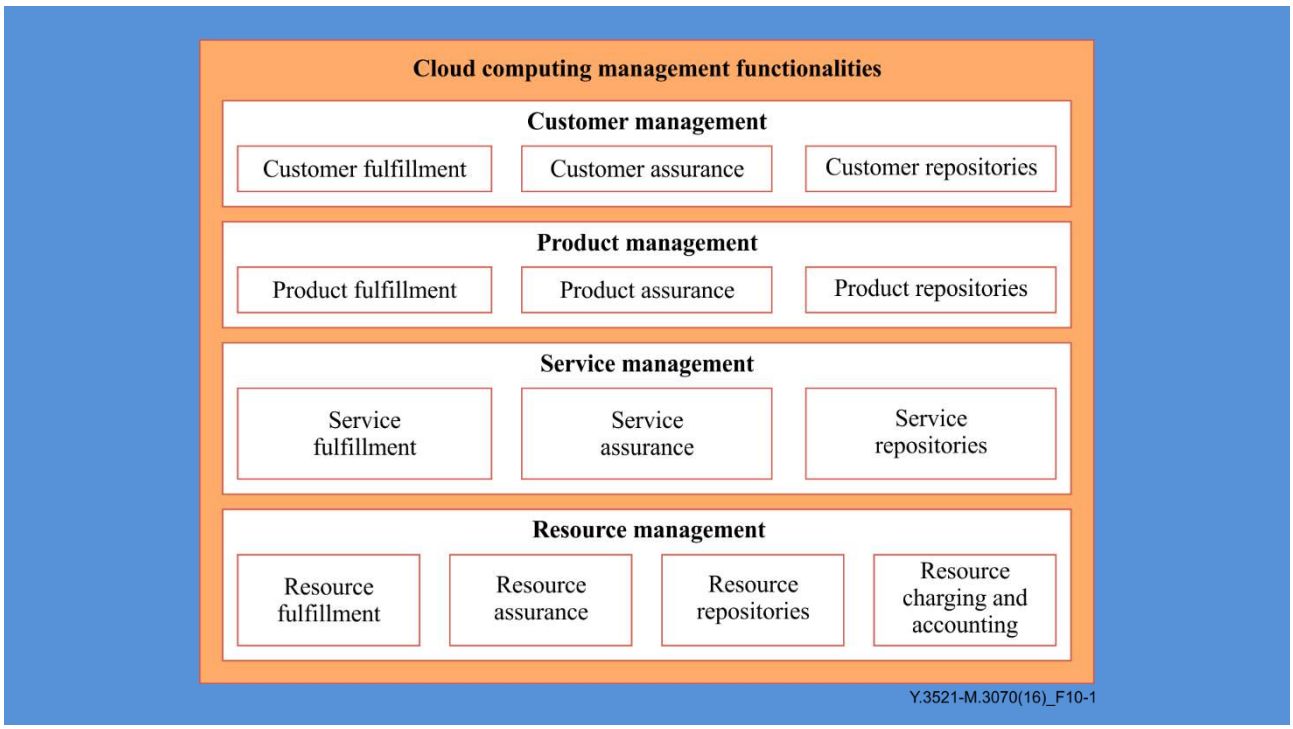


Figure 10-1 – The high-level organization of cloud computing management functionalities

10.1 Functionalities for cloud customer management

This clause identifies cloud customer management functionalities including customer fulfilment, customer assurance and customer repositories functionalities. The detailed functionalities for cloud customer management are presented in Figure 10-2.

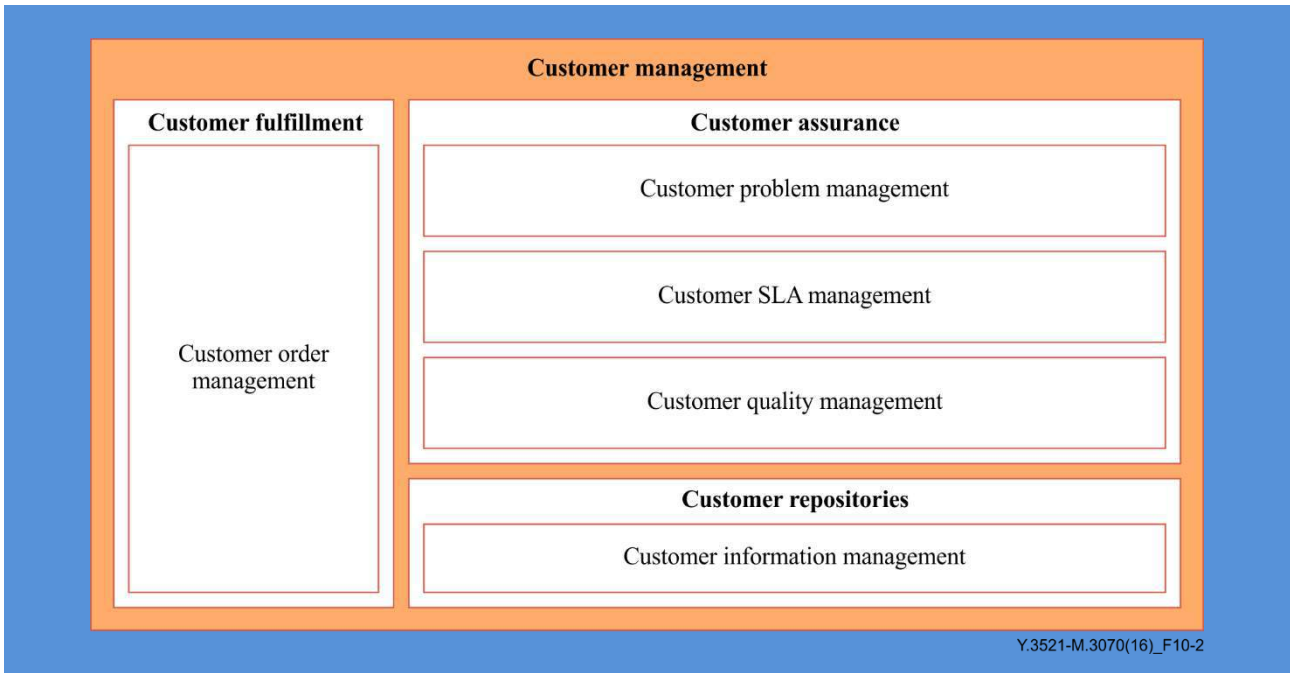


Figure 10-2 – Functionalities related to cloud customer management

10.1.1 Customer fulfilment functionalities

This covers a set of functionalities for the fulfilment management of cloud service customers. These functionalities include customer order management.

10.1.1.1 Customer order management

Customer order management is responsible for the E2E lifecycle management of a customer request for products. This includes customer order establishment (step guiding, data collection and validation), customer order publication as well as customer order orchestration and overall customer order lifecycle management.

Customer order management functionalities include the following:

1) customer order establishment. This functionality is responsible for the acquisition of a customer order for products;
2) customer order distribution. This functionality decomposes the customer order into product order requests (e.g., bundle decomposition);
3) customer order publication. This functionality issues valid and complete customer orders, and stores the order into an appropriate inventory;
4) customer order tracking and management. This provides the functionality necessary to track and manage the distributed requests decomposed by customer order distribution;
5) customer order orchestration. This functionality provides workflow and orchestration capability across customer order management;
6) customer order lifecycle management. This provides the functionality necessary to track and manage a customer order from establishment to cancellation.

10.1.2 Customer assurance functionalities

This covers a set of functionalities for the assurance management of cloud customers. These functionalities include customer problem management, customer SLA management and customer quality management.

10.1.2.1 Customer problem management

This set of functionalities is responsible for managing problems reported by customers, resolving these problems to the customer's satisfaction, and providing meaningful status on the issues, as needed, to the customer. These functionalities include customer problem reception and validation, customer problem lifecycle management, customer problem diagnostics, customer problem resolution and customer problem reporting.

10.1.2.2 Customer SLA management

Customer SLA management includes the required functionalities to assure that cloud SLAs made between CSCs and CSPs are met. This includes processing measurements made elsewhere and checking the measurements and taking appropriate actions when the specified agreements are not met. These functionalities include customer SLA issue reception, customer SLA analysis, and customer SLA reporting.

10.1.2.3 Customer quality management

Customer quality management enables CSPs to leverage customer insight gained from CSC transactions, interactions and activities with the CSP to treat the CSC in a personalized manner and provide a unique customer experience. These functionalities include customer profiling (e.g., customer profile inquiries, customer behaviour tracking, prediction), customer experience monitoring, customer satisfaction validation and customer operational decision making.

10.1.3 Customer repositories functionalities

This set includes functionalities for customer information management.

10.1.3.1 Customer information management

Customer information management ensures the management of a consistent, accurate and complete CSP view of customers. This includes functionalities for customer subscription management, customer profile management (e.g., managing customer preferences and customer details) and customer interaction collection and storage.

10.2 Functionalities for cloud product management

This clause identifies cloud product management functionalities including product fulfilment, product assurance and product repository functionalities. The detailed functionalities for cloud product management are presented in Figure 10-3.

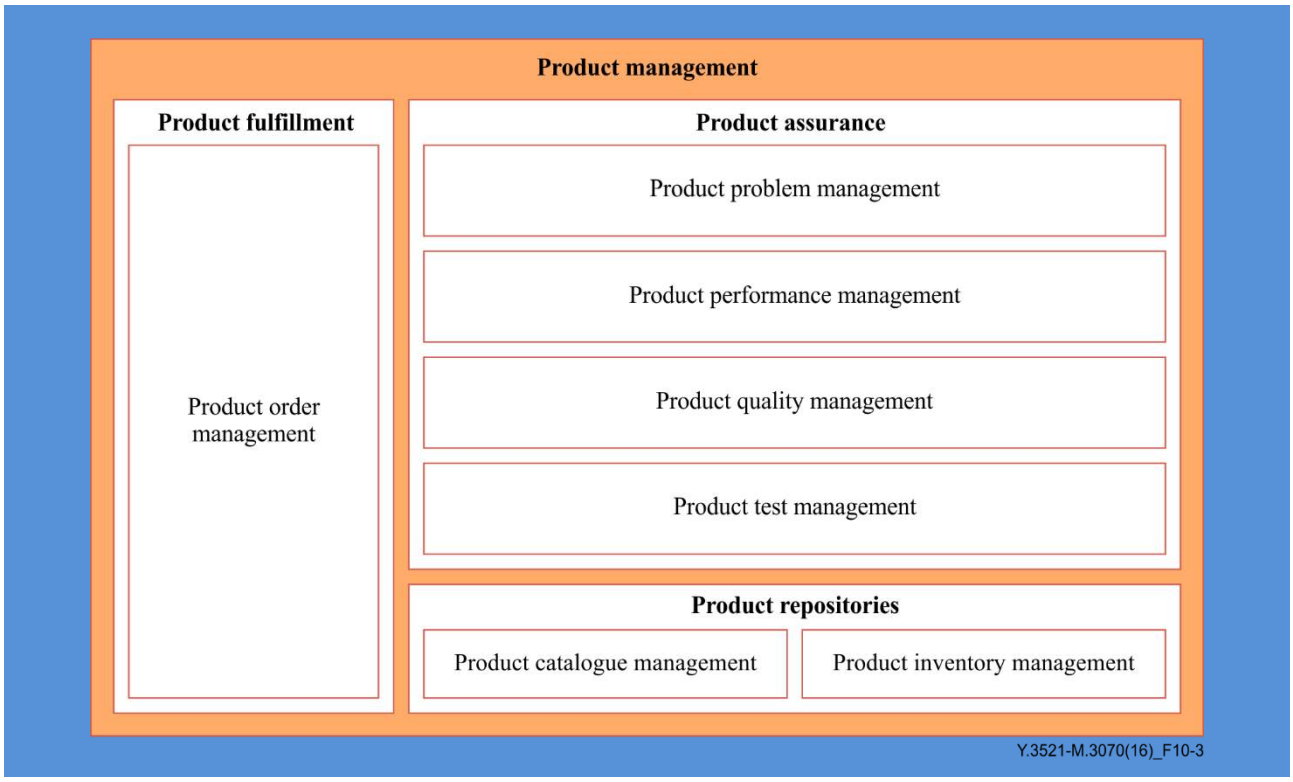


Figure 10-3 – Functionalities related to cloud product management

10.2.1 Product fulfilment functionalities

This covers a set of functionalities for the fulfilment management of cloud products. These functionalities include product order management.

10.2.1.1 Product order management

Product order management is responsible for the E2E lifecycle management of a product orders.

Product order management functionalities include the following:

1) product order establishment. This functionality is responsible for the acquisition of a product order request;
2) product order distribution. This functionality decomposes the product order into service order requests and then distributes each service order request to appropriate service order management functionalities;
3) product order publication. This functionality issues valid and complete product orders, and stores the order into an appropriate inventory;
4) product order tracking and management. This provides the functionality necessary to track and manage the distributed requests decomposed by product order distribution;
5) product order orchestration. This functionality provides workflow and orchestration capability across product order management.

10.2.2 Product assurance functionalities

This covers a set of functionalities for the assurance management of cloud products.

10.2.2.1 Product problem management

This set of functionalities is responsible for handling product-affecting CSC problems as well as CSP services problems. These functionalities analyse and resolve product problems in an efficient manner, tracking these problems and reporting them.

10.2.2.2 Product performance management

Product performance management includes the activities and tools that gather and analyse data regarding the efficiency of the product strategy, propositions and products based upon their performance in the marketplace.

This set of functionalities is responsible for monitoring, analysing and reporting on product performance. This includes the following functionalities:

1) performance monitoring. This functionality collects and monitors product performance data based upon parameters;
2) performance analysis. This functionality is responsible for the analysis and evaluation of products' performance (analysing data received from product performance monitoring). Examples of performance analysis include tracking the performance of a product based on its performance in the marketplace with regard to campaigns or product capacity analysis;
3) performance reporting. This functionality creates product performance reports (such as product revenue reporting or cost reporting) on a periodic basis or on-demand.

10.2.2.3 Product quality management

This set of functionalities is responsible for monitoring and managing the quality of products. They allow collect and compare quality related measurements against established products.

This includes the following functionalities:

1) product quality modelling. This functionality establishes what will be monitored and how it will be monitored in terms of product quality;
2) product quality monitoring. This functionality collects and monitors product quality as determined by the established product quality model;
3) product quality analysing. This functionality analyses and evaluates the quality of products being offered by the CSP;
4) product quality reporting. This functionality generates various reports on product quality and makes them available on a periodic basis or on-demand.

10.2.2.4 Product test management

This set of functionalities allows a CSP to test the quality of products. These functionalities collect and compare quality and performance related indicators. The results can be optionally available to interested parties.

10.2.3 Product repositories functionalities

This set includes functionalities for product catalogue management and product inventory management. The role of particular functionalities is described hereafter.

10.2.3.1 Product catalogue management

This set of functionalities allows the CSP to list and manage available products and their associated characteristics such as: product offering characteristics, product offering effective duration, product offering description.

10.2.3.2 Product inventory management

This set of functionalities allows the CSP to maintain information about already deployed and provided cloud products. It may also store and manage service relationships: the mapping to other services and/or service components.

10.3 Functionalities for cloud service management

This clause identifies cloud service management functionalities including service fulfilment, service assurance and service repository functionalities. The detailed functionalities for service management are presented in Figure 10-4.

NOTE – "Service order management" corresponds to the process of taking, organizing, tracking and satisfying CSC requests for cloud services provided by a CSP.

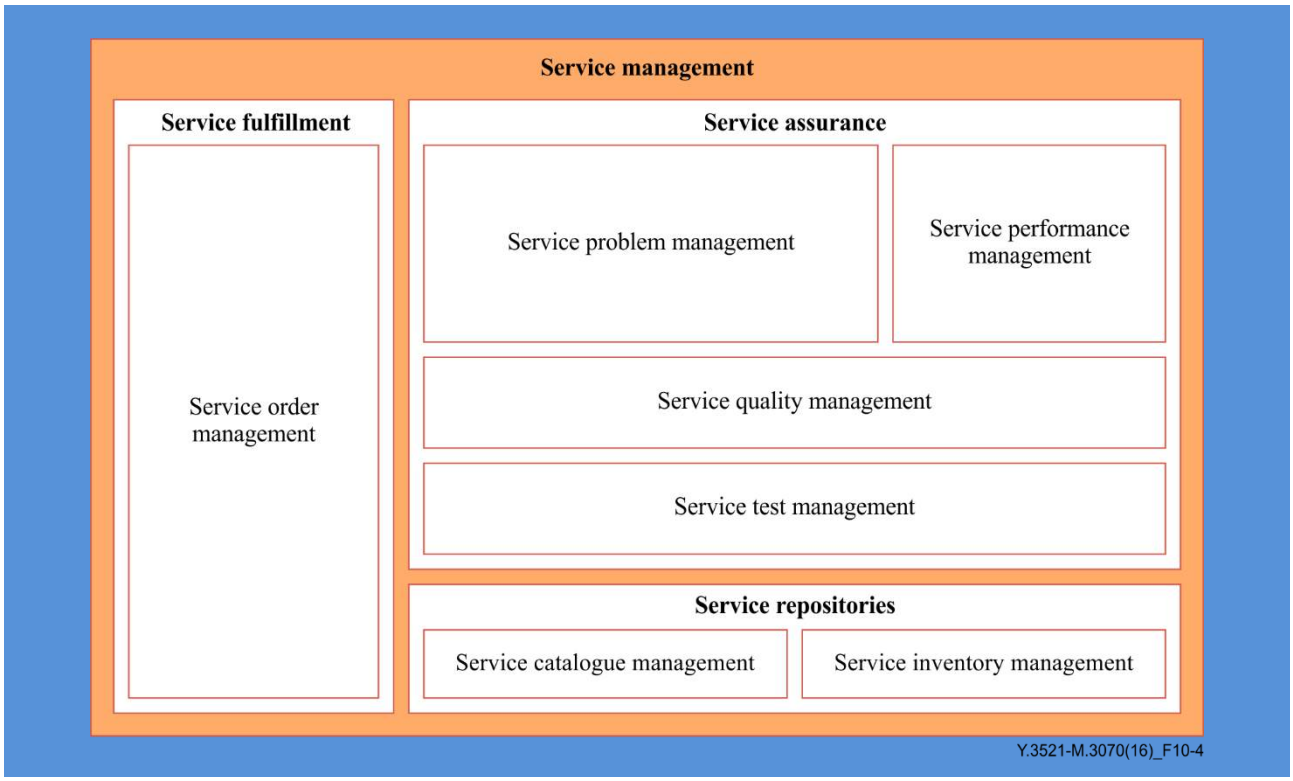


Figure 10-4 – Functionalities related to cloud service management

10.3.1 Service fulfilment functionalities

This covers a set of functionalities for the fulfilment of cloud services. These functionalities include service order management**.**

10.3.1.1 Service order management

Service order management provides a set of functionalities for the management of cloud services considering CSC requirements (e.g., cloud SLA). This set includes the following functionalities:

1) service order orchestration and distribution. This functionality provides for orchestration across service order management. It decomposes a cloud service order into resource order requests, and then distributes each request to provision the service order. It also provides the functionality necessary to track and manage these distributed requests, e.g., tracks the various resource orders until completed, sequences resource order provisioning if required, provides status on the overall service order;
2) service assign. This functionality determines the availability of facilities required to support a service;
3) service order tracking and lifecycle management. This functionality issues valid and complete service orders, and stores the service order into an appropriate repository;
4) service order establishment. This functionality establishes a complete and valid service order. It validates the cloud service order request according to the service catalogue and installed base, and to provisioning rules. It also validates that the cloud service specified on the service order is available and feasible from the CSP platform/infrastructure point of view;

5) service activation. This functionality is responsible for the activation of a cloud service based on the specific service configuration.

10.3.2 Service assurance functionalities

This covers a set of functionalities for the assurance management of cloud services. These functionalities include service problem management, service performance management, service quality management and service test management.

10.3.2.1 Service problem management

This set of functionalities is responsible for receiving service affecting CSC problems as well as CSP infrastructure faults. These functionalities analyse and resolve service problems in an efficient manner, tracking these problems and reporting them. This includes:

1) service problem reception. This functionality receives problems that are perceived to be service affecting;
2) service problem monitoring. This functionality monitors the operational status of cloud services;
3) service problem analysis. This functionality diagnoses service problems. It correlates CSC problems with resource faults, and prioritize service problems appropriately;
4) service problem correction and resolution This functionality resolves the service problem back to a normal operational state as efficiently as possible;
5) service problem tracking and management. This functionality assures that service problems are assigned, coordinated, and restored efficiently, escalating as needed;
6) service problem reporting. This functionality reports the status of service problems. This includes operational reports, management reports, reports against various metrics, as well as information needed by other related management and operations functionalities.

10.3.2.2 Service performance management

This set of functionalities is responsible for monitoring, analysing and reporting on the E2E service performance. This includes the following functionalities:

1) performance monitoring. This functionality collects and monitors service performance parameters;
2) performance analysing. This functionality is responsible for the analysis and evaluation of services' performance (analysing data received from service performance monitoring, determining the causes of changes, providing operations for adapting the performance);
3) performance reporting. This functionality creates service performance reports on a periodic basis or on-demand.

10.3.2.3 Service quality management

This set of functionalities is responsible for monitoring and managing the E2E quality of services. They allow, collect and compare quality related measurements against established services. The results can be optionally available to interested parties. This includes the following functionalities:

1) service quality modelling. This functionality establishes what will be monitored and how it will be monitored in terms of service quality. This includes the definition of the service quality model and its dependencies as establishment of key quality indicators (KQIs) and service level objectives (SLOs), accepting input from CSC contracts or service definitions, establishment of data sources for monitoring;
2) service quality monitoring. This functionality collects and monitors service quality as determined by the established service quality model;
3) service quality analysing. This functionality analyses and evaluates the quality of services being delivered by the CSP;
4) service quality reporting. This functionality generates various reports on service quality and makes them available on a periodic basis or on-demand.

10.3.2.4 Service test management

This set of functionalities allows a CSP to test the quality of services. They allow collect and compare quality and performance related indicators. The results can be optionally available to interested parties. This includes the following functionalities:

1) service test strategy and policy management. This functionality manages the rules that define the strategies for conducting various service tests;
2) service test lifecycle management. This functionality manages the E2E lifecycle of a service test;
3) service test command and control. This functionality provides access, commands, and controls the service testing environment;
4) service test services. This functionality provides the means to access the testing capabilities.

10.3.3 Service repositories functionalities

This set includes functionalities for service catalogue management and service inventory management.

The role of particular functionalities is described below.

10.3.3.1 Service catalogue management

This set of functionalities allows the CSP to list and manage available services.

10.3.3.2 Service inventory management

This set of functionalities allows the CSP to maintain information about already deployed and provided cloud services. It may also store and manage service relationships: the mapping to other services and/or service components as well as the mapping to resources used to implement a particular service.

10.4 Functionalities for cloud computing resource management

This clause identifies functionalities related to resource management for the support of cloud services. These include resource fulfilment, resource assurance, resource charging and accounting and resource repositories functionalities. These functionalities related to resource management are presented in Figure 10-5.

NOTE – "Resource order management" corresponds to the process of taking, organizing, tracking and satisfying resource requests for the support of cloud services provided by a CSP.

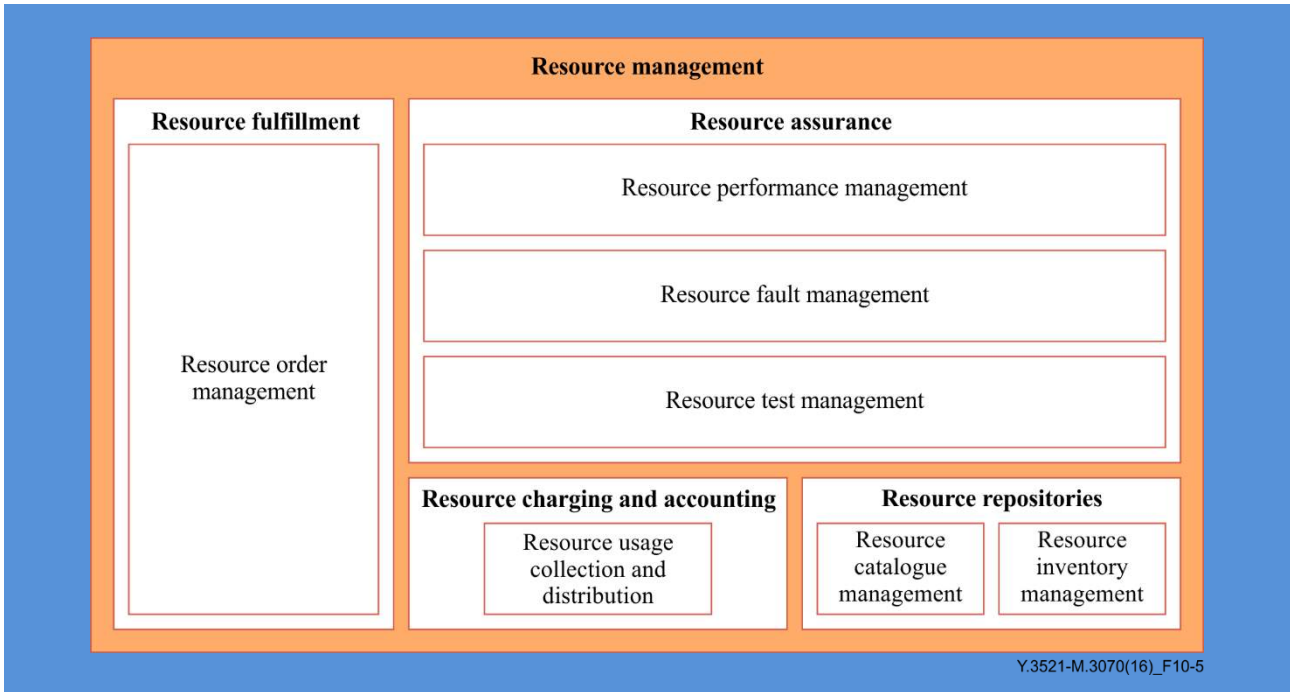


Figure 10-5 – Functionalities related to cloud computing resource management

10.4.1 Resource fulfilment functionalities

This covers a set of functionalities for the fulfilment management of resources for the support of cloud services. This functionality includes resource order management.

10.4.1.1 Resource order management

This set of functionalities manages the E2E lifecycle of a resource order request. This includes validating resource availability as well as the resource order request.

NOTE – Resource order management functionality will typically communicate with service order management and resource layer functionalities. Notifications can be issued to the service order management functionalities during the resource order orchestration process (especially upon completion). Such notification can trigger other steps in the service order management functionalities (e.g., resource order completion).

Resource order management functionalities include:

1) resource order orchestration and distribution. This functionality provides workflow and orchestration capability across resource order management. This functionality has the ability to distribute the resource order. It also provides functionality to track and manage the overall resource order as well as to track the overall order;
2) resource order validation. This functionality validates the resource order request based on contract, catalogue, and provisioning rules;
3) resource order tracking and lifecycle management. This functionality issues valid and complete resource orders, and stores the order into an appropriate repository;
4) resource assign. This functionality addresses resource configurations which are needed to support a service order.

10.4.2 Resource assurance functionalities

This set of functionalities covers the assurance management of resources in support of cloud services. These functionalities include resource performance management, resource fault management and resource test management. The role of particular functionalities is described below.

10.4.2.1 Resource performance management

This set of functionalities monitors, analyses, and reports on the performance of the CSP resources. This includes the following functionalities:

1) resource performance monitoring. This functionality supports data collection and performance monitoring of the CSP resources;
2) resource performance analysing. This functionality analyses the performance of the various CSP resources;
3) resource performance management reporting. This functionality generates reports about the performance of the CSP resources.

10.4.2.2 Resource fault management

This set of functionalities is responsible for the management of faults associated with the resources of CSP.

This includes the following functionalities:

1) resource fault monitoring. This functionality collects and monitors the operational status of the resource layer;
2) resource fault analysis. This functionality relates and analyses the various fault events in the resource layer;
3) resource fault correction and restoration. This functionality is responsible for repairing or replacement of faulty resources;
4) resource fault reporting. This functionality provides reports about the various faults within the resource layer.

10.4.2.3 Resource test management

This set of functionalities is focused on ensuring that the various resources are working properly.

This includes the following functionalities:

1) resource test strategy and policy management. This functionality manages the rules that define the strategies for conducting various resource tests;
2) resource test lifecycle management. This functionality manages the E2E lifecycle of a test of a resource;
3) resource test command and control. This functionality provides access, commands, and controls the resource testing environment;
4) resource test services. This functionality provides the means to access the testing capabilities.

10.4.3 Resource charging and accounting functionalities

This set of functionalities covers resource usage management of the services. This includes resource usage collection and distribution.

10.4.3.1 Resource usage collection and distribution

This set of functionalities is used to channel usage events from the resources to various processes such as billing, legal compliance, and service assurance. Usage event records are collected, processed, edited, correlated, enriched, formatted and distributed to upstream functionalities.

10.4.4 Resource repositories functionalities

This covers a set of functionalities for the resource repositories of the services. These functionalities include resource catalogue management and resource inventory management.

10.4.4.1 Resource catalogue management

This set of functionalities determines repositories of resource listing within the CSP and include the ability to design, create, augment and map new entities and supporting data.

10.4.4.2 Resource inventory management

This set of functionalities manages information of all CSP resources available for the implementation of services and products.

11 Security considerations

Security aspects for consideration within the cloud computing environment, including inter-cloud computing, are addressed by security challenges for the CSPs as described in [ITU-T X.1601]. [ITU-T X.1601] analyses security threats and challenges, and describes security capabilities that could mitigate these threats and meet the security challenges.

Annex A

Use of SMI-based model across various cloud architecture layers

(This annex forms an integral part of this Recommendation.)

This annex describes SMI-based models that can be used across various cloud computing architecture layers.

The following figure provides an example of mapping the E2E SMI concept onto the cloud computing reference architecture [ITU-T Y.3502].

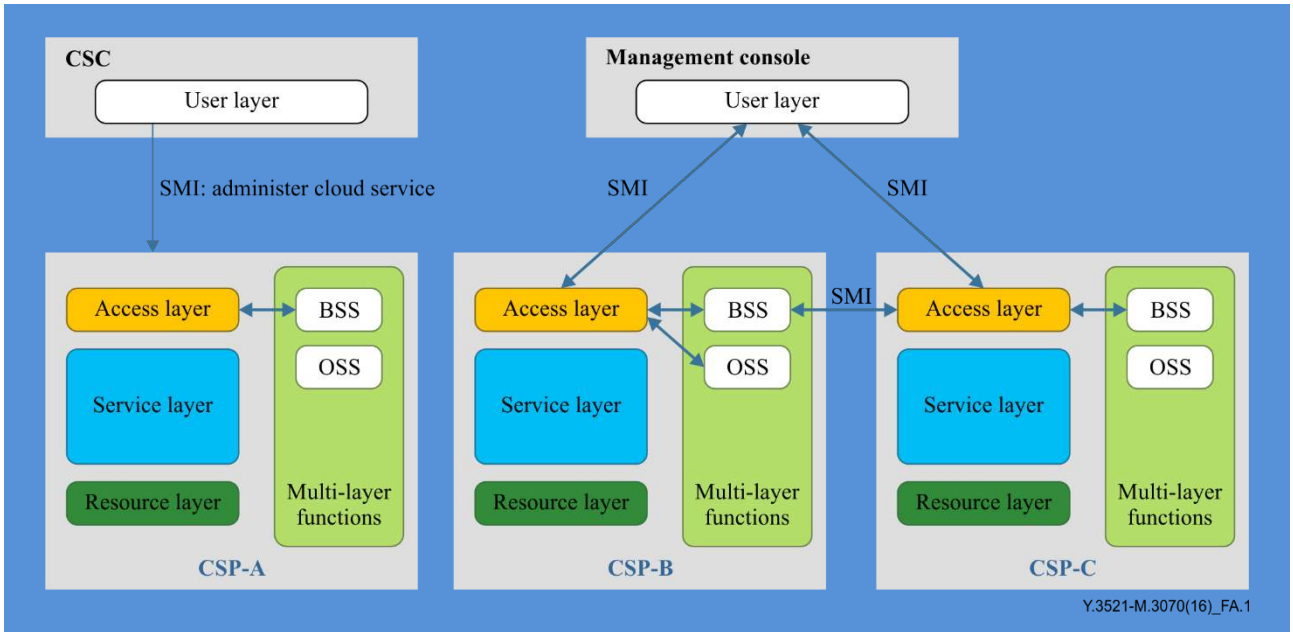


Figure A.1 – Example mapping of SMI to cloud computing reference architecture

In Figure A.1, a number of example SMIs are identified.

Firstly, an enterprise CSC's management interface into a cloud service, documented in [ITU-T Y.3502] as "administer cloud service", is implemented as an SMI. The interface is routed via the access layer for connectivity and access control purposes.

Secondly, as shown in [ITU-T Y.3520] to support inter-cloud scenarios [ITU-T Y.3511], it is possible for one CSP to act as the CSC of another, and as such it can employ the same type of SMI as in the first case. This is illustrated above in the SMIs between the BSS of CSP-B (acting as a CSU) and the access layer of CSP-C. This can then be cascaded through additional CSPs if desirable.

Thirdly, an operator's management console may employ multiple SMIs to different services and providers. In reference architecture terms, such a console is also acting as a CSC, although a very specialised one.

Thus the same SMI concept [ITU-T Y.3520] is being used in every case.

Appendix I

Illustration on E2E cloud computing management in practice

(This appendix does not form an integral part of this Recommendation.)

I.1 Introduction

This appendix provides an illustration of how a cloud computing management system can function in practice, following the conceptual view and common model described in clauses 8 and 9.

I.2 Vertical vs horizontal management

This Recommendation describes both vertical relationships within a BSS/OSS, as shown in Figure 8-1, as well as horizontal relationships between CSPs within each managed layer, as shown in clause 9.

Both vertical and horizontal interfaces are implemented as SMIs, however those vertical interfaces between management layers within a single CSP's system are likely to be implementation-specific.

I.3 Orchestrated management actions

For realising E2E cloud computing management, orchestration is required at multiple levels. In each case, this comprises the creation or management of multiple managed objects as a means to implement a higher layer construct. While orchestration can occur directly in the service layer (for example, the creation of a virtual machine (VM) within an infrastructure as a service (IaaS) service may automatically cause the creation of associated storage objects required to support the VM), this can also occur at higher layers of the management system. The following example (see clause I.5) is an illustration of such a case.

I.4 Monitoring and diagnostics

SMI interfaces can also be used for monitoring and diagnostics within a single cloud computing system and this can then be extended into a multi-cloud scenario (as described in [ITU-T Y.3520]). This allows for aggregated performance measurement, reporting, fault detection, and root cause analysis across multiple cloud services.

I.5 Example of E2E cloud computing management

For this example, consider the creation of a video streaming service, designed to deliver training content to a number of enterprise customers.

A cloud service provider is offering a product "video streaming platform" to its customers. This product provides:

1) a storage platform (library) for holding video content, including content management, cataloguing, metadata management;
2) a video-ingestion service, where content in various video formats can be uploaded for transcoding before being placed in the library;
3) a subscription management system, including digital rights management, subscription, payment, authorization, and billing;
4) service usage monitoring, including statistics, trends, and user behaviour;
5) managed network connectivity, both for uploading content to the cloud, and for efficient streaming of the content through a content delivery network and thus to end users.

The enterprise wishing to buy this bundle of services needs only to place a single product order, which will include various choices for capacity, throughput, etc.

Figure I.1 illustrates E2E cloud computing management in practice.

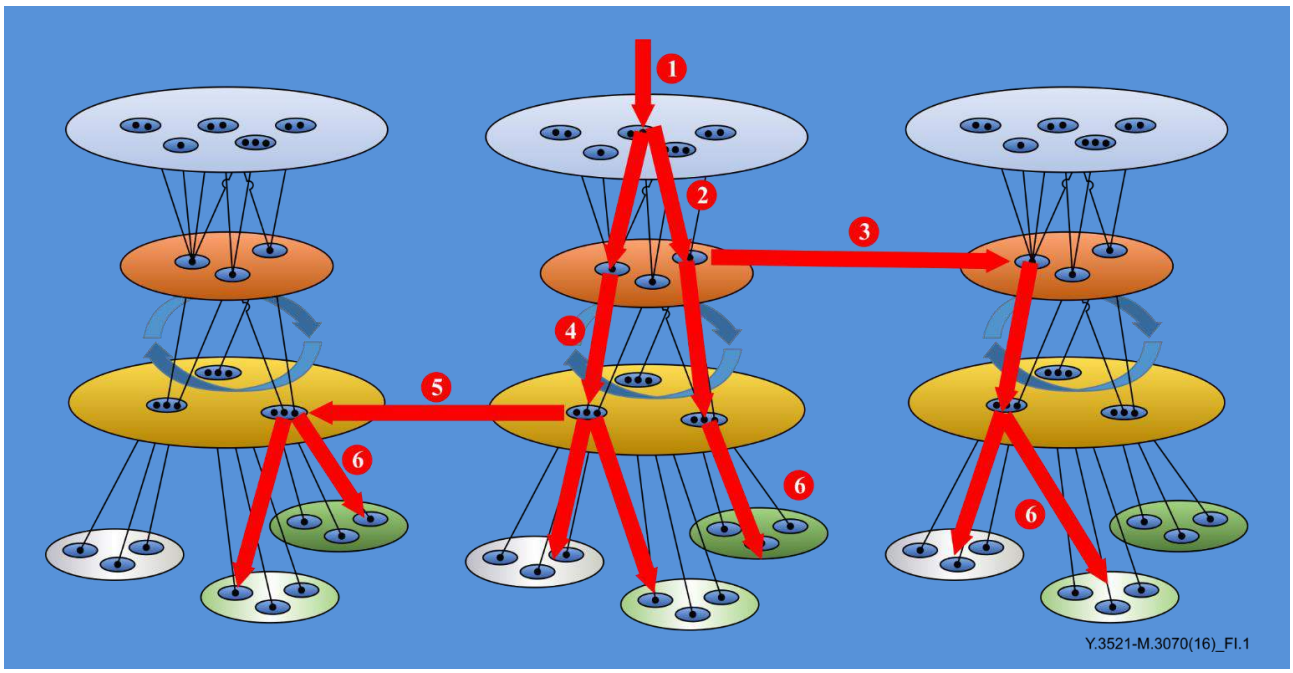


Figure I.1 – Example of E2E cloud computing management in practice

NOTE – This figure is based on the comprehensive view of cloud computing management. See clause 8.

The stages shown in Figure I.1 are as follows:

1) the CSC places the order for the entire package;

2) customer management assesses the validity of the order, determines the appropriate SLA to apply to the overall package, and invokes the individual product objects in the product management layer. There are two of these, a network product and a cloud service product;

3) the network product management creates a network as a service (NaaS) within the CSP service layer, identifying endpoint and network characteristics needed for the overall service. It also requests the creation of a NaaS service from another CSP which includes wide-area telecommunications connectivity. This is done by making SMI-based requests to instantiate the NaaS service at the other CSP. The internal and external NaaS instances are then interconnected with agreed endpoints and SLAs suitable to meet the overall objective;

4) the video cloud product orchestrates a set of cloud services including video processing, storage, content management, a software as a service (SaaS) for the billing and subscription, etc;

5) because the video processing service does not have the capability to directly handle some of the video formats the customer has requested, the video processing service requests this capability as a specialist platform as a service (PaaS) from a third CSP. The PaaS is provided with the code necessary to work with the content platform;

6) each of the invoked services is responsible for creating and managing the underlying cloud computing resources, including compute, storage, and networking. Each of them is also responsible for monitoring the functions of those resources, and reporting usage, performance, faults and SLA breaches up to their "parent" management layer for aggregation and analysis.

In this way, a very large and complex cloud-based solution is requested, instantiated, and managed as a whole, both for business and operational purposes. Within each CSP, the logic of orchestration is a key point of differentiation, but the individual management interfaces follow the general SMI approach, making for a relatively straightforward management architecture.

Bibliography

[b-ITU-T M.60] Recommendation ITU-T M.60 (1993), *Maintenance terminology and definitions*.

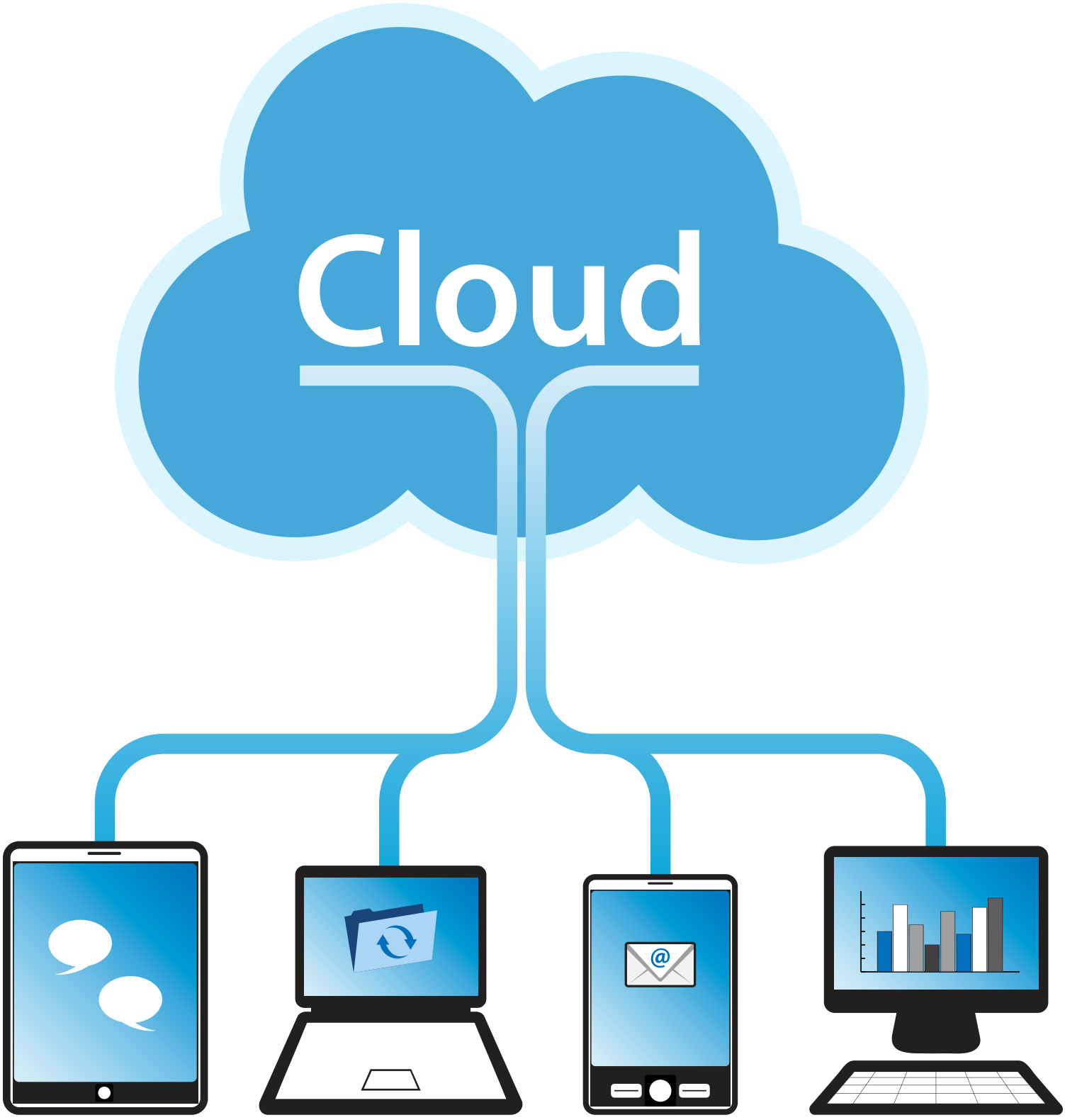
[b-ITU-T M.3010] Recommendation ITU-T M.3010 (2000), *Principles for a telecommunications management network*.

[b-ITU-T M.3050.0] Recommendation ITU-T M.3050.0 (2007), *Enhanced Telecom Operations Map (eTOM) – Introduction*.

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014), *Information technology – Cloud computing – Overview and vocabulary*.

[b-ITU-T Y.3501] Recommendation ITU-T Y.3501 (2013), *Cloud computing framework and high-level requirements*.

[b-TMF TR198] TM Forum TR198, *Multi-Cloud Service Management Pack – Simple Management API (SMI) Developer Primer and Code Pack, V2.2*. <https://www.tmforum.org/?s=TR198>


Cloud

Cloud-based network management functional architecture

Recommendation ITU-T M.3071

(01/2018)

SERIES M: TELECOMMUNICATION MANAGEMENT, INCLUDING TMN AND NETWORK MAINTENANCE

Summary

This Recommendation introduced a new network management functional architecture with the cloud computing technology. In this Recommendation, the background and basic concept of cloud-based network management are provided. This Recommendation also provides the cloud-based network management functional architecture, including the basic components of the cloud-based network management functional architecture, their functionalities and the relationship between the components.

Table of Contents

1 Scope

This Recommendation provides the concept of cloud-based network management functional architecture and its fundamental components.

This Recommendation describes the composition of a cloud-based network management functional architecture, explains the functions of each components in the architecture, and also introduces the relationship among the components.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T M.3010] Recommendation ITU-T M.3010 (02/2000), *Principles for a telecommunications management network*.

[ITU-T Y.3521/M.3070] Recommendation ITU-T Y.3521/M.3070 (03/2016), *Overview of end to end cloud computing management*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 network element [ITU-T M.3010]: An architectural concept that represents telecommunication equipment (or groups/parts of telecommunication equipment) and supports equipments or any item or groups of items considered belonging to the telecommunications environment that performs network element functions (NEFs).

3.1.2 management service [ITU-T M.3010]: A management service is an offering fulfilling specific telecommunications management needs.

3.2 Terms defined in this Recommendation

This Recommendation defines the following new terms.

3.2.1 cloud-based network management

Cloud-based network management is to perform network management functions using cloud computing technology, and it can also be used to manage both traditional telecommunication networks and/or cloud computing infrastructures.

3.2.2 management service analysis function

Management service analysis function provides the ability of analyzing each management service in network management. Each management service is registered in this analyzer function, and all the related information about this service is analyzed and stored for future use.

3.2.3 management service composing function

Management service composing function provides the ability of composing several small management functions into a new complex management service, so that they can easily provide a new type of management functionality without having to change the implementation of the component management functions.

3.2.4 management service deployment function

Management service deployment function provides the ability of deploying required services for a management task. Each management task may need the support of multiple management services, and for those services which are not ready for use will appropriately be deployed into some virtualized resources on the cloud infrastructure.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

IT Internet Technology

FS Function Set

NE Network Element

NEF Network Element Function

P&C Perception and Control

VM Virtual Machine

5 Conventions

None.

6 Introduction

The current network management and technologies have the weak point that when new management requirements are proposed, it is difficult to provide a new management service based on the existing services using the traditional management technology. It is also hard to compose a small system with simplified management functions on demand.

Cloud computing has become one of the mainstream technologies used in telecommunication networks as well as Internet services. Cloud computing technology has the following benefits: high usage rate of physical resources, reliable service provision, high extensibility, cost efficient, and service on demand etc. When introducing cloud computing technology into network management domain, it is easy to solve the above problems, and it will be very flexible to provide new management services.

When introducing cloud into network management, it means that different management function blocks can be placed into virtual resources, and the virtualized resources can be grouped together to form a composed management service that are more powerful to provide complex management functions. It is also capable of dealing with large amount of management data, as distributed computing can be carried out on cheap servers.

The term management services used in this Recommendation is not the cloud service provided by a network operator or a cloud operator. Management services are provided by a management system, no matter it is based on cloud or not. A cloud service is provided by a cloud service provider to end users for resource virtualization, which provides end users with the cloud computing and/or cloud storing capabilities.

A cloud-aware management system described in [ITU-T Y.3521/M.3070] is a management system which can be used to manage both traditional telecommunication networks and cloud computing infrastructures. A cloud-based management system in this Recommendation is a management system which is built using

cloud computing technology, and it can also be used to manage both traditional telecommunication networks and/or cloud computing infrastructures. A cloud-based management system can be a cloud-aware management system, but it is not necessary to manage cloud infrastructures using a cloud-based management system.

7 Cloud-based network management functional architecture

7.1 Basic concept

Cloud computing is a technology from IT domain, with the aim for a supplier to share computing and storage capabilities in the cloud to multiple customers. A system can be built using the traditional means, or using cloud computing technology to provide services to customer and using cloud as its infrastructure, as far as the services can be provided. A network management system is a software system which provides network management services to operators or telecommunication service providers. Thus using cloud technology in network management systems will also bring the benefits of cloud into the network management field.

Cloud-based network management system may include two main parts, one is the cloud-based network management platform, and the other is management applications for various network technologies which are built over the management platform.

Figure 1 shows the basic concept of the cloud-based network management platform and the management applications.

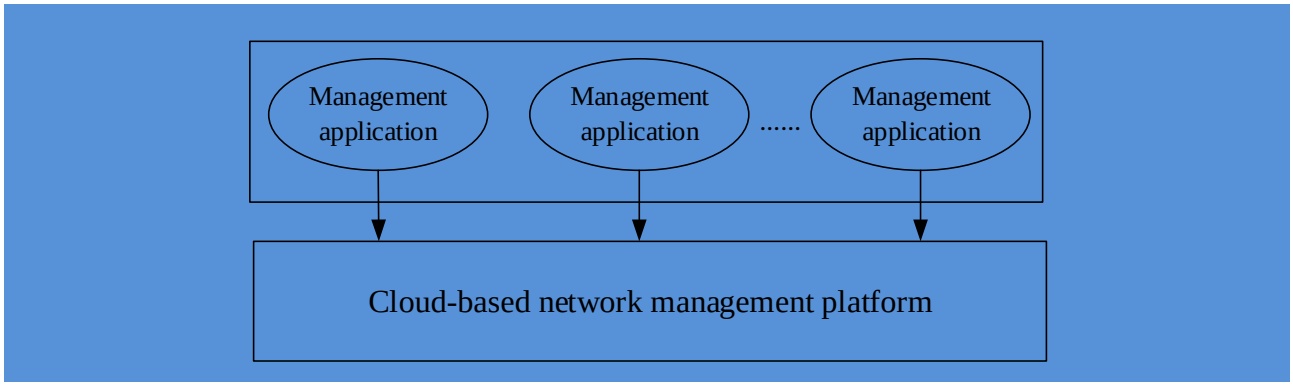


Figure 1 – Cloud-based network management platform and applications

The cloud-based network management platform is described in details in Clause 7.2. Management application functions can be the applications that provide functions dedicated for the management of a specific network technology (e.g. Mobile core network, transport network), and they provide their own functionality for its dedicated network, and share the lower layer functions of the cloud-based network management platform, e.g., cloud infrastructure management, or common management services.

7.2 Detailed structure of cloud-based network management functional architecture

7.2.1 High level layering of cloud-based network management functional architecture

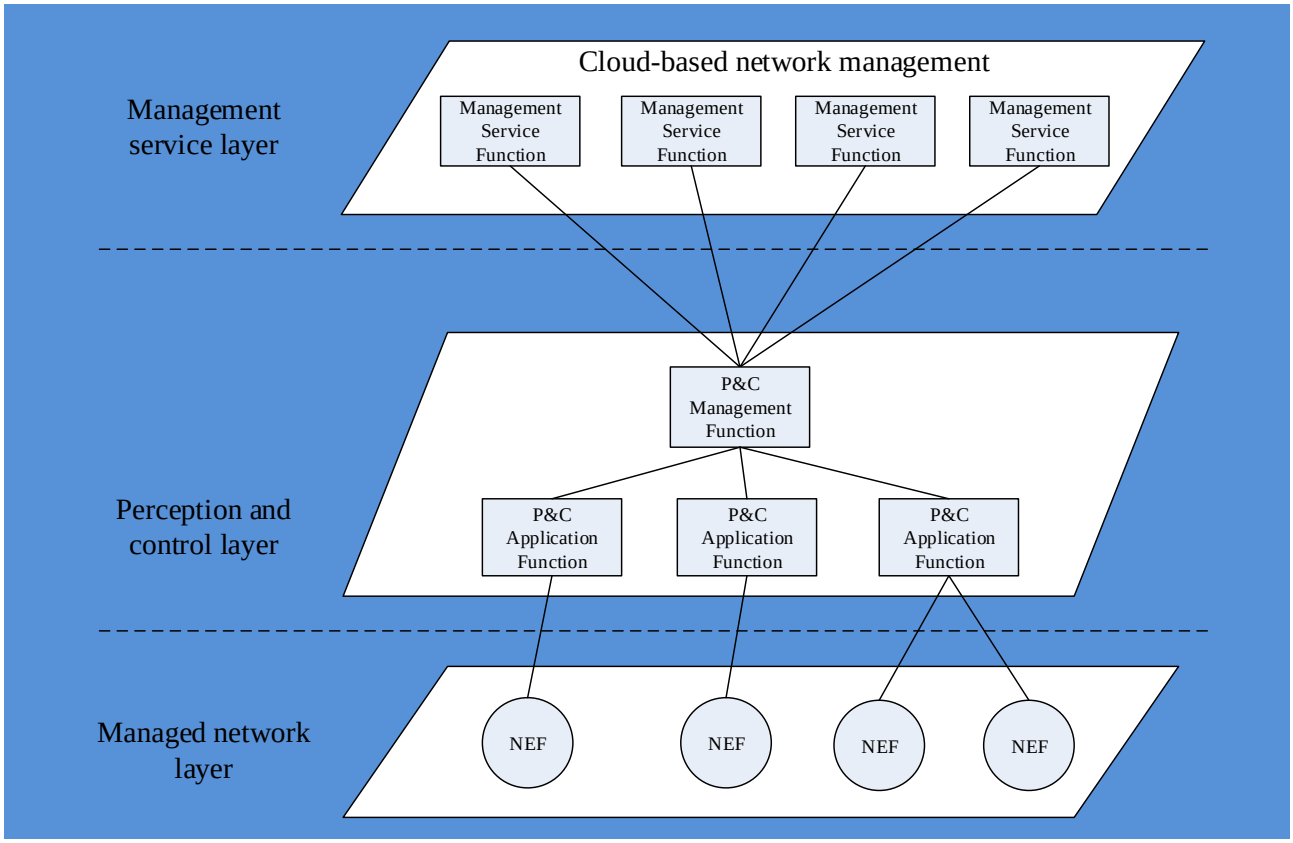


Figure 2 – High level layering of cloud-based network management functional architecture

Figure 2 shows the high level layering of cloud-based network management functional architecture, which include the following three layers:

– Managed network layer: it indicates the layer containing all the network element functions (NEFs) that are to be managed. The NEs providing the NEFs can be the traditional telecommunication network elements, or elements in a cloud infrastructure.

– Perception and control layer (P&C layer): it indicates the perception function blocks and the NE controlling function blocks. Perception function blocks have the capability to collect the configuration information, running status, or the performance data from the NEFs, and the NE controlling function blocks can be able to make necessary reconfiguration or modifications to NE parameters, through interactions with the specified NEFs.

– Management service layer: This layer mainly contains the network management function blocks, which provides management services to network operators.

7.2.2 Detailed composition of cloud-based network management functional architecture

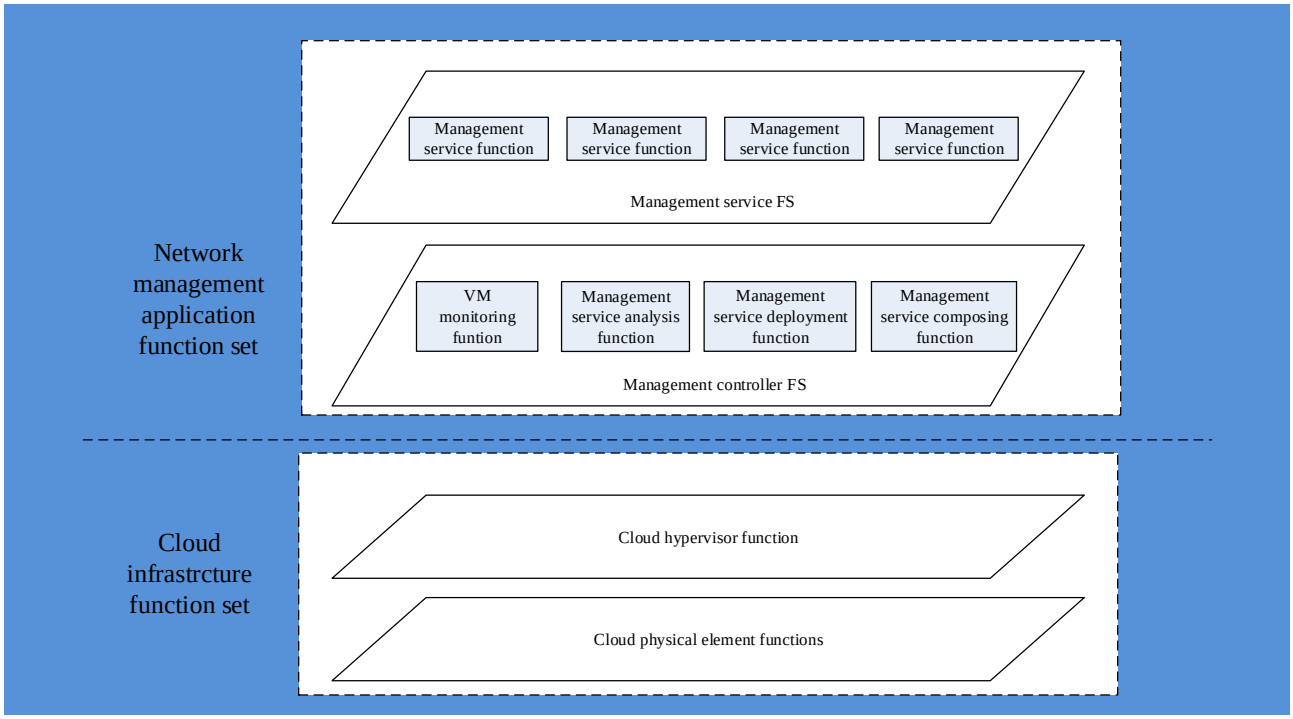


Figure 3 – Detailed composition in the management service layer

Figure 3 shows the detailed composition of cloud-based network management functional architecture, which is a refinery of the components in the management service layer as shown in Figure 2.

The cloud-based network management functional architecture is composed of the following two main parts: cloud infrastructure function set, and the network management application function set.

The cloud infrastructure function set include cloud physical element functions and a cloud hypervisor function above them. Cloud physical element functions provide the basic functions of computing and storage. Cloud hypervisor function provides the functionality to manage cloud physical elements, and provide virtualization functions above them.

The network management application function set may be further divided into two parts: management controller function set and management service function set. Management controller function set includes the basic supporting functions of the management platform, and also provide common functions to support management applications. Management service function set provides management functions, which are divided into several aspects for network management, and usually they are application specific.

7.3 The functions of each part in the architecture

In Figure 3, the functions of each component are further explained in this clause.

1) Cloud physical element function: this is the lowest level of cloud infrastructure, and it is usually composed of the functions provided by physical servers, computers, disks, network connectors and all other elements that form a physical cloud computing environment. They provide the basic computing and storage resources from the physical layer.

2) Cloud hypervisor function: it is a management layer over cloud physical element functions. Cloud hypervisor function provides the management ability of virtualized resources, for example, creating/deleting a new virtual machine (VM), start/suspend a VM, and query/change a configuration of a VM, etc. Cloud hypervisor function provides users virtualized resources using a unified interface. From the users' perspective, cloud hypervisor function can provide computing and storage capabilities dynamically, based on users' requirements.

3) Management controller function set: it contains multiple controlling functions that supports the running of the cloud-based network management platform, and each function can be implemented by a small function block. Some basic function blocks in the controllers are listed below.

- VM monitoring function: it provides the ability to monitor the performance of VMs. It monitors the dynamic information of the running status of VMs. When performance degradation is detected, the monitor informs the controller to handle the resource reassignment or service transportation.
- Management service analysis function: it provides the ability of analyzing each management services in network management. Each management service is registered in this analyzer, and all the related information about this service is analyzed and storage for future use.
- Management service deployment function: it provides the ability of deploying required services for a management task. Each management task may need the support of multiple management services, and for those services which are not ready for use will appropriately be deployed into some virtualized resources on the cloud infrastructure.
- Management service composing function: it provides the ability of composing several small management functions into a new complex management service, so that they can easily provide a new type of management functionality without having to change the implementation of the component management functions.
- More function blocks can be extended to support the running of the cloud-based network management architecture.

4) Management service function set: it provides management functions to network operators, and they are composed of all kinds of small management functions. Each network management function is performed by a service application, and those management functions can form composed services that provide more complex network management functions. Most management service applications are applications specific to a network technology, but there are still some applications which are more general to be used across different network technologies. In such cases, the common service application will be reused.

7.4 The relationship between the components in the architecture

This clause will introduce the relationship between the components in the architecture.

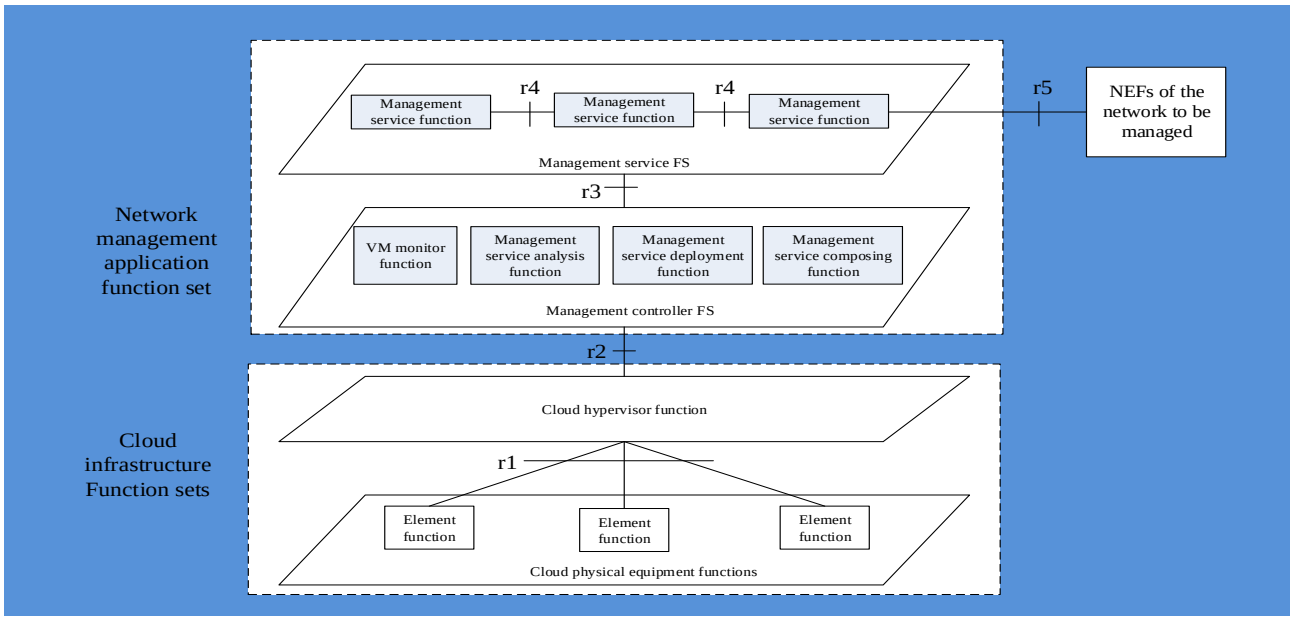


Figure 4 – Reference point between the components in the cloud-based network management functional architecture

Figure 4 shows the reference point between the components in the cloud-based network management functional architecture. All the reference points in Figure 4 are reference points as defined in [ITU-T M.3010]. In order to distinguish these references points in this Recommendation, which can show the relationship among functional components, they are numbered as r1, r2, r3 r4, and r5 respectively, as explained in Table 1.

Table 1 – Reference points in cloud-based network management functional architecture

Name	Position	Definition
r1	Between cloud hypervisor function and cloud physical element function.	Through reference point r1, a hypervisor function can connect to cloud physical element functions to perform the virtualized resource management functions. (for example, VM management, including but are not limited to creation, deletion, query, and modification of virtualized resource.) In this Recommendation, the virtualized resource will be assigned for building management system itself.
r2	Between management controller function set and cloud hypervisor function.	Through reference point r2, management controller function set can interact with cloud hypervisor function. Management controller function set sometimes may ask the cloud infrastructure function set to assign new virtual resources in order to meet new management requirements. Through this reference point, there is no need for management controller FS to know any details about the physical layer resources, and it only sends the command including the requirement for the virtualized resources, then cloud hypervisor function will handle the rest.
r3	Between management service function set and management controller function set.	Reference point r3 is provided from the management controller function set to the management service function set. Through this reference point, applications can use the common functions provided by the management controller FS. For example, one service application can search for another service application which may be able to meet its requirements. Management controller FS can also use this reference point to perform the management service analysis and composition, etc.
r4	Between management service applications.	Reference point r4 is between management service functions at the application level. Usually, there are cases when one management service function need the support of another management service function, then it just invokes the function provided by that management service function. Reference point r4 is used in this situation.
r5	Between management service function set and the NEFs of the network to be managed.	Network to be managed is the target for network management. Through reference point r5, management service functions can interact with the NEFs in the network to be managed, and perform the actual network management functions.

Requirements for service management in cloud-aware telecommunication management system

Recommendation ITU-T M.3371

(10/2016)

SERIES M: TELECOMMUNICATION MANAGEMENT, INCLUDING TMN AND NETWORK MAINTENANCE

Summary

Recommendation ITU-T M.3371 defines the general and functional management requirements that support service management in a cloud-aware telecommunication management system (see Recommendation ITU-T M.3070) and provides a functional framework for service management in a cloud-aware telecommunication management system.

Keywords

Cloud-aware telecommunication management system, cloud computing, functional framework, functional requirement, service management.

Table of Contents

1 Scope

This Recommendation defines the general and functional management requirements that support the service management in a cloud-aware telecommunication management system (see [ITU-T M.3070]), and it also provides a functional framework for service management in a cloud-aware telecommunication management system.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T M.3070] Recommendation ITU-T M.3070/Y.3521 (2016), *Overview of end-to-end cloud computing management.*

[ITU-T X.1601] Recommendation ITU-T X.1601 (2015*), Security framework for cloud computing.*

[ITU-T Y.3522] Recommendation ITU-T Y.3522 (2016*), End-to-end cloud service lifecycle management requirements.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 cloud computing [b-ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

3.1.2 cloud service [b-ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.3 cloud service provider [b-ITU-T Y.3500]: Party which makes cloud services available.

3.1.4 customer [b-ITU-T M.60]: An entity which receives services offered by a service provider based on a contractual relationship. It may include the role of a network user.

3.1.5 inter-cloud computing [b-ITU-T Y.3511]: The paradigm for enabling the interworking between two or more cloud service providers.

NOTE – Inter-cloud computing is also referred as inter-cloud.

3.1.6 service [b-ITU-T M.3050.1]: Services are developed by a Service Provider for sale within Products. The same service may be included in multiple products, packaged differently, with different pricing, etc.

3.1.7 service management interface [ITU-T M.3070]: Interface that provides a set of management capabilities exposed by a cloud service through which the cloud service can be managed.

3.1.8 service provider [b-ITU-T M.3320]: A general reference to an entity who provides telecommunication services to Customers and other users either on a tariff or contract basis. A Service Provider may or may not operate a network. A Service Provider may or may not be a Customer of another Service Provider.

3.1.9 telecommunication service [b-ITU-T M.60]: That which is offered by an Administration to its customers in order to satisfy a specific telecommunication requirement.

NOTE – Bearer service and teleservice are types of telecommunication service. Other types of telecommunication service may be identified in the future.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 TC-hybrid service: The service which consists of both telecommunication and cloud service components.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CSP Cloud Service Provider

CT Communications Technology

E2E End-to-End

IT Information Technology

KPI Key Performance Indicator

KQI Key Quality Indicator

SMI Service Management Interface

5 Conventions

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

In the body of this Recommendation and its annexes, the words shall, shall not, should, and may sometimes appear, in which case they are to be interpreted, respectively, as is required to, is prohibited from, is recommended, and can optionally. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative is to be interpreted as having no normative intent.

6 Overview

As an important part of telecommunication management, service management implements all of the functionalities necessary for the management and operations of communications and information services required by or proposed to customers.

It includes service fulfilment, service assurance and service billing through the lifecycle of the service:

– service fulfilment: To fulfil the resource capacity and service quality requirements of customers, maintain the readiness of the resource and service capacity, provide function and interface to customers for the access and consumption of service;

– service assurance: To support the function and process of service assurance, includes service level management, service incident and problem management, service monitoring and reporting management;

– service billing: To support the function and process of service billing.

With the convergence of information technology (IT) and communications technology (CT) industries, cloud computing is being adopted in telecommunication infrastructures. Telecommunication operators deliver cloud services, and also apply cloud computing technologies for the optimization of their telecommunication service platforms and telecommunication support systems.

[ITU-T M.3070] has defined a service management interface (SMI)-based common model for end-to-end (E2E) cloud computing management, which is described in Figure 6-1. In this model, a cloud-aware telecommunication management system can manage cloud-based facilities through the management interface "I1" which can correspond to a set of SMIs.

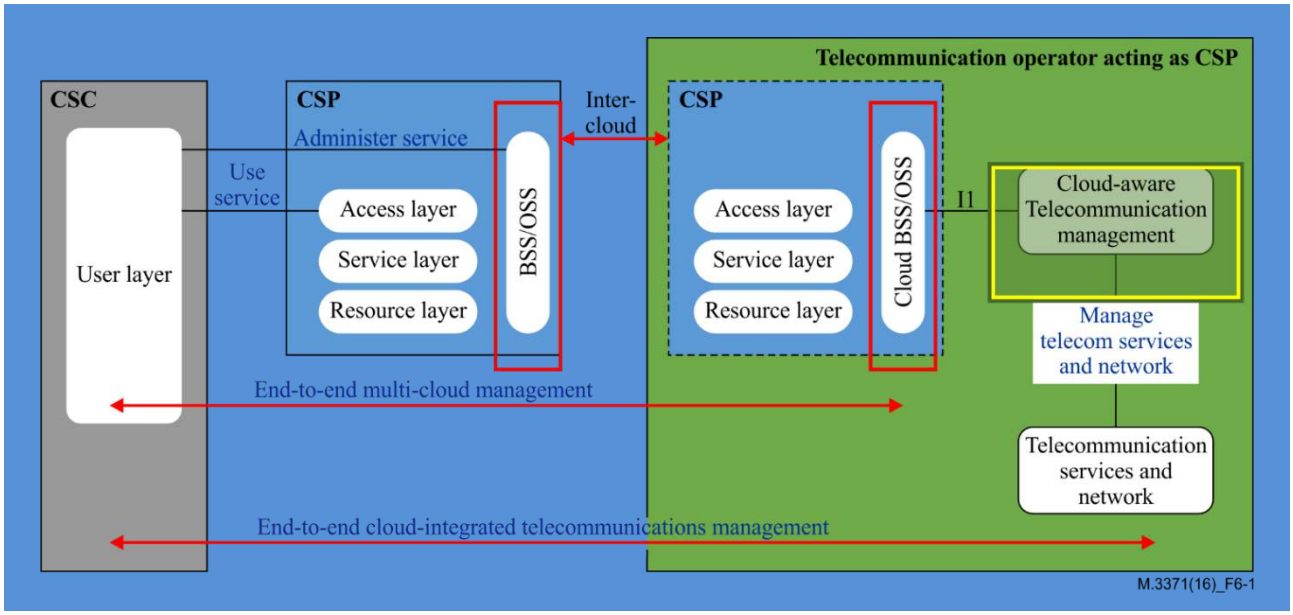


Figure 6-1 – Common model for E2E cloud computing management, with telecommunication operator acting as a CSP (after [ITU-T M.3070])

A cloud-aware telecommunication management system can manage both telecommunication services and cloud services in a consistent manner. Although the management layering could be the same as the traditional telecommunication management layering, with the introduction of cloud computing, there are still new requirements for cloud-aware telecommunication management. This Recommendation addresses the requirements of comprehensive service management in a cloud-aware telecommunication management system.

The relationship between cloud service management and service management in a cloud-aware telecommunication management system is also illustrated in Figure 6-1. The cloud service management is located in business support system(BSS)/operations support system (OSS) (marked by the red rectangle in Figure 6-1) which belongs to the cloud service provider (CSP), and the service management in the cloud-aware telecommunication management system (marked by the yellow rectangle in Figure 6-1) which belongs to telecommunication operator. As an important aspect of cloud service management, cloud service lifecycle management (see [ITU-T Y.3522]) is also located in BSS/OSS which belongs to CSP.

7 General requirements for service management in cloud-aware telecommunication management system

As a cloud-aware telecommunication management system, the difference with a traditional telecommunication management system is it could support comprehensive management for telecommunication services, cloud services and TC-hybrid services which consist of both telecommunication and cloud service components.

In a cloud-aware telecommunication management system, the general requirements include:

– it is required that service management provides service catalogue and service inventory management functionality for telecommunication service, cloud service and TC-hybrid service;

– it is required that service management supports the on-demand and automated service provisioning modification and termination for telecommunication service, cloud service and TC-hybrid service;

– it is recommended that service management supports the E2E quality assurance of telecommunication service, cloud service and TC-hybrid service, and provide high levels of reliability and availability according to the service level agreement (SLA);

– it is recommended that service management supports charging for telecommunication service, cloud service and TC-hybrid service, according to use time, bandwidth, resource usage and any combination of these;

– it is recommended that service management supports monitoring, auditing and reporting for telecommunication service, cloud service and TC-hybrid service, for the purpose of service quality evaluation and assurance.

All of the requirements listed above are suitable for services provided by single CSP as well as inter-cloud service provider.

8 Functional framework for service management in cloud-aware telecommunication management system

The high-level organization of service management functionalities in a cloud-aware telecommunication management system is composed of service catalogue management, service inventory management, service test management, service order management, service problem management, service quality management, service performance management and service rating/discounting management.

Figure 8-1 depicts the functional framework for service management in a cloud-aware telecommunication management system:

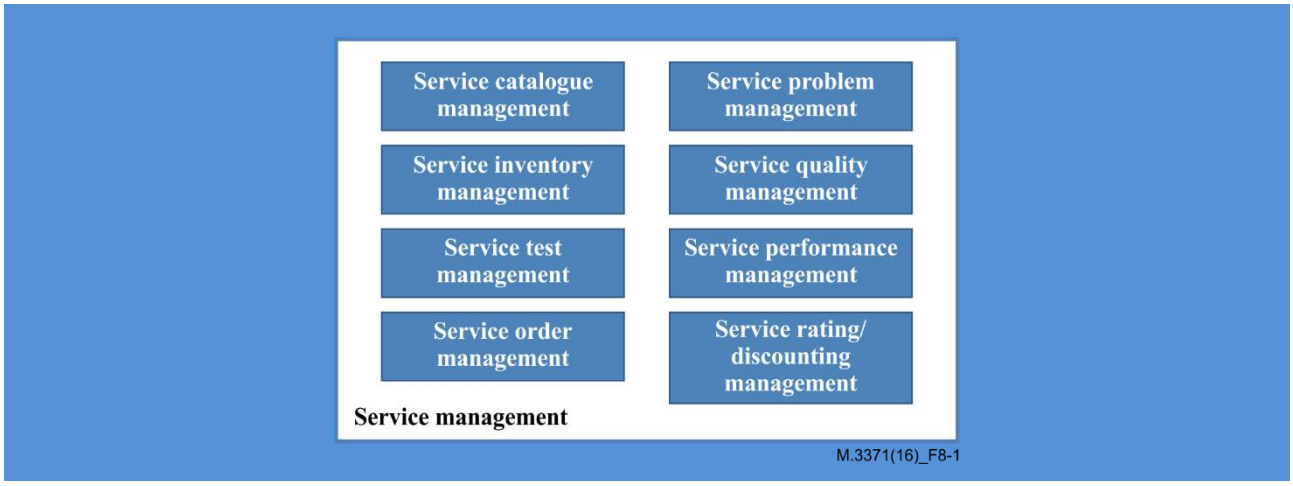


Figure 8-1 – Functional framework for service management in cloud-aware telecommunication management system

The functions are as follows:

– service catalogue management: Provides capabilities for creating and designing new services, mapping service definitions, managing complex rules, supporting componentization of services and managing their relationships and dependencies;

– service inventory management: Provides capabilities for storing and managing service instances and their attributes. It also stores and manages service relationships, which is the mapping of services to other services and/or service components;

– service test management: Provides the capabilities for ensuring that the various services are working properly. In the fulfilment process, the service test is responsible for ensuring that the assigned service works as designed. In the assurance process, the service test is responsible for service trouble/problem distinguishing;
– service order management: Provides the capabilities for managing the E2E lifecycle of a service request. This includes validating service availability as well as the service order request. It also includes service order issuance, service and/or product order decomposition, and service order tracking along with orchestrating the activation and the test processes;
– service problem management: Provides the capabilities for receiving service affecting customer problems as well as network troubles/faults, relating the various problems, and resolving them in an efficient manner;
– service quality management: Provides the capabilities for monitoring and managing the levels of service. Service quality measurements are collected and compared against established quality indicators, and the conclusions made available to interested parties;
– service performance management: Provides the capabilities for monitoring, analysing and reporting on the E2E service performance. This should include a real-time E2E view to ensure that each service is functioning correctly as well as a historical view;
– service rating/discounting management: Provides the capabilities for ensuring that the customer receives an invoice that is reflective of all the billable events delivered by the service provider dictated by their business relationship.

9 Functional requirements for service management in cloud-aware telecommunication management system

This clause provides functional requirements for service management in a cloud-aware telecommunication management system.

9.1 Service catalogue management

In a cloud-aware telecommunication management system, the service catalogue management requirements include:

– it is required that service catalogue management provides functions to manage cloud service information. It is required that service catalogue management provides functions to manage information of TC-hybrid services.

9.2 Service inventory management

In a cloud-aware telecommunication management system, the service inventory management requirements include:

– it is required that service inventory management provides functions to manage the attributes of cloud service;
– it is required that service inventory management provides functions to trace the relationship between the cloud service or TC-hybrid service and resource.

9.3 Service order management

In a cloud-aware telecommunication management system, the service order management requirements include:

– it is required that the service order management provides functions to validate cloud service availability as well as the cloud service order request;
– it is required that the service order management provides functions to manage service and or product order decomposition which contain cloud service;

– it is required that the service order management provides functions to track the provisioning process of service order which contain cloud service.

9.4 Service problem management

In a cloud-aware telecommunication management system, the service problem management requirements include:

– it is required that the service problem management provides functions to manage complaint tickets from the customer side as well as trouble tickets from network surveillance;

– it is required that the service problem management provides functions to separate a fault between the cloud and the telecommunication network;

– it is recommended that the service problem management has holistic view of configuration/relationship of different network layers to support root cause analysis.

9.5 Service performance management

In a cloud-aware telecommunication management system, the service performance management requirements include:

– it is required that the service performance management provides functions to monitor, analyse and report the key performance indicator (KPI) of cloud service.

9.6 Service test management

In a cloud-aware telecommunication management system, the service test management requirements include:

– it is required that the service test management provides functions to test the cloud service, both in the fulfilment and assurance process.

9.7 Service quality management

In a cloud-aware telecommunication management system, the service quality management requirements include:

– it is required that the service quality management provides functions to monitor, analyse and report the key quality indicator (KQI) of cloud service.

9.8 Service rating/discounting management

In a cloud-aware telecommunication management system, the service rating/discounting management requirements include:

– it is required that the service rating/discounting management provides functions to support service rating/discounting in the context of service bundling and composition which contains cloud service.

10 Security considerations

Security aspects for consideration within the cloud computing environment, including service management in a cloud-aware telecommunication management system, are addressed by security challenges for the CSPs as described in [ITU-T X.1601]. In particular, [ITU-T X.1601] analyses security threats and challenges, and describes security capabilities that could mitigate these threats and meet the security challenges.

Bibliography

[b-ITU-T M.60] Recommendation ITU-T M.60 (1993), *Maintenance terminology and definitions*.

[b-ITU-T M.3050.1] Recommendation ITU-T M.3050.1 (2007), *Enhanced Telecom Operations Map (eTOM) – The business process framework*.

[b-ITU-T M.3320] Recommendation ITU-T M.3320 (1997), *Management requirements framework for the TMN X-interface*.

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014), *Information technology – Cloud computing – Overview and vocabulary*.

[b-ITU-T Y.3511] Recommendation ITU-T Y.3511 (2014), *Framework of inter-cloud computing*.

[b-ITU-T Y.3520] Recommendation ITU-T Y.3520 (2015), *Cloud computing framework for end to end resource management*.


network
www

Cloud computing framework for end to end resource management

Recommendation ITU-T Y.3520

(09/2015)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Summary

Recommendation ITU-T Y.3520 presents general concepts of end to end resource management in cloud computing; a vision for adoption of cloud resource management in a telecommunication-rich environment; and multi-cloud, end to end resource management for cloud services, i.e., management of any hardware and software used in support of the delivery of cloud services.

Keywords

Cloud computing, cloud service, framework, requirement, resource management.

Table of Contents

1 Scope

This revised Recommendation provides a framework for end to end resource management in cloud computing. It includes:

– general concepts of resource management for end to end cloud computing resource management;

– a vision for adoption of resource management for cloud computing in a telecommunication-rich environment;

– multi-cloud, end to end management of cloud computing resources and services, e.g., management of any hardware and software used in support of the delivery of cloud services.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1601] Recommendation ITU-T X.1601 (2014), *Security framework for cloud computing*.

[ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014), *Information technology – Cloud computing – Overview and vocabulary*.

[ITU-T Y.3501] Recommendation ITU-T Y.3501 (2013), *Cloud computing framework and high-level requirements*.

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), *Information technology – Cloud computing – Reference architecture*.

[ITU-T Y.3511] Recommendation ITU-T Y.3511 (2014), *Framework of inter-cloud computing*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 cloud computing [ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications and storage equipment.

3.1.2 cloud deployment model [ITU-T Y.3500]: Way in which cloud computing can be organized based on the control and sharing of physical or virtual resources.

NOTE – The cloud deployment models include community cloud, hybrid cloud, private cloud and public cloud.

3.1.3 cloud service [ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.4 cloud service category [ITU-T Y.3500]: Group of cloud services that possess some common set of qualities.

3.1.5 cloud service customer [ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

NOTE – A business relationship does not necessarily imply financial agreements.

3.1.6 cloud service provider [ITU-T Y.3500]: Party which makes cloud services available.

3.1.7 cloud service user [ITU-T Y.3500]: Natural person, or entity acting on their behalf, associated with a cloud service customer that uses cloud services.

NOTE – Examples of such entities include devices and applications.

3.1.8 emergency telecommunications (ET) [b-ITU-T Y.2205]: ET means any emergency related service that requires special handling from the NGN relative to other services. This includes government authorized emergency services and public safety services.

3.1.9 emergency telecommunication service (ETS) [b-ITU-T E.107]: A national service providing priority telecommunications to the ETS authorized users in times of disaster and emergencies.

3.1.10 inter-cloud computing [ITU-T Y.3511]: The paradigm for enabling the interworking between two or more cloud service providers.

3.1.11 management system [b-ITU-T M.60]: A system with the capability and authority to exercise control over and/or collect management information from another system.

3.1.12 service level agreement [ITU-T Y.3500]: Documented agreement between the service provider and customer that identifies services and service targets.

NOTE 1 – A service level agreement can also be established between the service provider and a supplier, an internal group or a customer acting as a supplier.

NOTE 2 – A service level agreement can be included in a contract or another type of documented agreement.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 resource management: The most efficient and effective way to access, control, manage, deploy, schedule and bind resources when they are provided by service providers and requested by customers.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

3G	Third Generation
4G	Fourth Generation
BSS	Business Support System
CDN	Content Delivery Network
CRM	Customer Relationship Management
CSC	Cloud Service Customer
CSP	Cloud Service Provider
ET	Emergency Telecommunications
ETS	Emergency Telecommunication Service
FI	Functional Interface
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
LTE	Long Term Evolution
MPLS	Multi-Protocol Label Switching
NGN	Next Generation Network

OAM	Operations, Administration and Maintenance
OSS	Operations Support System
PaaS	Platform as a Service
PHP	Hypertext Pre-processor
QoS	Quality of Service
SES	Software Enabled Services
SLA	Service Level Agreement
SMI	Service Management Interface
SNMP	Simple Network Management Protocol
VM	Virtual Machine
VoIP	Voice over IP
WAN	Wide Area Network
WiFi	Wireless Fidelity

5 Conventions

In this Recommendation:

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

In the body of this Recommendation and its appendices, the words shall, shall not, should, and may sometimes appear, in which case they are to be interpreted, respectively, as is required to, is prohibited from, is recommended, and can optionally. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative are to be interpreted as having no normative intent.

6 End to end cloud resource management overview

The following clauses provide an overview of the general concepts of end to end cloud computing resource management in a telecommunication rich environment.

6.1 Introduction

One significant value of cloud service providers will most likely be the rapid design, development, deployment and management of cloud services. With the adoption of cloud computing service delivery capabilities, multiple service providers will provide more cloud services as composite or mash-up services. Service providers will increasingly have as their objective the rapid delivery of more customized, composite cloud-based services tailored to various customer scenarios [b-FGCC Part 4].

In this Recommendation, the term multi-cloud refers to usage scenarios involving the use of various cloud services implemented by more than one cloud service provider (CSP), though this multiplicity of CSPs may not be visible to the cloud service customer (CSC). This is not to be confused with the multi-platform cloud computing environment, which is a characteristic of cloud service providers that have chosen to offer a variety of programming and runtime execution facilities to assist in the development and execution of cloud applications. Nor should it be confused with the term "inter-cloud" which refers to the relationship and interconnection between CSPs and not to the overall end to end system.

Cloud applications (also known as cloud workloads) are applications (i.e., software programs designed for a specific purpose) that require execution in the cloud service provider's data centres in order for cloud services

to be instantiated and become available for use by the cloud service users. In other words, a cloud application needs to be executed to make one or more cloud services available.

Cloud service providers need to increasingly offer multi-cloud platform solutions to support the above scenarios. Such solutions will need to be flexible and effective in managing resources across multiple cloud service providers [ITU-T Y.3501].

These solutions can be realized using cloud services, delivered through cloud computing capabilities with reusable services. Cloud service providers need to develop a deep insight into, and understanding of, the run-time aspects of service delivery as well as the management of these services and the resources required to deliver them.

Therefore, there is a need for a common concept for end to end resource management across multiple cloud service providers.

Complex, media-rich, composite services use a variety of both telecommunication and information technology (IT) infrastructures and are composed of individual service components that may be acquired from, or exposed to, third parties.

6.2 Service delivery management structure

The framework described in this Recommendation can be used to enable the delivery of cloud services, independent of the underlying software or network technologies. This framework, which is a service delivery management structure, needs to address the full cloud services lifecycle, covering such important use cases as service composition, aggregation and service catalogues.

Management of cloud services needs to provide a framework for the essential building blocks required to manage the delivery of cloud services and foster the basis for detailed service delivery management.

One objective is to provide a means to allow consistent end to end management, including accounting, of services exposed by and across, domains and platforms of different cloud service providers. A standard framework and best practices are needed to support business practices associated with multiple provider cooperation throughout the lifecycle of the service and to foster wide adoption of the standard artefacts in any architecture, technology environment and service domain.

Achieving consistent maintenance of cloud services sourced from different domains is a challenging task. To address this challenge, an approach that enables and supports consistent management access to the cloud services is desired. Such an approach is desired to complement the service capabilities exposed by the software component's interfaces with additional lifecycle management operations. This approach should also enable reusability of services in different environments, especially in cloud computing.

Frameworks, architecture, design patterns and best practices are required to realize the above objectives for the cloud service providers. The interfaces of individual service components are not the primary focus as the actual interfaces may vary across different implementations, vendor technologies and operator requirements. Standard design principles and frameworks are required to allow for the rapid development, deployment and management of composite multi-cloud services provided by the telecommunication industry.

This provides a framework to guide architects and developers of cloud services regarding the end to end management of cloud computing resources.

6.3 Difference between cloud computing and the traditional form of computing

There are two principal differences between cloud computing and the traditional form of computing that make the problem of managing resources associated with cloud services more difficult. One difference is the virtualization of the computing and network resources in the cloud computing reference architecture [ITU-T Y.3502]. The other difference is that multiple cloud service provider domains are increasingly involved in the delivery of cloud services and this environment greatly complicates end to end resource management.

6.4 Resource management for a single cloud service provider

The overall resource management should be viewed from the point of view of the lifecycle management of a cloud application. The application, as it passes through its lifecycle, must be acted upon by traditional business processes associated with management system functions such as administration, provisioning, configuration, service assurance and charging.

As shown in Figure 1, in the simpler case of an application that resides on a single cloud computing system, it becomes dependent on two distinct categories of virtualized resources. The dotted arrows depict the active coordinated relationship that must be maintained between resources at each level.

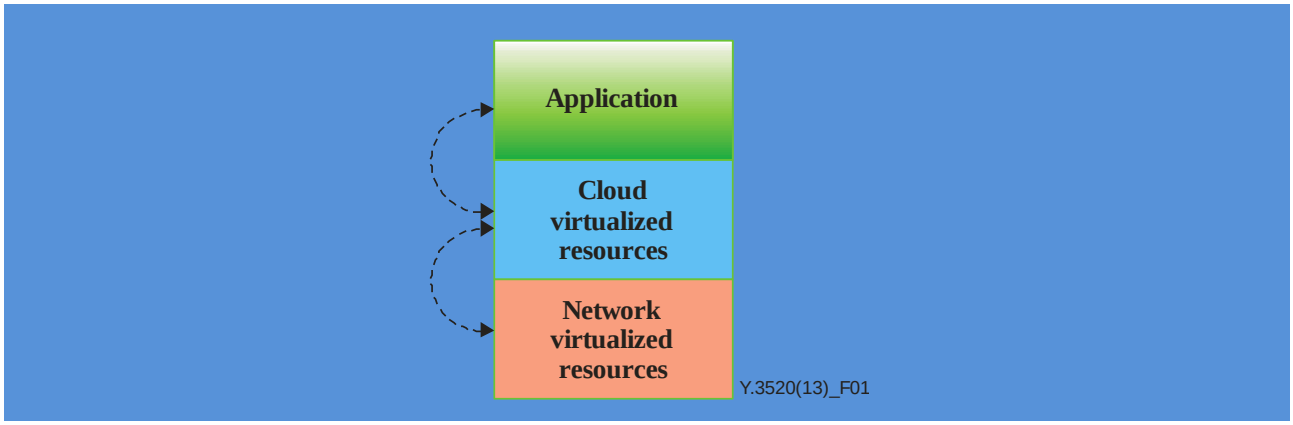


Figure 1 – Applications residing on a single cloud computing system

NOTE – Although Figure 1 divides virtualized resources into "cloud" and "network", cloud computing considers all resources at the same level [ITU-T Y.3502].

A resource management issue requiring further work is how to use existing cloud management systems to maintain awareness of which logical and physical resources are actually relevant to a specific instance of a specific application at any given point in time.

Due to the rapid elasticity and scalability characteristic of cloud computing [ITU-T Y.3500], the cloud computing system can configure additional resources to handle changing application demands; there are additional requirements, needing further analysis, for dynamically reconfiguring the underlying network configurations in response to the changing resources at various components of the cloud computing system. This issue arises both within the internal network fabric of large cloud computing data centres, between the interconnecting networks in hybrid scenarios, and across transport networks and content delivery networks.

Another issue that arises is the division of responsibility between an internal cloud computing virtualization management system and an external management system. Although the cloud computing virtualization function can typically manage its own physical and logical resource allocations for supported applications, an external management system may be desired to dynamically reallocate resources in a coordinated fashion across the three levels shown in Figure 1 or to track and have knowledge of those changing relationships.

As shown in Figure 2, the capability of a management system to both manage resource allocations and track their instantaneous state could enable that management system to provide the information necessary to display the status of a given service and all of the underlying relevant resources, at any given point in time.

From the point of view of the quality of service of resource management, the issue is how to ensure that the service assurance systems are receiving relevant telemetry from the cloud computing or network resources actually involved in delivering a particular instance of a service. The issue is less concerned with what telemetry data needs to be managed, as each dataset is often unique to a given management system implementation, but is more concerned with how to use the cloud computing system to do so effectively.

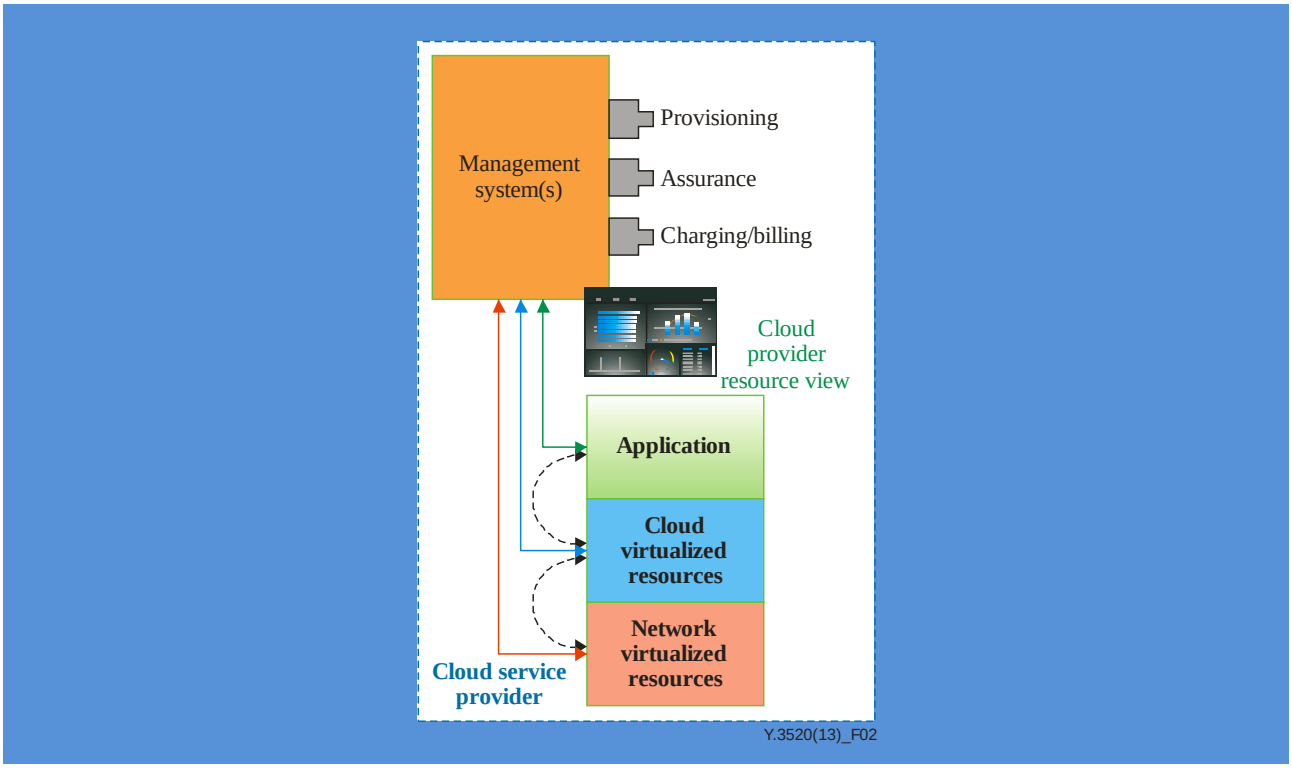


Figure 2 – Cloud resource management system (OSS and BSS)

6.4.1 Software enabled services

The software enabled services (SES) management approach enables both traditional service providers as well as Internet content and media service providers to leverage the opportunities and service marketplace that are presented by the convergence of networking and IT. Specifically, the SES management approach provides a means to allow consistent end to end management and metering of services exposed by and across different service providers' domains and technologies.

Operations, administration and management interfaces for cloud services today are structured in silos per technology, standardized by specific standards development organizations or implemented by vendors as proprietary implementations. This presents a challenge in the rendering of consistent management of services sourced from different domains.

The SES management approach proposes a mechanism to allow consistent access to the software components information as well as management operations. This consistent access is achieved by incorporating the management interface in addition to the functional interface (FI) definition that is part of software component creation. The SES approach enables reusability of services in different environments, including that of cloud computing by manipulating the SES lifecycle management metadata which is supporting the service management interface (SMI) operations.

For further information about SES and SMI concepts, please refer to Appendix III.

The SES pattern is defined to also handle those cases where the composed service is not able to manage all of the management dependencies by means of the logic which is triggered by the SMI operations. In this case, the lifecycle management metadata associated with the SMI is providing a recipe which describes how to manage the composition members.

Protocol neutral interface information models and class models of the SMI, along with corresponding statements of interface information requirements and interface information use cases, can then be defined [b-TMF TR198].

In order for implementation of SESs to be as useful as possible, the following requirements should be addressed:

- It is recommended that service design be as efficient as possible, requiring only the needed information for both input and output parameters, without being verbose. There should not be many arguments on the different management system operations.
- It is recommended that service design be simple, allowing for easy implementation in legacy as well as in new services. There should be no complex dependencies between the arguments of the different management information system operations.
- It is recommended that service implementation rely on industry standards in order to guarantee that it will be interoperable between different platforms.
- It is recommended that the SMI be extensible and generic to accommodate all SES scenarios.
- It is recommended that the SMI be easy to extend and that this interface be adapted to support additional management aspects of a specific domain or of a specific vendor.
- It is recommended that the SMI be agnostic to implementation, architecture, or business processes, to ensure adoption by many industry sectors.
- It is recommended that a non-"well designed service" be wrapped by a façade service in order to make it a "well designed service".

The SMI in the software enabled services reference architecture can be used to describe the management capabilities of SES. Examples of these capabilities are in the areas of invocation, provisioning, status, history, usage and health monitoring and associated alerts, management lifecycle state configuration as well as decommissioning of a given software enabled service [b-TMF TR198].

The SES management approach was designed to address the management of a single cloud service provider. In the next clause, it will be explained how the same concept can be applied to address a multiple cloud service provider scenario.

6.5 Resource management for multiple cloud service providers

Clause 6.4 describes the managing of resources for a single cloud service provider. However, cloud service delivery scenarios typically involve coordination across multiple cloud service providers residing in different domains.

Figure 3 illustrates the end to end management framework in a multi-cloud service provider domain scenario. Given the way in which customized management interfaces are exposed in a single cloud service provider implementation, the framework enables end to end management of composed services and their underlying dynamically changing resources.

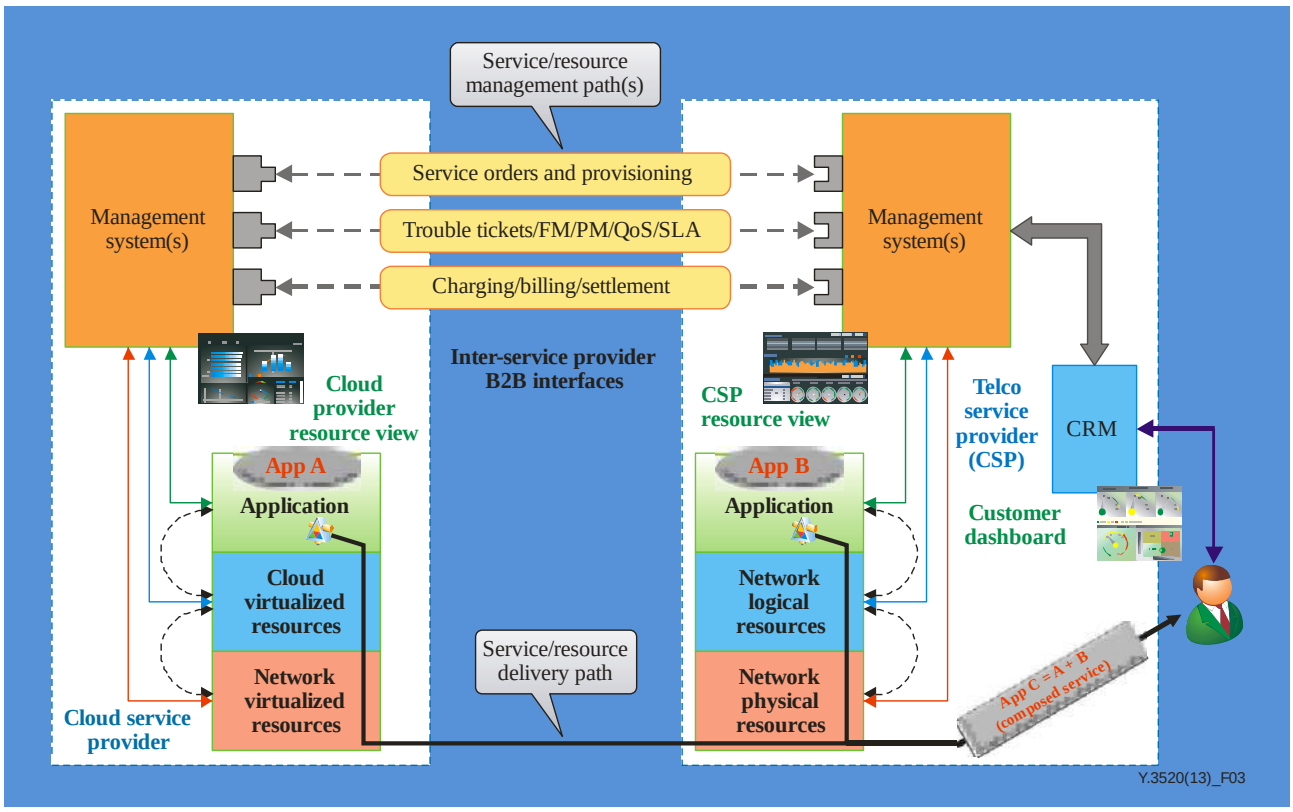


Figure 3 – End to end management expectations in a multi-cloud scenario

Similar to the case of a single cloud scenario, service and resource management interfaces need to be able to manage the relevant underlying resources in a coordinated manner that is effectively transparent to the external systems that are interacting with those management interfaces.

Figure 3 depicts a management system architecture providing the needed management interfaces (again, the interfaces themselves are not at issue, as each implementation may have fine-tuned its own). The best practices should provide the flexibility for the cloud application itself to expose its service or resource management interfaces. In addition, they need to enable a management system to expose one or more of the interfaces so that the management system is tracking the dynamic changes in the underlying resources allocated to support the cloud application being managed.

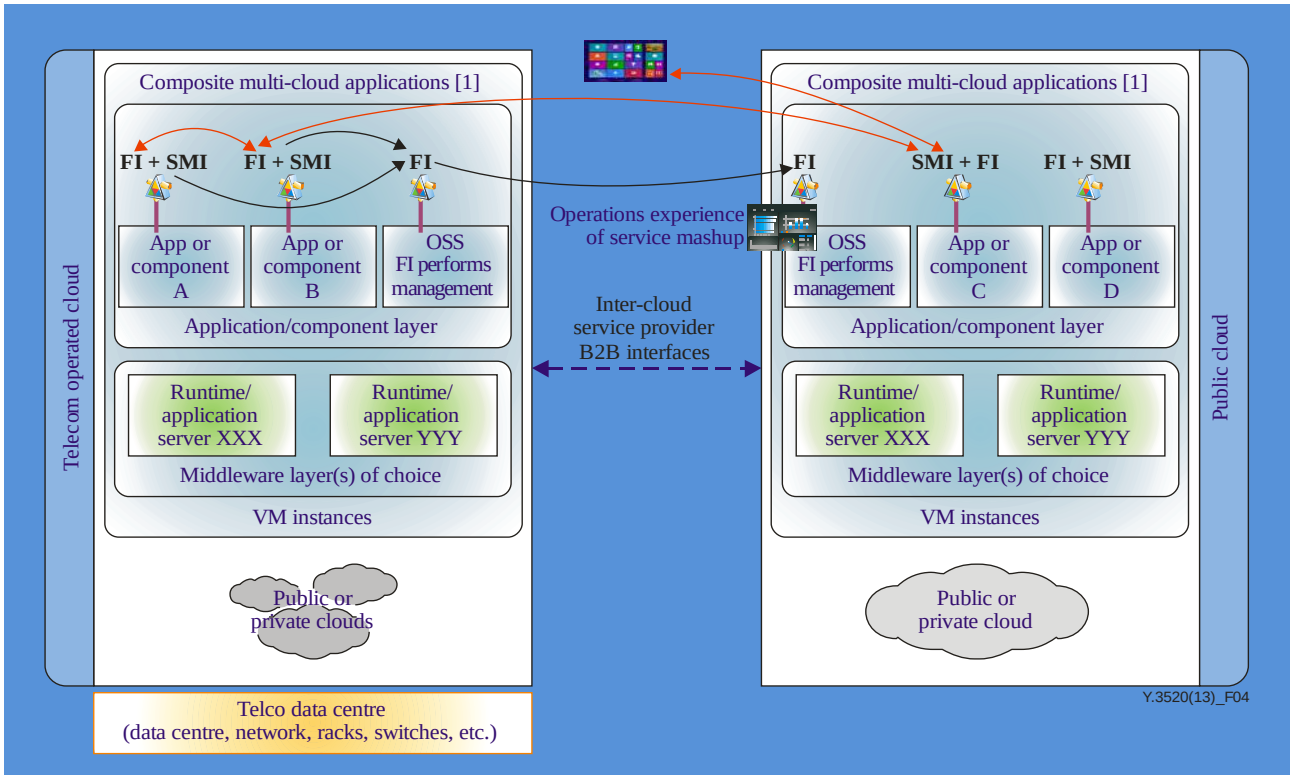
The framework permits each CSP, as well as the CSC, to have accurate knowledge regarding the actual status of services via metrics retrieved from the underlying relevant resources across a multi-cloud environment. In other words, all three dashboards depicted in Figure 3 need to accurately display the status of the services. In addition, the framework should consider a comprehensive service lifecycle management process from the point of view of CSPs and CSCs, i.e., the stages needed from the time the CSC makes a request until the CSP receives compensation.

7 Requirements for the resource management involving multi-cloud service providers

7.1 High-level architecture for end to end multi-cloud resource management

Figure 4 shows a high-level architecture for end to end multi-cloud resource management. This architecture depicts the virtual machines containing a software stack consisting of middleware layers containing application servers hosted by the runtime environment of choice, on top of which cloud applications execute.

Figure 4 also shows both functional interfaces (FIs) and service management interfaces (SMIs) being exposed by various cloud applications running on multiple cloud data centres. The information can be consumed from various SMIs that are exported by multiple applications executing in multiple cloud data centres, allowing for a comprehensive end to end multi-cloud resource management and monitoring system to be realized.



NOTE – Composite multi-cloud applications can be written in a runtime and programming environment of choice, independent of the choice of cloud provider or cloud-deployment model. For example, use of Java, Node.js, PHP or .NET in both private and public clouds.

Figure 4 – Architectural vision for multi-cloud, multi-platform cloud management

In Figure 4, the applications executing in the virtual machines (VMs) could be a composite, distributed application built from various software components. A VM instance could contain all software components that belong to such an application, or only some of them in the case where the application is distributed and executing in more than one VM (hence the references to applications or components in Figure 4).

The architectural vision shown in Figure 4 enables interoperable applications to support cloud burst or hybrid cloud computing scenarios.

7.2 Functional requirements for end to end cloud resource management

To meet the high level architecture of end to end cloud resource management described in this Recommendation, a cloud computing platform should conform to the following requirements:

- It is required that the CSP supports the architectural and functional capabilities offered by the SES management approach in order to realize end to end cloud resource management.
- It is recommended that the cloud computing platform offers the cloud deployment model [ITU-T Y.3500] choice and workload portability across multiple CSPs in order to share workloads.
- It is recommended that the cloud computing platform provide the ability to support hybrid cloud applications, where the components of the cloud application run on various cloud data centres managed by different CSPs.
- It is recommended that cloud service provider, irrespective of the cloud deployment model they use, provide the support for multiple application frameworks, programming languages, tools and technology platforms, thereby lowering the potential for lock-in into specific solution or middleware technology.
- It is recommended that the cloud computing platform provides an architecture enabling telecommunications-grade capabilities including reliability, fail-over and monitoring inclusive of choice of middleware, programming language and runtime.

- It is recommended that the cloud computing platform supports workload portability and related management capabilities (e.g., control, operation and monitoring) amongst cloud service providers, supporting various cloud deployment models [ITU-T Y.3500], in a cost effective way.

8 Cloud resource management for emergency telecommunications

Emergency telecommunications (ET) [b-ITU-T Y.2205] are any emergency related service that requires special handling relative to other services (i.e., priority access for authorized users and priority treatment to emergency traffic).

While not always required, if the resources of the CSP are used to support the emergency telecommunications service (ETS) [b-ITU-T E.107], appropriate resource management functions will be needed to allow priority treatment in the use of the cloud computing resources by authorized users. The requirements in [b-ITU-T Y.1271] are relevant.

NOTE – Requirements in [b-ITU-T Y.1271] apply across multiple layers of the cloud computing reference architecture [ITU-T Y.3502].

9 Security considerations

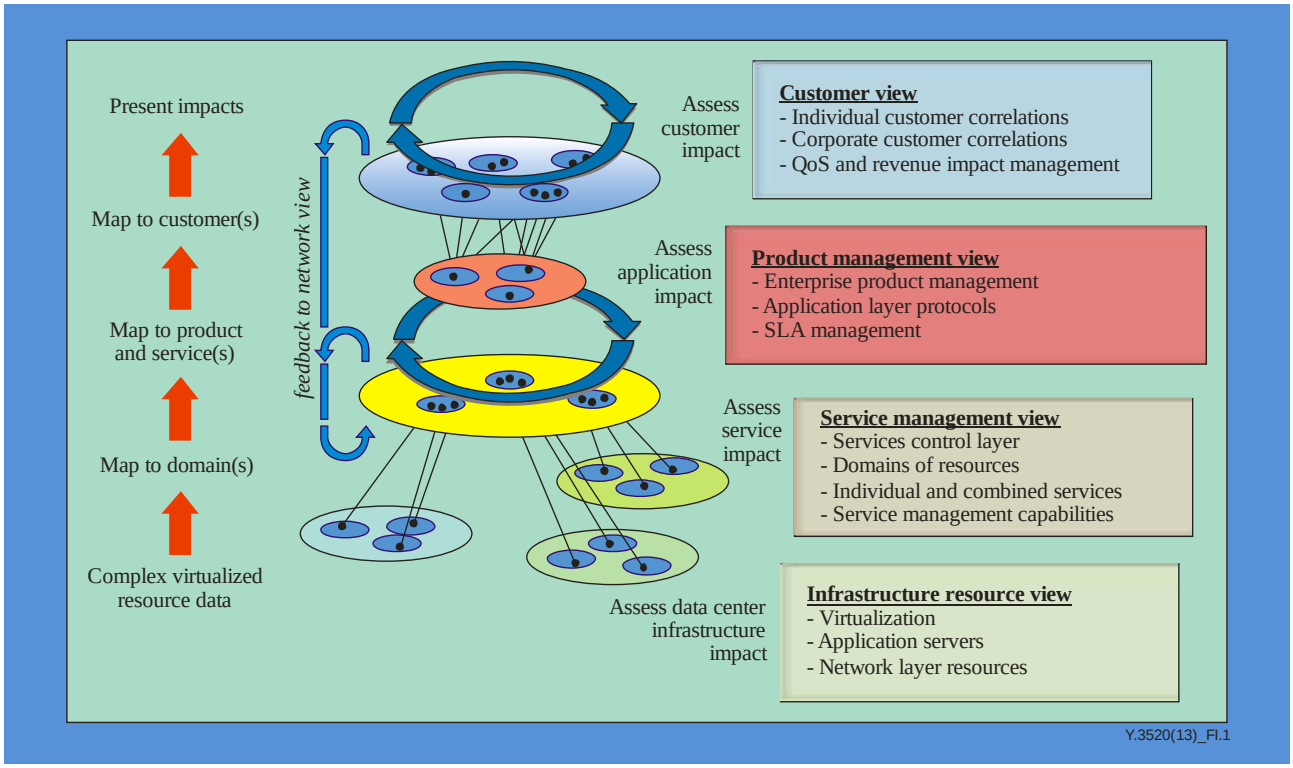
The security framework from cloud computing [ITU-T X.1601], analyses security threats and challenges in the cloud computing environment and describes security capabilities that could mitigate these threats and address security challenges. The single cloud and multi-cloud resource management framework described in this Recommendation is based on the interconnections within a single cloud service provider or between two or more cloud computing systems operated by different service providers. Thus, secure interconnection within and across the systems should be considered. Protection of internal management system interfaces and information against unauthorized access, internally or by an external interconnected entity, should also be considered. Exposed internal and external management interfaces should also be security protected. It is recommended that the applicable X, Y and M series of ITU-T security Recommendations be taken into consideration, including access control, authentication, data confidentiality, communications security, data integrity, availability and privacy.

Appendix I

Comprehensive view of management layers

(This appendix does not form an integral part of this Recommendation.)

Figure I.1 is an attempt at describing the management layers and how the service management interface (SMIs) for each layer correlate with each other to offer a complete picture. The cloud computing data centre implementation layers are depicted by large circles parallel to each other. The SMIs are depicted by small blue circles containing the information required by the management system in order to achieve a holistic view of the entire operation. The straight lines between each plane show the flow of information and relationship between what is happening at each layer, depicting how each layer is related to and affected by, the neighbouring one. Looking at the diagram in its entirety helps the viewer to realize why it makes sense to expose consistent SMIs from each layer and to expose management information and telemetry in a consistent matter that can then be rolled up into a comprehensive diagnostics and management solution that can be used by a telecom operator offering and consuming cloud services and products.



NOTE – Domains are related to CSP.

Figure I.1 – Comprehensive view of management layers

Appendix II

Multi-cloud end to end service management

(This appendix does not form an integral part of this Recommendation.)

The following use case describes the challenges associated with multi-cloud end to end service management.

Figure II.1 illustrates an example where a cloud VoIP service is provided by CSP1 to CSP2 that is bundling it with other services and reselling a package to a cloud service customer (CSC). Even if CSP1 runs network services such as a content delivery network (CDN), CSP2 provides network connectivity services to the end user through its own core networks (e.g., IP/MPLS) and access networks (e.g., the backhaul, WiFi, 3G/4G/LTE and enterprise LAN/WAN infrastructures).

When a CSC, such as an IT department, has a problem with the cloud VoIP quality of service, it contacts CSP2 using a customer relations management (CRM) system. The CSP2 support agent should have the capability to see the health and welfare of the VoIP service from a holistic (end to end) perspective. This requires visibility into the VoIP and network resource management systems of both CSP1 and CSP2.

As shown in Figure II.1, there are the two types of connection paths:

1. **Service delivery path** – used by the functional interfaces of the services to deliver the combined service value to the customer. In this use case, cloud VoIP and IP/MPLS are combined to create a premium ICT bundle.
2. **Service management path(s)** – all of the logical management paths that perform operations and maintenance functions such as provisioning, service assurance and charging/billing of the relevant services to this bundle.

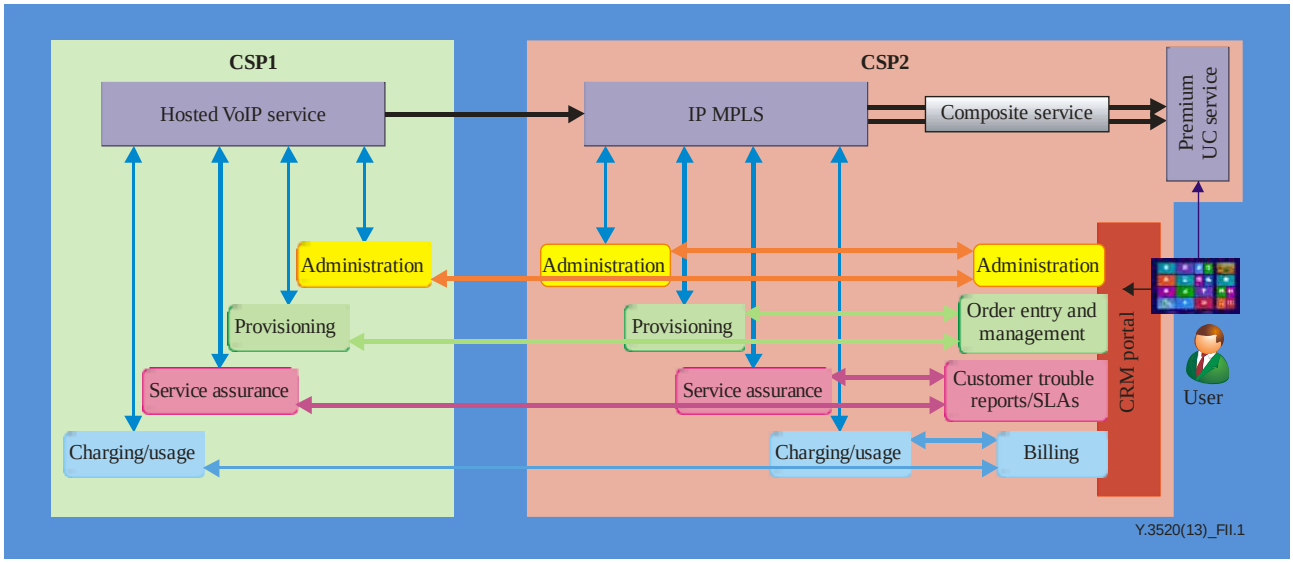


Figure II.1 – Managing multi-cloud services end to end

The delivery path for the service, via their functional interfaces, is not addressed by this use case.

What is addressed is efficient implementation of all of the resource management functions depicted by the lines between the customer relationship management (CRM) portal and the administrative, provisioning, service assurance and charging functions for each component (VoIP, etc.) that makes up a complete service. This challenge, associated with effective cloud resource management, is a major technical issue and can be a limiting factor for the adoption of cloud computing based solutions. In order for the composite cloud computing services to work effectively, all the prerequisite services of both CSP1 and CSP2 must function properly.

When either of the two CSPs becomes aware of a VoIP problem, tools are needed so that they can quickly resolve the problem in an effective manner. This includes being able to see via a service dashboard or CRM portal what has occurred relative to the VoIP service and to investigate in order to obtain greater details concerning any significant item. Additionally, the customer service agent should also be able to initiate an order for new or changed service configurations. However, if the agent lacks access to useful end to end cloud resource management tools and can only create a trouble ticket and then pass the problem off to another agent for action, the cloud service customer will be unsatisfied and this could potentially result in excessive operational expenses.

Appendix III

Summary of SES and SMI concepts

(This appendix does not form an integral part of this Recommendation.)

This Recommendation makes reference to various software enabled service (SES) and service management interface (SMI) concepts as developed in the TM Forum. This appendix is intended to provide a further informative introduction to these concepts; however reference should be made to the relevant TM Forum specifications for all technical details.

III.1 Software enabled service (SES)

A software enabled service is a service that exposes a management interface in addition to its functional interface (FI). Just like a router or switch exposes a simple network management protocol (SNMP) or other style management interface here we are referring to a digital service. However, since a digital service, such as represented by a Platform as a Service (PaaS) workload, is hosted on a virtualized cloud infrastructure, the cloud platform must enable the SMI for each instance of a given service/role at a given point in time. An SES may represent a physical device, a "software" instance, or indeed a distributed function that has no single location or instance.

The TM Forum developed the concept of SES to provide a means to allow consistent end to end management and metering of services exposed by and across different service provider's domains and technologies, such as communication or Web 2.0 services. The TM Forum specifications are intended to support business practices associated with multi-provider cooperation throughout the lifecycle of the service and this by means of lightweight design to foster wide adoption of the standard artefacts in any architecture, technology environment and service domain.

Management interfaces today are siloed per technology, standardized by specific SDOs or implemented by vendors as proprietary implementations. This renders the consistent management of services sourced from different domains as challenging.

The SES management approach proposes a way to allow consistent access to the software components for operations, administration and maintenance (OAM) tasks. This consistent access is achieved by incorporating the service management interface (SMI) in addition to the functional interface (FI) definition that is part of software component creation.

III.2 Service management interface (SMI)

In the context of managing an SES, the SMI concept delivers the ability to configure, activate or suspend a service instance and to receive or be notified of any kind of metrics, health state and detailed information about eventual failures, independent of the underlying technology or architecture.

Perhaps the best way to think of the SMI is as a simple "base class" in object oriented software development that defines the core management interface that can then be inherited by specific interface classes for specific purposes. The base SMI provides the set of operations supported by management objects, which can then be implemented using various management protocols.

The following operations are exposed on the SMI:

- Activation of an SES: Making the SES available for a particular context (deploying the SES)
- Provisioning of an SES: Configuring the settings of an SES or an SES instance
- State monitoring of an SES: Querying the history and current status in terms of life cycle management (for a specific instance of the SES) and listening for status updates
- Usage monitoring of an SES: Querying for usage metrics from the SES instance or listening for usage metrics reports or alarms (e.g., if metrics conditions imply notifications)
- Health monitoring of an SES: Querying for health metrics from the SES instance or listening to alarms from the resource

- Update of an SES: Modification of the setting or life cycle management status of an SES instance
- De-activation of an SES: making the SES unavailable in a particular context

III.3 SMI interface

The SMI support a set of simple operations to allow SES components to interact with management systems in a consistent way:

- getExecutionState
- getManagementReport
- getServiceConfiguration
- setExecutionState
- setServiceConfiguration

For further information about SMI concepts, refer to [b-TMF TR198].

Bibliography

[b-ITU-T E.107] Recommendation ITU-T E.107 (2007), *Emergency Telecommunications Service (ETS) and interconnection framework for national implementations of ETS*.

[b-ITU-T M.60] Recommendation ITU-T M.60 (1993), *Maintenance terminology and definitions*.

[b-ITU-T Y.1271] Recommendation ITU-T Y.1271 (2014), *Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit-switched and packet-switched networks*.

[b-ITU-T Y.2205] Recommendation ITU-T Y.2205 (2011), *Next Generation Networks – Emergency telecommunications – Technical considerations*.

[b-FGCC Part 4] ITU-T Focus Group on Cloud Computing – Technical Report (2012), *Part 4: Cloud Resource Management Gap Analysis.*
www.itu.int/dms_pub/itu-t/opb/fg/T-FG-CLOUD-2012-P4-PDF-E.pdf

[b-TMF TR198] TM Forum TR198, *Multi-Cloud Service Management Pack – Simple Management API (SMI) Developer Primer and Code Pack, Release 2.2*.
www.tmforum.org/?s=TR198


FULL
SERVICE

End-to-end cloud service lifecycle management requirements

Recommendation ITU-T Y.3522

(09/2016)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Summary

Recommendation ITU-T Y.3522 provides an overview of end-to-end (E2E) cloud service lifecycle management by specifying cloud service lifecycle metadata, the cloud service lifecycle management framework, cloud service lifecycle management stages and the relationship with cloud computing reference architecture. This Recommendation also provides E2E cloud service lifecycle management functional requirements derived from the corresponding typical use cases.

Keywords

Cloud service lifecycle management, end-to-end, functional requirements, metadata, model, stage.

Table of Contents

1 Scope

This Recommendation specifies the functional requirements of end-to-end (E2E) cloud service lifecycle management. This Recommendation comprises the following:

– cloud service lifecycle metadata;
– cloud service lifecycle management framework;
– cloud service lifecycle management stages;
– relationship with cloud computing reference architecture;
– functional requirements and typical use cases of cloud service lifecycle management.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T M.3030] Recommendation ITU-T M.3030 (2002), *Telecommunications Markup Language (tML) framework.*

[ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing.*

[ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary.*

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014) | ISO/IEC 17789:2014, *Information technology – Cloud computing – Reference architecture.*

[ITU-T Y.3511] Recommendation ITU-T Y.3511 (2014), *Framework of inter-cloud computing.*

[ITU-T Y.3520] Recommendation ITU-T Y.3520 (2015), *Cloud computing framework for end to end resource management.*

[ITU-T Y.3521] Recommendation ITU-T Y.3521/M.3070 (2016), *Overview of end-to-end cloud computing management.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 cloud computing [ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications and storage equipment.

3.1.2 cloud service [ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.3 cloud service customer [ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

NOTE – A business relationship does not necessarily imply financial agreements.

3.1.4 cloud service partner [ITU-T Y.3500]: Party which is engaged in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer, or both.

3.1.5 cloud service provider [ITU-T Y.3500]: Party which makes cloud services available.

3.1.6 inter-cloud computing [ITU-T Y.3511]: The paradigm for enabling the interworking between two or more cloud service providers.

NOTE – Inter-cloud computing is also referred as inter-cloud.

3.1.7 metadata [ITU-T M.3030]: Data that describes other data.

3.1.8 role [ITU-T Y.3502]: A set of activities that serves a common purpose.

3.1.9 product catalogue [ITU-T Y.3502]: A listing of all the cloud service products which cloud service providers make available to cloud service customers.

3.1.10 service catalogue [ITU-T Y.3502]: A listing of all the cloud services of a particular cloud service provider.

3.1.11 service management interface (SMI) [ITU T Y.3521]: Interface that provides a set of management capabilities exposed by a cloud service through which the cloud service can be managed.

NOTE – For additional details of SMI concepts, see [ITU T Y.3520] and [b-TMF TR198].

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 functional interface: Interface that provides a set of functional capabilities exposed by a cloud service through which the cloud service can be consumed.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CSC	Cloud Service Customer
CSN	Cloud Service Partner
CSP	Cloud Service Provider
CSU	Cloud Service User
CT	Communications Technology
E2E	End-to-End
FI	Functional Interface
IT	Information Technology
OSS	Operational Support Systems
QoS	Quality of Service
SMI	Service Management Interface
WSDL	Web Services Description Language

5 Conventions

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

In the body of this Recommendation and its appendixes, the words shall, shall not, should, and may sometimes appear, in which case they are to be interpreted, respectively, as is required to, is prohibited from, is recommended, and can optionally. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative are to be interpreted as having no normative intent.

6 Overview of E2E cloud service lifecycle management

Nowadays, cloud computing technologies are widely used in both information technology (IT) and communications technology (CT) industries. Telecommunication operators use cloud-based technologies to deliver cloud services to their users as well as to leverage their telecommunication services and network. This allows for automation and acceleration provisioning of cloud services across cloud and non-cloud facilities. Therefore, effective cloud service lifecycle management becomes one of the most important challenges from telecommunication operators' perspectives.

Cloud service lifecycle management integrates and optimizes processes such as service provisioning, service assurance, service fulfilment, service charging and service change management for particular workloads respecting relevant governance and polices.

In both telecommunication and cloud computing environments, cloud service lifecycle management has to be considered in an E2E manner which means service lifecycle management chains across cloud and non-cloud facilities. In practice, cloud service lifecycle management could be achieved by using a service management interface (SMI) based common model for E2E cloud computing management supported by operational support systems (OSS), see [ITU-T Y.3521].

The OSS encompass the set of operational related management capabilities, including service catalogue, provisioning, monitoring and reporting, service policy management, service automation, etc., in order to manage and control cloud services offered to cloud service customers (CSCs), see [ITU-T Y.3502]. OSS realize the required E2E cloud service lifecycle management functionalities by using service management interfaces (SMIs). These operational related management capabilities can help to achieve the service lifecycle management objective with the pre-defined distributed metadata in each stage.

The consistent approach to service lifecycle management includes representative definitions for the particular stages which cloud services pass through. This is based on a lifecycle management metadata model, which can hold all the data about a service throughout its lifecycle.

Cloud service lifecycle management consists of three parts:

1) service dependencies management: represents resources that are prerequisites for the service to function;
2) service lifecycle management stages: represents stages through which cloud service passes over lifecycle management;
3) additional information about the service management interface: placeholder for additional information but otherwise undefined.

The development of an E2E cloud service lifecycle management process is based on the following elements interacting with each other:

1) service catalogue, see [ITU-T Y.3502], [ITU-T Y.3521];
2) service inventory, see [ITU-T Y.3521];
3) SMI, see [ITU-T Y.3521].

6.1 Cloud service lifecycle metadata

The cloud service capabilities are exposed and consumed through the functional interfaces (FIs) of the service while the management or operations of the service are available through the SMI.

The cloud service capabilities may participate/contribute in many different product offerings that are delivered to CSCs. They may also have different configuration constraints and policies due to constraints from distinct implementation technologies and CSCs' devices that the service is delivered through.

These complicated re-design, re-configuration and re-deployment problems can be addressed through the cloud service lifecycle metadata, which represents all of the lifecycle aspects of the virtualized elements, as expressed in the form of logical objects within a defined model space.

The alignment between elements in the defined model and the real world can be achieved by tools which can address service dependency and drive the required actions based on the metadata associated with the modelled elements. This approach allows a new service to be created with changes only in metadata and minimal modifications. Therefore, the lifecycle metadata can be regarded as the linkage between design time and execution time. From the point of view of cloud service developers (see [ITU-T Y.3502]), FIs and SMIs may only be described in common service languages such as web services description language (WSDL) or web service implementation environment. The aim of this is to define the SMI operations that all services can understand. Therefore, cloud service lifecycle metadata can be designed to capture the cloud service dependencies and service properties to support multi-cloud management.

In order to support consistent management, business process automation and CSC experience, cloud services should understand a set of operations requirements. The word "understand" means that, for example if there is a request for a SMI to configure a service, then the SMI may:

1) intelligently perform the steps required to configure the service per its operation environment, or
2) transfer the request to other applications/services to perform the request, or
3) simply return to the management application that there is no operation or capability to support this function.

Therefore the cloud service compatibility can be provided in any of the following forms:

1) new service component that is implemented by supporting the SMI specification and metadata to be defined;
2) cloud service wrapper on existing service components;
3) cloud service proxy where it transfers the actual operation tasks to other application/service components.

6.2 Cloud service lifecycle management framework

E2E cloud computing management is the capability to manage services and resources (addressing fulfilment, assurance and repositories) of single or multiple cloud services spanning across one or more cloud service providers (CSPs), see [ITU-T Y.3521]. The common model for E2E cloud computing management is based on SMIs. The SMI based approach provides a means to allow consistent E2E management of cloud computing services exposed by and across, different domains of CSPs. Figure 6-1 depicts a conceptual framework of E2E cloud service lifecycle management.

As the Figure 6-1 shows, the E2E cloud service lifecycle management system interacts with CSC and other E2E cloud service lifecycle management systems as follows:

1) CSC can take an action (function) to search for a product (see "Product1" in Figure 6-1) in a self-service fashion (see clause 7.2). In fact, "Product1" is provided by CSP1 and it consists of three services: "Service1", "Service2" and "Service3". The "Service1" and "Service2" are provided by CSP1 while "Service3" is provided by CSP2. After the provisioning process, the CSC can access the E2E service management functions provided by CSP1 and the function of the services can be accessed through the FI provided by CSP1 and CSP2 respectively.
2) The E2E cloud service lifecycle management system performs cloud service lifecycle management through SMIs in domains as follows:
    a) Defining services: all services need to be defined according to their role and what they offer.
    b) Building cloud service catalogue: the cloud service catalogue contains a list of services of a particular CSP. Besides the definition of the service, many attributes such as who can use this service, resource configurations, service levels, processes, networking options, constraints, etc. can be defined and provided through a service catalogue.

c) Management of policy: CSCs require the ability to set policies for which cloud services are configured and managed i.e., controls over who has access to cloud assets, periodic and on-demand logging and reporting.

d) Managing self-service portal: a self-service portal can be managed by a CSP to provide a product catalogue and to take CSCs' requests and offer a degree of control.

e) Configuring: cloud services can be configured for provisioning and use.

f) Provisioning service: cloud service should be provisioned automatically according to CSCs' requests.

g) Composition/orchestration of services: multiple cloud services may need to be composed into a single cloud service.

h) Service decommissioning: for the best utilization of resources, when a cloud service (or resource) is suspended, it should be managed by freeing the associated resources. Decommissioning can be achieved on-demand, when a request from a CSC occurs or according to a schedule.

i) Charging: according to the policy, time of use and service type, charging information can be provided.

3) E2E cloud service lifecycle management system implemented by CSP1 can interact with E2E cloud service lifecycle management system implemented by CSP2 through the SMIs between CSPs as shown in Figure 6-1.

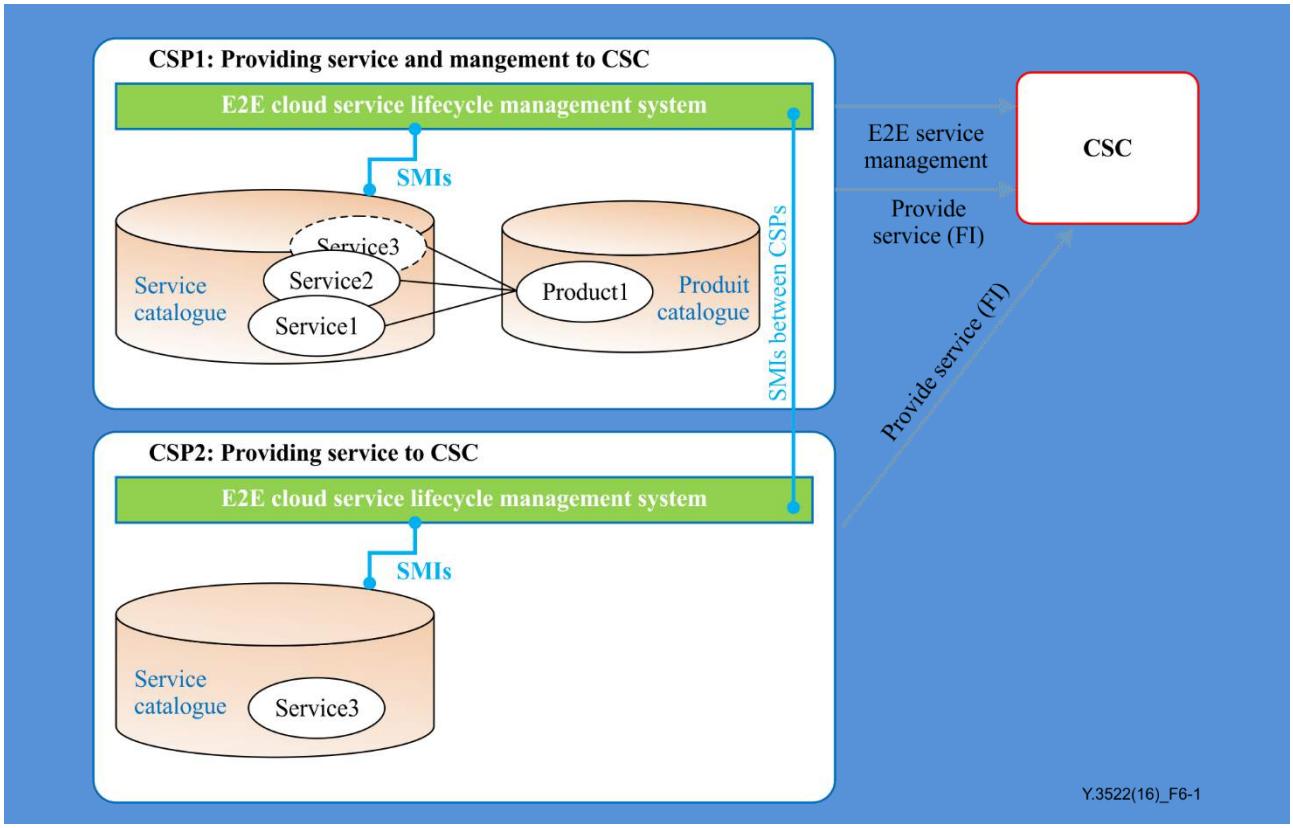


Figure 6-1 – E2E cloud service lifecycle management framework

6.3 Cloud service lifecycle management stages

A cloud service is managed differently in the various stages of its lifecycle. At a high level view, the lifecycle of the cloud service includes four stages: design, deployment, operation and retirement. The term stage is used to designate the various steps in this overall process. Particular tasks in each stage and how to control the level of independence or interaction from one stage to another stage vary from one organization to another.

The tasks in each stage depend on development process considerations (e.g., software development, testing, deployment, etc.) and operational or business considerations (e.g., how a software component becomes a service in the organization and what are the resulting constraints that are then imposed on the software). Such considerations are part of CSP operational style. This clause presents the basic stages description below but in reality, the involved roles and implementation will vary based on the actual conditions.

The cloud service lifecycle management stages are as follows:

1) Stage 1: Design

The service design metadata is built or the existing one is modified by creating new versions or variants in order to capture at the service level the necessary artefacts to support the business considerations.

During the design stage, the necessary service process specification, template, rules, etc. are created and developed for the operation stage. Policies and their enforcement points are also defined for different service conditions.

2) Stage 2: Deployment

The more specific service deployment metadata specialized from the same service design metadata is built. It is typically done by associating specific values or value ranges for each invariant non-functional characteristic. Several sets of service deployment metadata associated with the same service design metadata constitute in a sense a specific family of related service deployment metadata. These service deployment metadata sets will be mapped to different product offerings and will be used as essential entry points during the fulfilment process.

3) Stage 3: Operation

This stage covers all the activities related to the actual instantiation, monitoring, analysis and feedback to design stage of each service. The management tasks of this stage actually involve two aspects:

a) the cloud service itself (seen as a coordinated set of resources in the execution environment from one or several domains);

b) the cloud service operation metadata, which is the unique representation of the service in the management infrastructure of the CSP.

The operation stage includes the service instantiation and delivery process, during which, the designed templates and policies are distributed to the involved roles. The service is instantiated based on CSC's request and CSP's infrastructure condition. The monitoring control mechanism is set up along with the service instantiation.

The automation of configuration is also provided in this stage, including the initial and subsequent changes. To achieve automation, the inventory, monitoring and control functions are activated.

During the whole operation stage, the monitoring activities are performed via event listening; computing analysis is enforced based on data collection. The event, requiring healing and/or scaling, is published, based on pre-defined policies. The actions (healing and/or scaling) are preformed to implement the changed demands.

Based on the analytical data obtained during the operation stage, the patterns governing usage, thresholds, events, policy effectiveness, etc., are discerned and the feedback necessary to effect changes in the design stage is enabled.

4) Stage 4: Retirement

Triggered by the end of the contractual agreement between CSC and CSP, this stops the monitoring and usage activities and releases the resources and components associated with the cloud service resulting in its disappearing. Note that the retirement process does not necessarily mean that the associate service instance is removed from the service inventory. The CSP may want to keep the service operation metadata in "unconfigured" state in its management infrastructure.

A conceptual cloud service will therefore evolve throughout stages such as those described above. This may affect the service lifecycle metadata as structure (e.g., adding a new element), or as value (e.g., modifying the current value of an element or attribute in the metadata associated with the service). Hence cloud service lifecycle metadata representation evolves with cloud service lifecycle stages while the stages essentially represent the different steps a service would be subject to, from design stage to retirement stage.

6.4 Relationship with cloud computing reference architecture

The cloud computing reference architecture, see [ITU-T Y.3502] provides an architectural framework that is effective for describing the cloud computing roles, sub-roles, cloud computing activities, cross-cutting aspects, as well as the functional architecture and functional components of cloud computing. Although the cloud computing reference architecture does not mention the cloud service lifecycle management in the activities and functional architecture, some of its functional components can be used in different cloud service lifecycle management stages. For example, the subscription management functional component in cloud computing reference architecture handles subscriptions from CSC to particular cloud services, aiming to record new or changed subscription information from CSC and ensure the delivery of the subscribed service(s) to CSC. In addition the operation stage in the cloud service lifecycle covers all the activities related to the actual creation and monitoring of each service, which includes service subscription. Therefore the subscription management functional component can be used in operation stage.

Figure 6-2 illustrates the relationship between E2E cloud service lifecycle stages and functional components of cloud computing reference architecture.

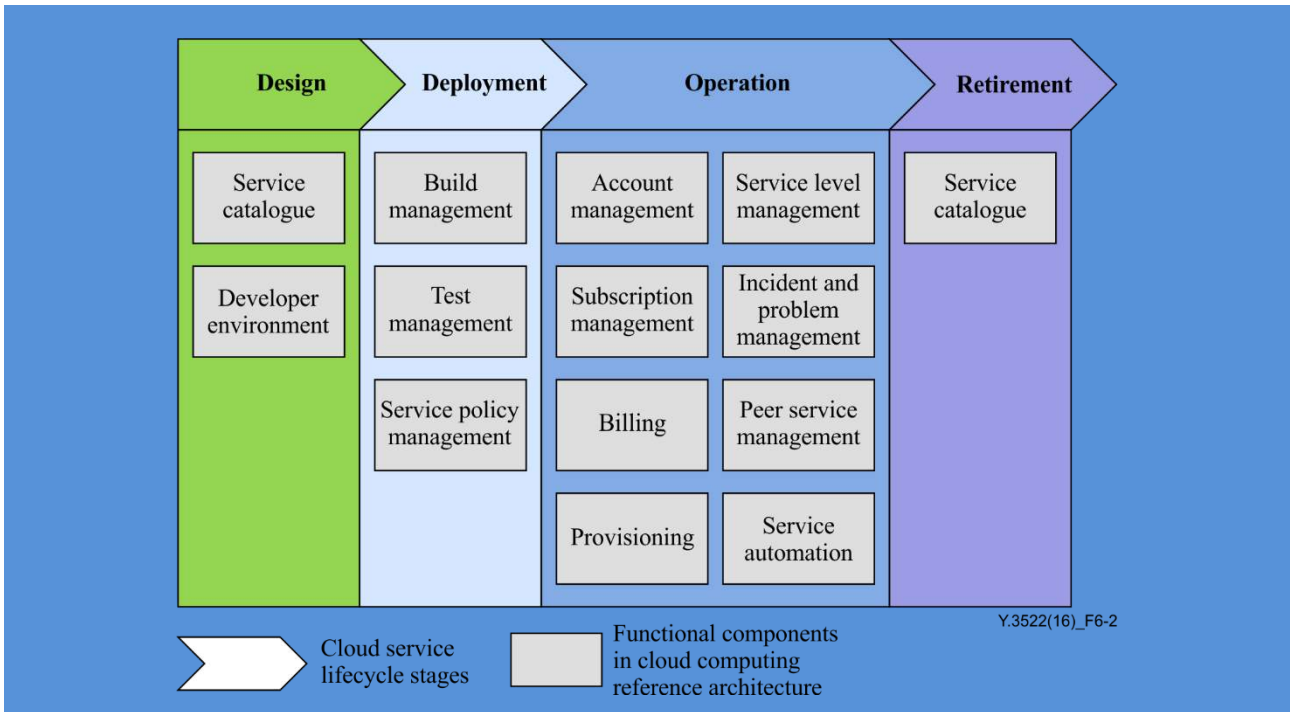


Figure 6-2 – Relationship E2E cloud service lifecycle stages and functional components of cloud computing reference architecture

7 E2E cloud service lifecycle management functional requirements

This clause provides requirements of E2E cloud service lifecycle management derived from the use cases described in Appendix I.

7.1 Service management interface

It is recommended that the CSP provides SMI between cloud services and an E2E cloud service lifecycle management system.

It is recommended that the CSP provides management functionalities of its own cloud service to others CSPs through SMI between CSPs.

7.2 Self-service

It is recommended that the CSP provides an easy method (web portal or other automated approaches) to discover, purchase, configure, deploy, activate and deactivate a service and to check service status to the CSC.

7.3 Service maintenance

It is recommended that the CSP provides automated software enabled cloud services for continuous service maintenance to manage stability and availability of its service.

7.4 Reporting

It is recommended that the CSP provides functions to report (according to local laws and regulations) service health condition, performance, security, geo-location of services, events and other related activities which affect E2E cloud service performance.

7.5 Composite applications or mash-ups

It is recommended that the CSP provides functions to support the rapid delivery of cloud services that are delivered as composite apps, or mash-ups built from multiple services implemented by multiple cloud providers residing in different domains.

7.6 Traditional business processes

It is recommended that the CSP provides functions to support the application of traditional business processes associated with administration, provisioning/configuration, service assurance and charging /billing/settlement involved across inter-clouds residing in different domains.

7.7 Decommissioning

It is recommended that the CSP provides automatic de-commissioning of service resources either based on original service request expiration date or CSC decommission request initiated while the service is running.

7.8 Policy

It is recommended that the CSP provides a set of policies for cloud service access and control.

7.9 Lifecycle stage management

It is required that the CSP provides the ability to run the given service through its lifecycle stages and offers the needed functionality at every step of the process.

7.10 Service automation and continuous delivery

It is required for the CSP to enable automated response to deal with the demand variations and offer necessary feedback to effect changes in the iterative design, by monitoring the service during its operation in order to provide the necessary service automation and continuous delivery without human intervention.

7.11 Metadata management

It is required that the CSP provides metadata schema to support the dynamicity of the services by capturing the service dependencies and service properties at a per-instance level.

8 Security considerations

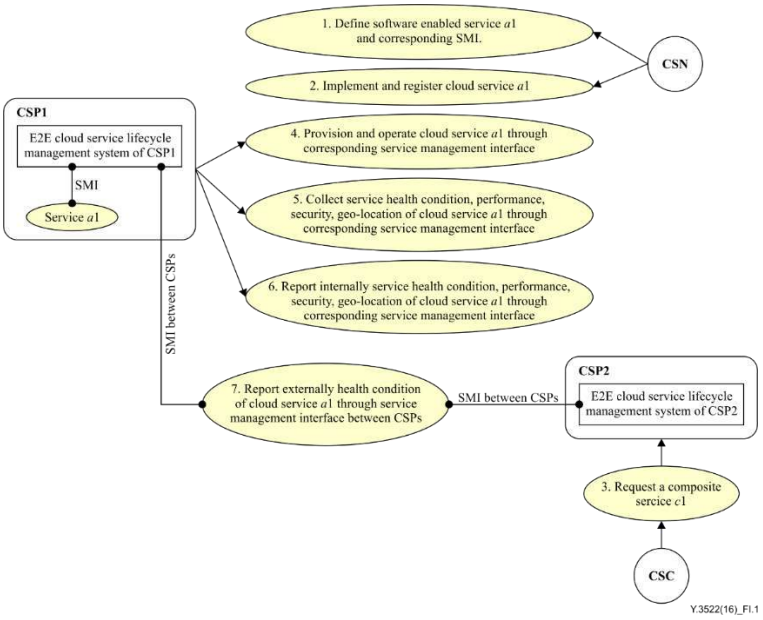
Security aspects for consideration within the cloud computing environment are addressed by security challenges for the CSPs as described in [ITU-T X.1601]. In particular, [ITU-T X.1601] analyses security threats and challenges and describes security capabilities that could mitigate these threats and meet the security challenges.

Appendix I

E2E cloud service lifecycle management use cases

(This appendix does not form an integral part of this Recommendation.)

I.1 Service management interface

Title	Service management interface
Description	CSP1 and CSP 2 established an inter-cloud relationship. Each of them has their own E2E cloud service lifecycle management system inside. CSP1 defines a software enabled service and provides the corresponding service management interface (SMI). CSN makes use of the SMI capabilities provided by CSP1 and develops a new implementation of cloud service a1. CSN registers the developed cloud service a1. The status, availability, performance and/or delay time of a service a1 can be collected through SMI. The CSP1 provides his cloud service a1 to CSP2. CSC requests a composite service c1 to CSP2. This composite service includes the a1 service offered by CSP1 which provides a service and management to CSC. The E2E cloud service lifecycle management system of CSP1 provisions and operates service a1 through its SMI. The E2E cloud service lifecycle management system of CSP1 collects (according to local laws and regulations) service health condition, performance, security, geo-location and events results of the service a1through its SMI. The E2E cloud service lifecycle management system of CSP1 reports (according to local laws and regulations) service health condition, performance, security, geo-location of the service a1 events results internally to CSP1. The E2E cloud service lifecycle management system of CSP1 can report the service health condition of service a1 externally to CSP2 through SMI between CSPs .
Roles	CSP, CSC, CSN
Figure (optional)	

Pre-conditions (optional)	
Post-conditions (optional)	– The status, availability, performance and/or delay time of cloud service can be collected through SMI. – The E2E cloud service lifecycle management system of CSP1 reports internally service health condition, performance, security, geo-location of cloud service a1 through corresponding SMI. – The E2E cloud service lifecycle management system of CSP1 reports externally service health condition of cloud service a1 o CSP2 through SMI between CSPs.
Derived requirements	– Service management interface (refer to clause 7.1) – Service Management Interface between CSPs (refer to clause 7.1) – Reporting (refer to clause 7.4)

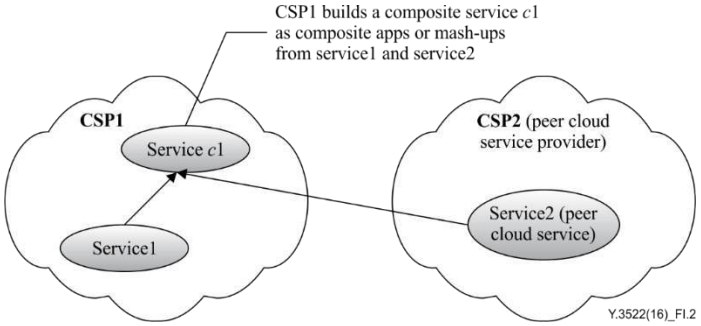
I.2 Self-service use case

Title	Self-service use case
Description	CSP provides cloud services to the market. For improvement of CSC experiences, the CSP provides self-service method to CSCs (e.g., web portal or other automated approaches) to discover, purchase, configure, deploy, activate and deactivate cloud service and to check cloud service status.
Roles	CSP, CSC
Figure (optional)	/
Pre-conditions (optional)	/
Post-conditions (optional)	– The self-service method is provided to CSCs to discover, purchase, configure, deploy, activate and deactivate cloud service and to check cloud service status.
Derived requirements	– Self-service (refer to clause 7.2)

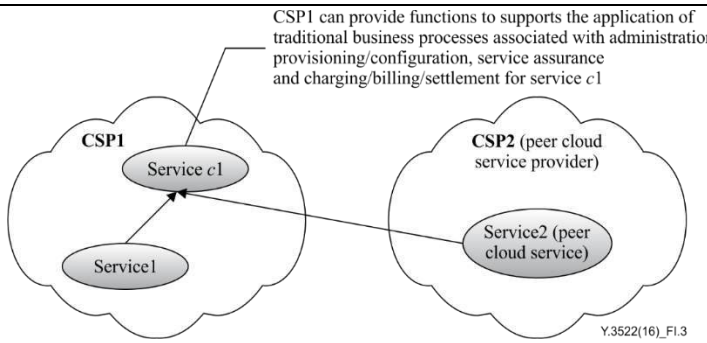
I.3 Service maintenance use case

Title	Service maintenance use case
Description	A CSP provides cloud services to the market. For the stability and availability of its service, periodic maintenance is needed. For a good customer experience, the maintenance cannot result in a long suspension and deactivation of a service. Therefore it is required that CSP can provide automated software enabled cloud services to shorten the maintenance time.
Roles	CSP
Figure (optional)	/
Pre-conditions (optional)	– The CSP can provide automated software enabled cloud services.
Post-conditions (optional)	– The duration of suspension and deactivation is reduced markedly.
Derived requirements	– Service maintenance (refer to clause 7.3)

I.4 Composite applications or mash-ups use case

Title	Composite applications or mash-ups use case
Description	CSP1 builds cloud service c1 as composite apps, or mash-ups from service1 delivered by CSP1 and sevice2 delivered by CSP2.
Roles	CSP
Figure (optional)	
Pre-conditions (optional)	– Service1 delivered by CSP1. – Service2 delivered by CSP2.
Post-conditions (optional)	– A composite service c1 is built from service1 and service2.
Derived requirements	– Composite applications or mash-ups (refer to clause 7.5)

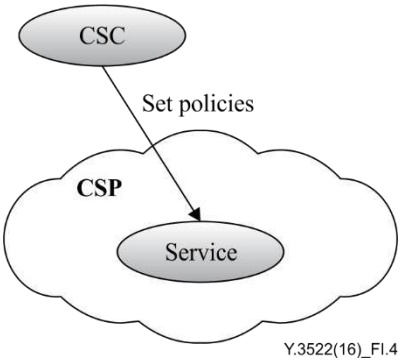
I.5 Traditional business processes use case

Title	Traditional business processes use case
Description	CSP1 builds a composite service c1 from service1 delivered by CSP1 and sevice2 delivered by CSP2. CSP1 can provide functions to support the application of traditional business processes associated with administration, provisioning/configuration, service assurance and charging /billing/settlement for service c1.
Roles	CSP
Figure (optional)	
Pre-conditions (optional)	– CSP1 builds a composite service c1 from service1 delivered by CSP1 and sevice2 delivered by CSP2.
Post-conditions (optional)	– CSP1 can provide functions to support the application of traditional business processes associated with administration, provisioning/configuration, service assurance and charging /billing/settlement for service c1.
Derived requirements	– Traditional business processes (refer to clause 7.6)

I.6 Decommissioning use case

Title	Service decommissioning use case
Description	A CSP provides cloud services to the market. When an original service request passes its expiration date or a user decommission request initiated while the service is running, the resources of this service should be decommissioned automatically.
Roles	CSP
Figure (optional)	/
Pre-conditions (optional)	– An original service request passes its expiration date or a user decommission request initiated while the service is running.
Post-conditions (optional)	– The service resources have been decommissioned automatically.
Derived requirements	– Decommissioning (refer to clause 7.7)

I.7 Policy use case

Title	Policy use case
Description	A CSP provides some kind of cloud services to the market. The CSC of its service want to have the abilities to control who can access to cloud assets, plus both periodic and on-demand logging and reporting. Therefore the CSP is required to provide functions to support the CSC's ability to set policies for doing this.
Roles	CSP, CSC
Figure (optional)	
Pre-conditions (optional)	CSC can set policies on the service.
Post-conditions (optional)	The policies of the service have been set successfully.
Derived requirements	– Policy (refer to clause 7.8)

I.8 Lifecycle stage management use case

Title	Lifecycle stage management use case
Description	A CSP provides some kind of cloud services to the market. For a better management for its services, the CSP is required to provide the ability to run the given service through its lifecycle stages and offers the needed functionality at every step of the process.
Roles	CSP
Figure (optional)	/
Pre-conditions (optional)	/
Post-conditions (optional)	/
Derived requirements	– Lifecycle stage management (refer to clause 7.9)

I.9 Service automation and continuous delivery use case

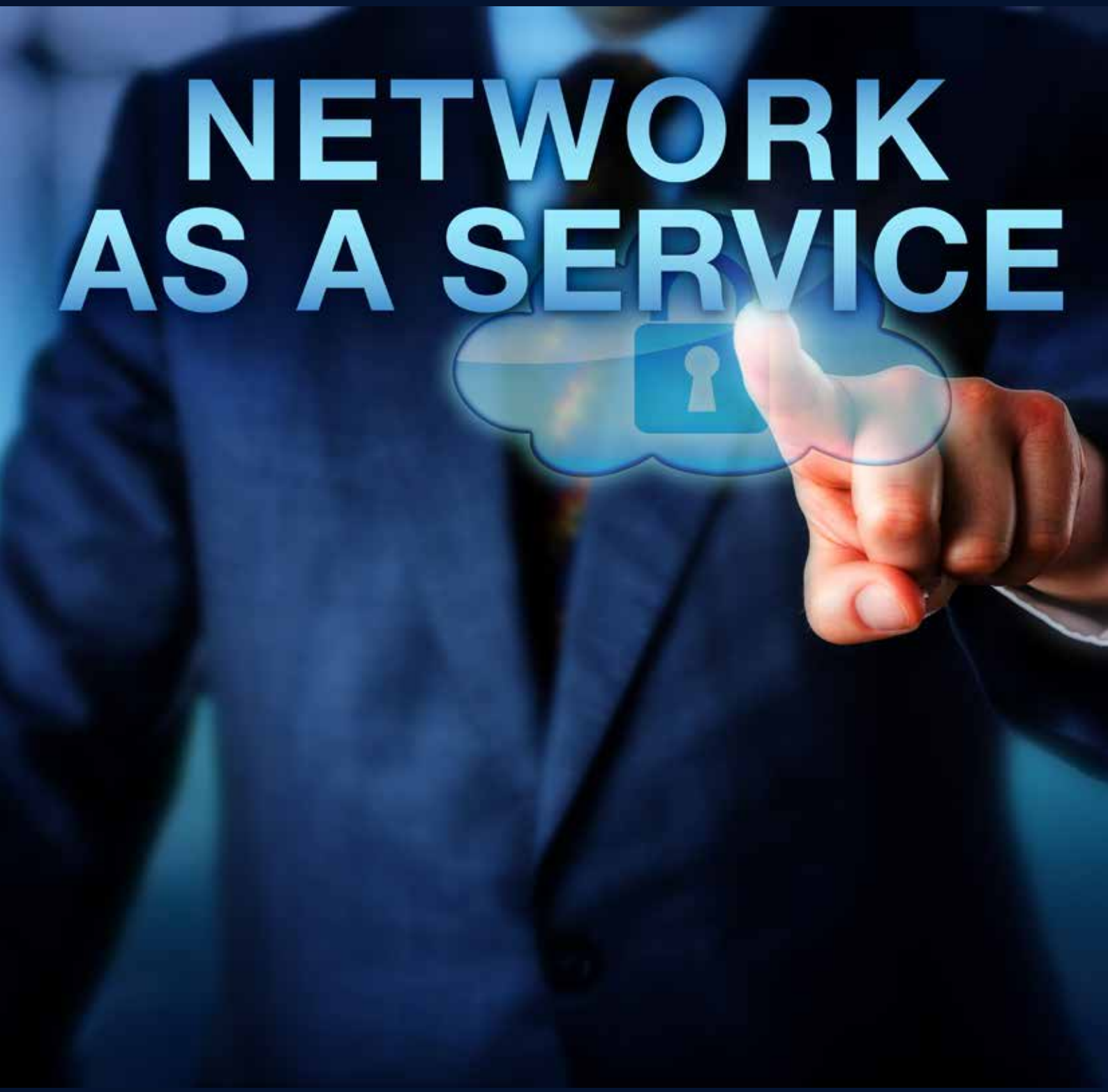
Title	Service automation and continuous delivery use case
Description	A CSP provides cloud services to the market. Because of the continuous changing of the market and CSC's requirements, the design of the cloud service should be an iterative process. By monitoring the service during its operation, the demand variations should be responded to automatically and the necessary feedback to effect changes should be offered to the service designer.
Roles	CSP, CSC
Figure (optional)	/
Pre-conditions (optional)	/
Post-conditions (optional)	/
Derived requirements	– Service automation and continuous delivery (refer to clause 7.10)

I.10 Metadata management use case

Title	Metadata management use case
Description	A CSP provides cloud services to the market. According to market requirement changes, it is needed to adjust the already existing cloud services. Therefore, a robust schema like metadata which can be distributed in each stage needs to be provided.
Roles	CSP
Figure (optional)	/
Pre-conditions (optional)	/
Post-conditions (optional)	CSP can support new cloud service creation with minimal modifications.
Derived requirements	– Metadata management (refer to clause 7.11)

Bibliography

[b-TMF TR198] TM Forum TR198, *Multi-Cloud Service Management Pack – Simple Management API (SMI) Developer Primer and Code Pack, Release 2.2*. https://www.tmforum.org/?s=TR198


NETWORK
AS A SERVICE

Metadata framework for NaaS service lifecycle management

Recommendation ITU-T Y.3523

(08/2019)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Summary

Recommendation ITU-T Y.3523 specifies the metadata framework for Network as a Service (NaaS) service lifecycle management in a closed-loop automation environment. This Recommendation is an extension to Recommendations ITU-T Y.3512 and ITU-T Y.3515 as the NaaS series Recommendations. It provides the metadata framework for NaaS service lifecycle management with a highlight on a NaaS operational policy framework.

Keywords

Closed-loop automation, lifecycle management, metadata framework, NaaS service, NaaS service operational policy framework.

Table of Contents

1 Scope

This Recommendation provides the metadata framework for the closed-loop automation lifecycle management of Network as a Service (NaaS) service, specifically in the environments of development and operations (DevOps) and continuous integration/continuous delivery (CI/CD). This Recommendation covers the following aspects:

– general description of metadata for NaaS service lifecycle management;

– metadata in NaaS service;

– metadata framework for NaaS service lifecycle management;

– NaaS service operational policy framework.

This Recommendation also provides Appendix I describing:

– metadata applicability in NaaS service lifecycle management.

NOTE 1 – The objective in defining a metadata framework of NaaS service lifecycle management is not to invent new metadata, but rather to make the existing metadata interoperable and integrated in the closed-loop automation management of NaaS service, especially in the environments of DevOps and CI/CD.

NOTE 2 – "Metadata" in this Recommendation refers to NaaS service data model, NaaS service operational policy data model and NaaS resource data model.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing*.

[ITU-T Y.3512] Recommendation ITU-T Y.3512 (2014), *Cloud computing – Functional requirements of Network as a Service*.

[ITU-T Y.3515] Recommendation ITU-T Y.3515 (2017), *Cloud computing – Functional architecture of Network as a Service*.

[ITU-T Y.3522] Recommendation ITU-T Y.3522 (2016), *End-to-end cloud service lifecycle management requirements*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 cloud computing [b-ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications and storage equipment.

3.1.2 cloud service [b-ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.3 cloud service customer [b-ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

NOTE – A business relationship does not necessarily imply financial agreements.

3.1.4 cloud service provider [b-ITU-T Y.3500]: Party which makes cloud services available.

3.1.5 Network as a Service (NaaS) [b-ITU-T Y.3500]: Cloud service category in which the capability provided to the cloud service customer is transport connectivity and related network capabilities.

3.1.6 network function [ITU-T Y.3515]: A function of a network infrastructure whose external interfaces and functional behaviour are well specified.

NOTE – Examples of network functions include network switches and network routers.

3.1.7 network service [ITU-T Y.3515]: A collection of network functions with a well specified behaviour.

NOTE – Examples of network services include content delivery networks (CDNs) and IP multimedia subsystem (IMS).

3.1.8 software-defined networking [b-ITU-T Y.3300]: A set of techniques that enables to directly program, orchestrate, control and manage network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 NaaS service operational policy administration point (NPAP): An entity in the Network as a Service (NaaS) service operational policy framework that administrates the policies.

3.2.2 NaaS service operational policy decision point (NPDP): An entity in the Network as a Service (NaaS) service operational policy framework that makes authorization decisions and distributions of the policies.

3.2.3 NaaS service operational policy enforcement point (NPEP): An entity in the Network as a Service (NaaS) service operational policy framework that implements the decisions of NPDP (3.2.2).

3.2.4 NaaS service operational policy information point (NPIP): An entity in the Network as a Service (NaaS) service operational policy framework that stores the policies.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CI	Continuous Integration
CD	Continuous Delivery
CDN	Content Delivery Network
CE	Customer Edge
CSC	Cloud Service Customer
CSP	Cloud Service Provider
DevOps	Development and Operations
ECA	Event, Condition and Action
IMS	IP Multimedia Subsystem
NaaS	Network as a Service
NF	Network Function
NPAP	NaaS Service Operational Policy Administration Point
NPDP	NaaS Service Operational Policy Decision Point
NPEP	NaaS Service Operational Policy Enforcement Point
NPIP	NaaS Service Operational Policy Information Point
NS	Network Service

OSS	Operation Support System
PE	Provider Edge
SDN	Software-Defined Networking
VM	Virtual Machine
VPC	Virtual Private Cloud
VPN	Virtual Private Network

5 Conventions

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

In the body of this Recommendation and its annexes, the words shall, shall not, should, and may sometimes appear, in which case they are to be interpreted, respectively, as is required to, is prohibited from, is recommended, and can optionally. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative is to be interpreted as having no normative intent.

6 General description

The increasing demands on the closed-loop automation management of cloud service causes methods and technology widely used in information technology (IT) like DevOps and CI/CD to be considered and adopted by the telecommunications industry.

The existing initiative aims to enable operational processes and tasks (e.g., delivery, deployment, configuration, assurance and optimization) to be executed automatically, such as ETSI ZSM ISG [b-ZSM], or to provide a comprehensive platform for real-time, policy-driven orchestration and automation of physical and virtual network functions (NFs), like open source open network automation platform (ONAP) [b-ONAP].

According to [ITU-T Y.3522], the complexity of re-design, re-configuration and re-deployment problems can be addressed through cloud service lifecycle management metadata. A new service can be created with changes only in metadata, which can be regarded as the linkage between design time and execution time. Taking NaaS service as an example, whose functional requirements and architecture are well defined in [ITU-T Y.3512] and [ITU-T Y.3515], the related metadata has been defined in several different standards developing organizations (SDOs) and used in many network areas.

However, there is no specification to address the detailed position and function of metadata in the context of the entire closed-loop automation lifecycle management of the NaaS service, whose dependencies and constraints vary unavoidably.

This Recommendation specifies the interoperability and integration of the existing NaaS-related data models as a typical kind of Anything as a Service (XaaS). Although, there are other activities on data models' development on NaaS service aspect (e.g., OASIS TOSCA [b-TOCSA], IETF YANG [b-YANG], OASIS BPEL [b-BPEL]), this Recommendation is focused on specifying the framework with attention on policy aspects, and applicability of data models in closed-loop automation management of NaaS service.

7 Metadata in NaaS service

This clause aims to specify the positions and functions of NaaS service metadata for the entire lifecycle management. The positions of NaaS-related data models are illustrated as shown in Figure 7-1.

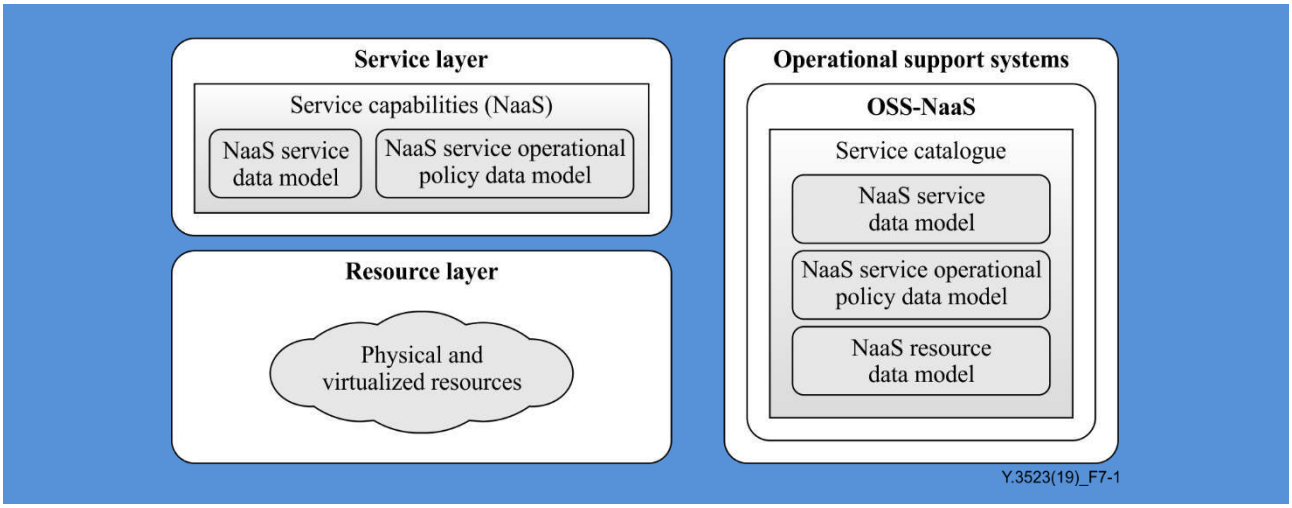


Figure 7-1 – Illustration of NaaS-related metadata positions

Operation support system (OSS)-NaaS service catalogue functional components (see clause 8.3.1 of [ITU-T Y.3515]) includes a listing of all cloud services of NaaS cloud service providers (CSPs) including the relevant NaaS services. NaaS service data model, NaaS service operational policy data model and NaaS resource data model are needed in this functional component for NaaS service instantiation.

The service capabilities (NaaS) functional component (see clause 8.2.3 of [ITU-T Y.3515]) in the service layer provides capabilities exposed to the NaaS cloud service customer (CSC) according to the NaaS service data model and NaaS service operational policy data model selected by the NaaS CSC through business level interactions with the NaaS CSP.

7.1 NaaS service data model

The NaaS service data model (see clause 8.3.1 of [ITU-T Y.3515]) describes the specific network service based on the characteristic of the service that can be used for service delivery, e.g., L3VPN and L2VPN data models under development of the working groups L3SM [b-L3SM] and L2SM [b-L2SM] of IETF.

7.2 NaaS service operational policy data model

The NaaS service operational policy data model (see clause 8.3.1 of [ITU-T Y.3515]) describe high-level network-wide polices for a given NaaS service, which can be input into the network management function (within a software-defined networking (SDN) controller, an orchestrator, or a network element), and combined with the NaaS service data model and mapped into a target configuration of network elements, e.g., generic policy data model described in [b-SUPA] of IETF. The network management function can control the configuration and monitor the network elements and services according to such policies.

7.3 NaaS resource data model

The NaaS resource data model (see clause 8.3.1 of [ITU-T Y.3515]) describes topology of NaaS CSP's resources across different layers and reflects the attributes and operational parameters of given NaaS resources (e.g., network services (NSs), NFs, virtualised resources, physical resources).

7.4 Relationship among metadata in NaaS service

The NaaS service operational policy data model can manage and adjust service behaviours as necessary. The NaaS service operational policy data model and the NaaS service data model have a one-to-many relationship.

The NaaS service operational policy data model can manage and adjust resources behaviour as necessary. The NaaS service operational policy data model and the NaaS resource data model have a one-to-many relationship.

8 Metadata framework for NaaS service lifecycle management

This clause aims to specify the metadata framework in NaaS service lifecycle management by reflecting the interoperability and integration of the NaaS service metadata, especially in the environments of DevOps and CI/CD.

As described in [ITU-T Y.3522], metadata is used in the entire cloud service lifecycle management, from design, deployment, operation, to retirement stages. For NaaS service, closed-loop automation management is achieved by using data models of NaaS service, NaaS service operational policy, and NaaS resource, as a linkage, in the four iterative stages of NaaS service lifecycle management. These four iterative stages can be categorized into design time, including design stage, and runtime execution time, including deployment stage, operation stage and retirement stage.

Figure 8-1 depicts the metadata framework for NaaS service lifecycle management. The metadata of NaaS service is created in design time, and then distributed to runtime execution time to be used in implementing a metadata-driven service deployment, operation and retirement. The feedback from runtime execution time to design time is to help identify the changes needed for the metadata.

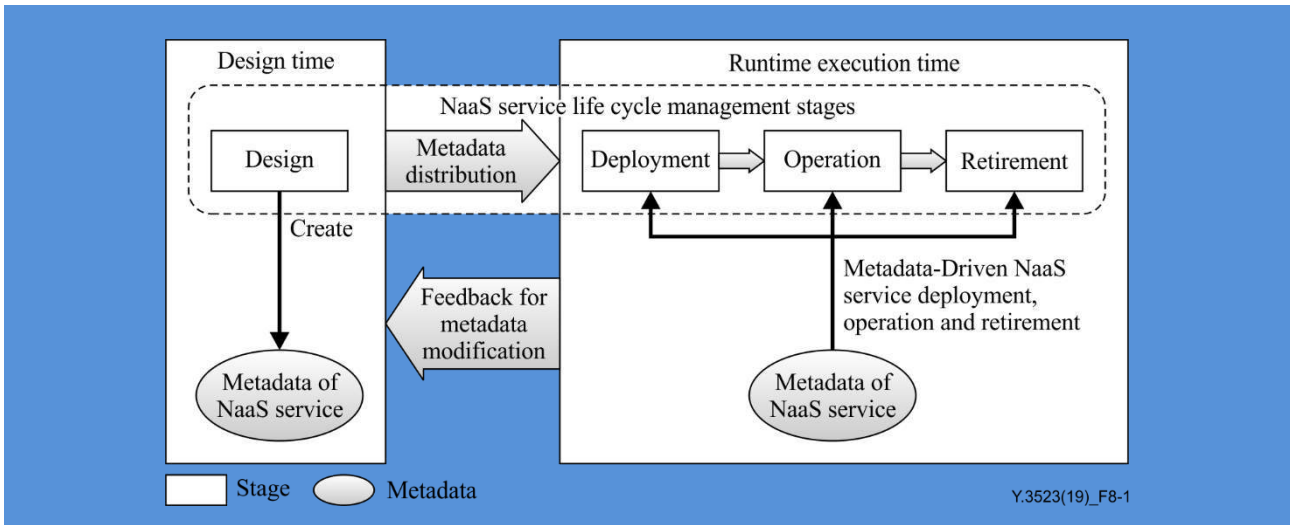


Figure 8-1 – Metadata framework for NaaS service lifecycle management

8.1 Metadata of NaaS service in design time

Models of NaaS service, NaaS service operational policy, and NaaS resource are created and developed in design time for making services and resources available, using modelling tools provided by NaaS CSP. The modelling process will not trigger any NaaS service instantiation in the runtime execution environment until the OSS-NaaS receives a request to do so.

The basic extendable model templates are defined and stored in service catalogue of OSS-NaaS (NaaS service data model and NaaS service operational policy data model) and network controller (NaaS resource data model) during design time and can be configured and extended with additional parameters, parameter value ranges and validation rules according to NaaS CSC's request.

8.2 Metadata of NaaS service in runtime execution time

The modelled NaaS service is instantiated in runtime execution time and the specific NaaS service model and its NaaS service operational policy data model drive the corresponding codes. The active NaaS service is continuously monitored by event listening. The event, requiring healing and/or scaling based on real-time NaaS CSC requests, is responded to based on the associated condition pre-defined in NaaS service operational policy data model.

Based on the monitoring data collected during runtime execution time, the patterns governing usage, thresholds, events, policy effectiveness, etc., are discerned and the necessary feedback to effect modelling changes in design time is enabled.

9 NaaS service operational policy framework

This clause aims to present the NaaS service operational policy framework which consists of elements and functions provided by the CSP and the corresponding procedure.

9.1 Elements of NaaS service operational policy

NaaS service operational policy data models are operated from creation to execution in the NaaS service operational policy framework. The main elements of the NaaS service operational policy framework are described as follows.

9.1.1 NaaS service operational policy administration point

The NaaS service operational policy administration point (NPAP) is responsible for the creation, translation, and validation of new NaaS service operational policy data models, and the modification of existing ones, both during design time and runtime execution time. NaaS service operational policy data models are created with the integration of NaaS service data models.

9.1.2 NaaS service operational policy decision point

The NaaS service operational policy decision point (NPDP) is responsible for the distribution and decisions of NaaS service operational policy data models. Once the NaaS service operational policy data model is initially created or an existing one is modified, the NPDP sends it from the repository to the NaaS service operational policy enforcement point (NPEP) before it is actually needed. In this distributed manner, NaaS service operational policy data models will be available when needed in order to minimize the latency for real-time requests or triggers to the NPDP. In some required cases, NaaS service operational policy data models can be subscribed and automatically updated on the NPEP.

9.1.3 NaaS service operational policy information point

The NaaS service operational policy information point (NPIP) is responsible for storing new NaaS service operational policy data models in the repository which are verified by the NPAP. The existing ones can be retrieved in the repository.

In the repository, NaaS service operational policy data models are grouped by different dimensions, which include, but are not limited to, the corresponding NaaS service data model, the type or category, the lifecycle, the ownership or administrative domain, the geographic area or location, the technology type, the describing language and version, and the security level.

9.1.4 NaaS service operational policy enforcement point

The NPEP is responsible for the enforcement of NaaS service operational policy data models during the runtime execution time.

9.2 Functions of NaaS service operational policy

Table 9-1 provides descriptions of the main functions related to the NaaS service operational policy data model.

Table 9-1 – Functions related with NaaS service operational policy data model

No.	Function	Description
1	Create policy	The CSP creates a NaaS service operational policy data model on the NPAP based on the required policy parameters and the NPIP stores it with the allocated labels which indicates its dimensions.
2	Delete policy	The CSP deletes the specified NaaS service operational policy data model on the NPAP and the NPIP removes it from the repository.
3	Update policy	The CSP updates a NaaS service operational policy data model on the NPAP based on the new policy parameters and the NPIP re-stores it and the original one is overwritten accordingly.
4	Get policy	The NPDP requests the specified NaaS service operational policy data model from the NPIP and gets it from the repository.
5	Distribute policy	The NPDP distributes the specified NaaS service operational policy data model to the NPEP and the NPEP makes the subscription on the NPDP for its update.
6	List policy	The NPIP lists all the NaaS service operational policy data models on demand.
7	Retrieve policy	The NPIP provides the retrieved NaaS service operational policy data models on demand based on the specified retrieval conditions.
8	Enforce policy	The NPEP enforces the NaaS service operational policy data models based on the trigger condition or request.

9.3 Procedure of NaaS service operational policy from creation to enforcement

The interactions among the main elements of NaaS service operational policy framework from creation to enforcement of the policy data model are described as follows in Figure 9-1.

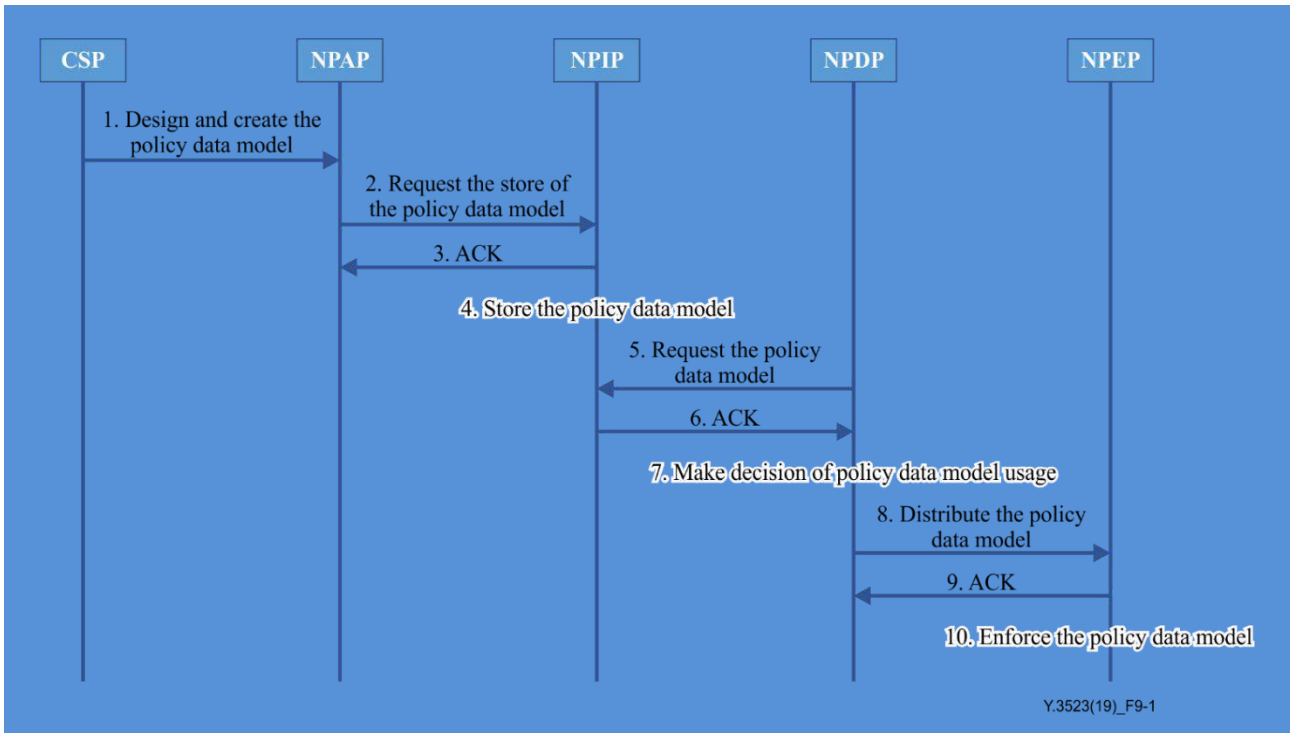


Figure 9-1 – Procedure from creation to enforcement of the NaaS service operational policy data model

1) The CSP designs and creates the NaaS service operational policy data model on NPAP.
2) The NPAP requests the NPIP to store the newly created NaaS service operational policy data model.
3) The NPIP sends an acknowledgement to the NPAP.
4) The NPIP stores the newly created NaaS service operational policy data model in the repository.
5) The NPDP requests the NaaS service operational policy data model from the NPIP for decision.
6) The NPIP sends an acknowledgement to the NPDP.
7) The NPDP decides how to deal with the NaaS service operational policy data model.
8) The NPDP distributes the NaaS service operational policy data model to the NPEP which subscribed it.
9) The NPEP sends an acknowledgement to the NPDP.
10) The NPEP enforces the NaaS service operational policy data model once it is triggered.

10 Security considerations

Security aspects for consideration within the cloud computing environment, including inter-cloud computing, are addressed by security challenges for CSPs as described in [ITU-T X.1601]. [ITU-T X.1601] analyses security threats and challenges, and describes security capabilities that could mitigate these threats and meet the security challenges. This Recommendation does not introduce any new security issues.

Appendix I

Metadata applicability in NaaS service lifecycle management

(This appendix does not form an integral part of this Recommendation.)

This appendix aims to provide applicability examples of NaaS service lifecycle management metadata.

I.1 Virtual private cloud

The manipulation of the virtual private cloud (VPC) network may also affect the configuration of physical networks. For example, when two new virtual machines (VMs) associated to a given VPC are deployed in two different data centres (DCs), the VPC control mechanism needs to generate a virtual private network (VPN) between these two data centres for the internal VPC communications. Therefore, the control mechanism for a VPC should be able to adjust the underlying network at run time when a CSC requests changes to the VPC network or service deployment.

When a CSC moves from one location to another, which is near to another CSP's data centre, and in the case where the network load between these two data centres is low, the CSC's VM(s) should be migrated to the new data centre to allow for a better user experience.

As illustrated by Figure I.1, a VPC corresponds to a combination of cloud computing resources with a VPN infrastructure to give NaaS service CSCs the abstraction of a private set of cloud resources that are transparently and securely connected to their own infrastructure. VPCs are created by taking dynamically configurable pools of cloud resources and connecting them to enterprise sites with VPNs.

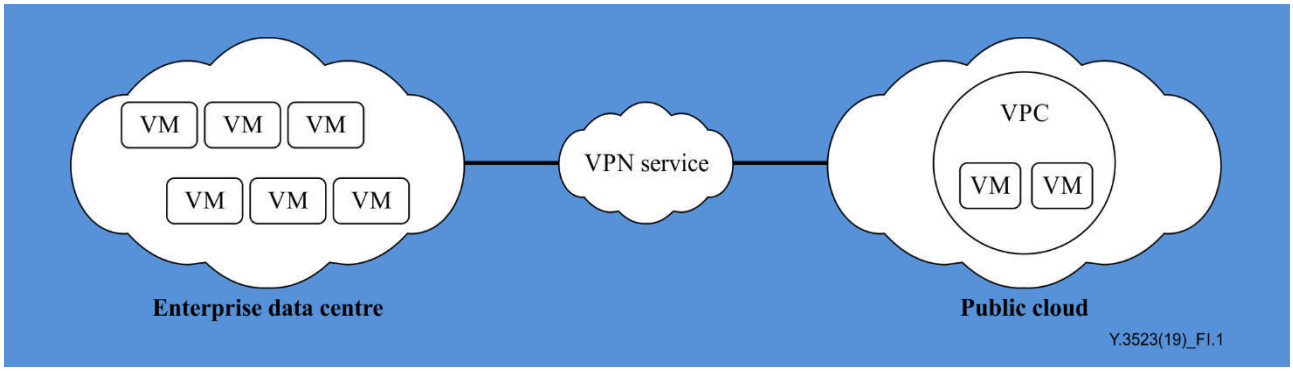


Figure I.1 – Illustration of virtual private cloud

The NaaS resource data model needs to be used in this scenario for modelling the physical nodes and links.

The NaaS service data model, specifically for L3VPN, is needed to model the L3VPN attributes, including, but not limited to: tenant ID, VPN site IDs, VPN type, access bandwidth.

Here, the NaaS policy data model can be described as follows, using event, condition and action (ECA) policy.

– Event: a VPC user's location is changed (near to another DC)
– Condition: network_load(DC_old, DC_new) < threshold
– Action:
  1) migrate the VM to the new data center (DC_new);
  2) update the VPNs connecting the CSC's services.

I.2 Instant VPN

Traditionally, when a NaaS CSP needs to deploy VPN services for an enterprise NaaS CSC, the NaaS CSP will send service staff to the NaaS CSC site to make the wired connection between the customer edge (CE) and

provider edge (PE) devices. The service staff also collects configuration information such as port/frame/slot of PE and the PE ID, and then sends the collected information back to the management system. The management system then configures the network according to this information, as well as the NaaS CSC's information (e.g., bandwidth, SLA). The problem with this approach is that the service staff needs to collect the connection information and feed it back to the management system, and they must make sure that the collected information matches the actual connection. This process is error prone.

New approaches should not count on the physical/geographical information feedback by the service staff and should minimize the operational procedures. The CE should send an authentication request (with credentials) to the PE, and the PE should forward the request to the management system, together with the port/frame/slot on which the request is received, the PE ID, etc. The goal is that NaaS CSP configures a VPN for an enterprise NaaS CSC to connect its enterprise network. The NaaS resource data model needs to be used in this scenario for modelling the physical nodes and links.

The NaaS service data model, specifically for L3VPN, is needed to model the L3VPN attributes, including, but not limited to: tenant ID, VPN site IDs, VPN type and access bandwidth.

Here, the NaaS policy data model can be described as follows, using ECA policy.

– Event: service management system receives a CE request for VPN creation (forwarded by PE);
– Condition: authentication and authorization results are acknowledged;
– Action: configure a VPN based on received requests, including the NaaS CSC's grade and physical information (port/slot/frame/route id, etc.) from which the request is received.

Bibliography

[b-ITU-T Y.3300] Recommendation ITU-T Y.3300 (2014), *Framework of software-defined networking*.

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary*.

[b-BPEL] OASIS BPEL 2.0 (2007), *Web Services Business Process Execution Language Version 2.0.* <http://docs.oasis-open.org/wsbpel/2.0/wsbpel-v2.0.html> (last accessed 28 June 2019)

[b-L2SM] IETF RFC 8466 (2018), *A YANG Data Model for Layer 2 Virtual Private Network (L2VPN) Service Delivery*.

[b-L3SM] IETF RFC 8299 (2018), *YANG Data Model for L3VPN Service Delivery*.

[b-ONAP] ONAP, *Open Network Automation Platform*. https://www.onap.org/ (Referenced 28 06 2019).

[b-SUPA] IETF RFC 8328 (2018), *Policy-Based Management Framework for the Simplified Use of Policy Abstractions (SUPA)*.

[b-TOCSA] OASIS TOSCA 1.0 (2013), *Topology and Orchestration Specification for Cloud Applications Version 1.0.* <http://docs.oasis-open.org/tosca/TOSCA/v1.0/TOSCA-v1.0.html> (last accessed 28 June 2019)

[b-YANG] IETF RFC 6020 (2010), *YANG – A Data Modeling Language for the Network Configuration Protocol (NETCONF)*.

[b-ZSM] ETSI ISG ZSM, *Industry Specification Group Zero touch network and Service Management*. <https://portal.etsi.org/tb.aspx?tbid=862&SubTB=862,863> (last accessed 28 June 2019)

Cloud computing – Functional requirements of inter-cloud data management

Recommendation ITU-T Y.3518

(12/2018)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Summary

Recommendation ITU-T Y.3518 provides the overview of inter-cloud data management and its functional requirements. It describes typical use cases and specifies functional requirements for three aspects, namely inter-cloud data policy, inter-cloud data isolation and protection, as well as inter-cloud data management, which are derived from the corresponding use cases.

Keywords

Inter-cloud; data management; inter-cloud data policy; inter-cloud data isolation and protection.

Table of Contents

1 Scope

This Recommendation provides the overview and functional requirements of inter-cloud data management. This Recommendation consists of:

– the overview of inter-cloud data management;

– functional requirements for inter-cloud data policy;

– functional requirements for inter-cloud data isolation and protection;

– functional requirements for inter-cloud data management.

This Recommendation also provides an appendix describing use cases aimed at deriving the corresponding functional requirements.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing.*

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), *Information technology – Cloud computing – Reference architecture.*

[ITU-T Y.3511] Recommendation ITU-T Y.3511 (2014), *Framework of inter-cloud computing.*

[ITU-T Y.3600] Recommendation ITU-T Y.3600 (2015), *Big data – Cloud computing based requirements and capabilities.*

[ITU-T Y.3601] Recommendation ITU-T Y.3601 (2018), *Big data – Framework and requirements for data exchange.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 cloud service [b-ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.2 cloud service category [b-ITU-T Y.3500]: Group of cloud services that possess some common set of qualities.

NOTE – A cloud service category can include capabilities from one or more cloud capabilities types.

3.1.3 cloud service customer [b-ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

NOTE – A business relationship does not necessarily imply financial agreements.

3.1.4 cloud service provider [b-ITU-T Y.3500]: Party which makes cloud services available.

3.1.5 inter-cloud computing [ITU-T Y.3511]: The paradigm for enabling the interworking between two or more cloud service providers.

NOTE – Inter-cloud computing is also referred as inter-cloud.

3.1.6 Network as a Service (NaaS) [b-ITU-T Y.3500]: Cloud service category in which the capability provided to the cloud service customer is transport connectivity and related network capabilities.

3.1.7 Platform as a Service (PaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer is a platform capabilities type.

3.1.8 Software as a Service (SaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer is an application capabilities type.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 inter-cloud data policy decision point (IDPDP): An inter-cloud environment entity that makes authorization decision and negotiation of inter-cloud data processes and usage.

3.2.2 inter-cloud data policy enforcement point (IDPEP): An inter-cloud environment entity that implements data policy decision of an inter-cloud data policy decision point (IDPDP) (see clause 3.2.1).

3.2.3 inter-cloud data policy information point (IDPIP): An inter-cloud environment entity that stores the data policy.

3.2.4 inter-cloud data policy administration point (IDPAP): An inter-cloud environment entity that administrates data policies.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Program Interface
BSS	Business Support System
CPPL	Compact Privacy Policy Language
CSC	Cloud Service Customer
CSP	Cloud Service Provider
DPL	Data Policy Language
IDPAP	Inter-cloud Data Policy Administration Point
IDPDP	Inter-cloud Data Policy Decision Point
IDPEP	Inter-cloud Data Policy Enforcement Point
IDPIP	Inter-cloud Data Policy Information Point
KPI	Key Performance Indicator
NaaS	Network as a Service
NFV	Network Function Virtualization
OSS	Operational Support System
PaaS	Platform as a Service
SaaS	Software as a Service
SDN	Software-Defined Networking
SW	Software
vHGW	virtual Home Gateway
XML	extensible Markup Language

5 Conventions

In this Recommendation:

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

6 Overview of inter-cloud data management

Nowadays, one of the main challenges for cloud service providers (CSPs) is to ensure credibility of data storage and transport in multi-cloud environments. Inter-cloud data management functions need to consider and reflect security and governance aspects of data handling uniformity and interoperability across different CSPs.

Inter-cloud data categorization in aspects of identification qualifiers and dependency, as well as inter-cloud data annotation, processing and usage, is necessary to attain the data treatment required among multiple CSPs. The appropriate security and access control mechanisms determine access control to inter-cloud data under particular conditions (e.g., temporarily, a certain number of times or related to a particular community and context).

With the development and wide usage of big data-related technologies, more and more data and datasets are stored in geographically distributed and heterogeneous computing environments, also known as inter-cloud environments (e.g., in a high-performance computing scenario). Migrating an application from a centralized or static place to the distributed computing environments may bring the following challenges:

1) transmission of intensive data among different CSPs may cause low data access efficiency;
2) heterogeneous dataset access and sharing may bring extra computation consumption;
3) the necessary and unavoidable maintenance of extensive tracking of metadata, data locations, access control policies, etc.

NOTE – Intensive data transmission and heterogeneous dataset access and sharing-related technologies lie outside the scope of this Recommendation.

[ITU-T Y.3601] specifies the big data exchange framework and requirements based on the big data ecosystem and capabilities specified in [ITU-T Y.3600]. In [ITU-T Y.3601], data exchange is described as a process of receiving source data under a source schema from data source, transforming it into target data under a target schema without altering the representation of source data, and delivering the target data to the data target. This Recommendation focuses on the inter-cloud data management aspects and does not aim to specify any concrete data exchange details. For more information about big data exchange, please refer to [ITU-T Y.3601].

6.1 Inter-cloud data categorization

[b-ISO/IEC 19944] identifies the categories of data that flow across cloud service customer (CSC) devices and cloud services, and can be captured, processed, used and shared. It extends the definitions of CSC data, cloud service-derived data, CSP data and account data. This Recommendation follows the taxonomy of data in [b-ISO/IEC 19944] and focuses on the inter-cloud data aspect. Similarly to [b-ISO/IEC 19944], this Recommendation is not intended to be exhaustive, but is intended to be extensible. It is recommended that the hierarchical relationship based on the four topmost categories defined in [b-ISO/IEC 19944] be maintained.

6.2 Data policy language

The data policy language (DPL) allows CSPs to annotate, manage, process and use CSC or CSP data in an inter-cloud environment (who can do what and when) according to data policies in force. The main challenges for DPL are related to small storage footprint, human readability, detection of conflicts at time of specification, performance and adaptation to new policy statements that come up with emerging inter-cloud services. The DPL expresses inter-cloud data policies for different cloud service categories [e.g., NaaS, SaaS, platform as a service (PaaS)] provided by the CSPs in an inter-cloud environment.

6.3 Inter-cloud data policy-based management

Inter-cloud data policy-based management enables peer CSPs to control and evaluate who can access which inter-cloud data, how to manage inter-cloud data, how to process and use inter-cloud data.

The main elements of data policy-based management in inter-cloud are as follows.

– An IDPDP collects information about available resources and corresponding properties of the peer CSPs to decide which of these CSP can process and use the inter-cloud data from peer CSPs. The functionalities of IDPDP depend on role-based, rule-based and context-based data policies applied in inter-cloud computing.

– An IDPEP is responsible for enforcing the terms of a CSC or CSP access. This enforcement is run-time based on the capabilities of the IDPEP.

– An IDPIP is a repository of information to support the access decision.

– An IDPAP provides inter-cloud administration, management and monitoring of entitlement policies, as well as delegation and integration with inter-cloud information repositories.

Figure 6-1 illustrates how an IDPAP and IDPIP are related with each other to operate data management policies for a data supplier, and shows that an IDPEP, IDPDP and IDPIP cooperate for a data customer to access data based on policies set by the data supplier.

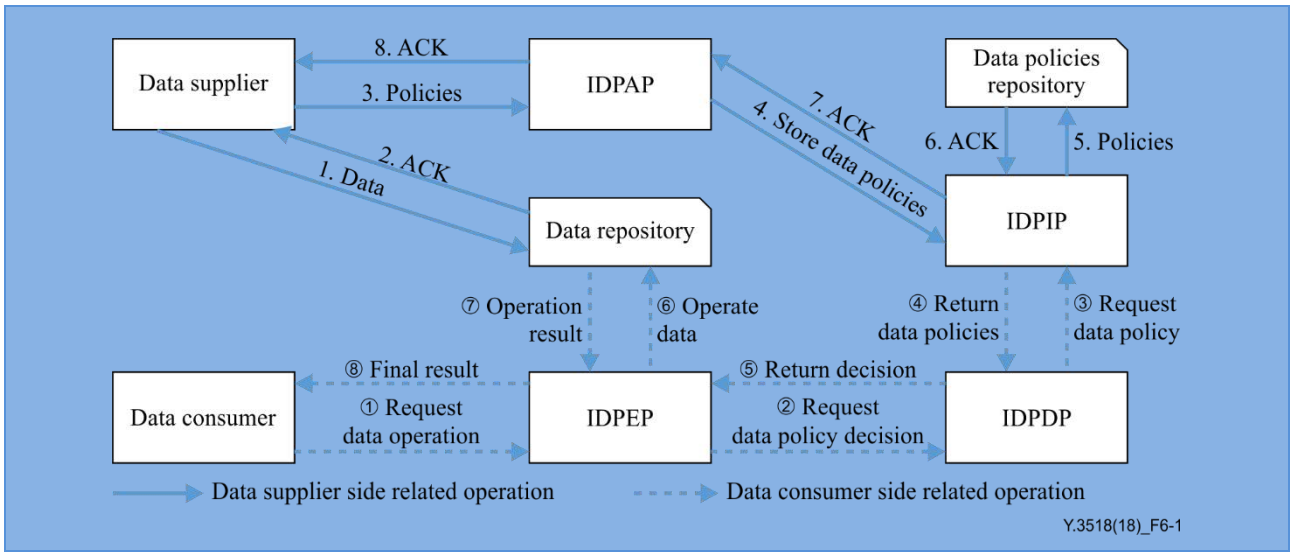


Figure 6-1 – Relationship of main elements in inter-cloud data policy-based management

In Figure 6-1, the data supplier generates and provides data, and also sets the data policies. The data customer uses the data that is provided by the data supplier and processed by policy-based management.

The data supplier side-related operations can be described as the following procedure.

1) The data supplier provides the data to the data repository.
2) The data repository sends an acknowledgement to the data supplier.
3) The data supplier sets the corresponding data policies, which are managed by the IDPAP.
4) The IDPAP requests the IDPIP to store the data policies.
5) The IDPIP stores the data policies in the data policies repository.
6) The data policies repository sends an acknowledgement to the IDPIP.
7) The IDPIP sends an acknowledgement to the IDPAP.
8) The IDPIP sends an acknowledgement to the data supplier.

The data consumer side-related operations can be described as the following procedure.

1) The data consumer requests a data operation from the IDPEP.
2) The IDPEP requests a data policy decision from the IDPDP.
3) The IDPDP requests the specific data policy from the IDPIP.
4) The IDPIP returns the requested data policy to the IDPDP.
5) The IDPDP returns the decision result to the IDPEP based on the collected available resources.
6) The IDPEP performs the data operation based on the data policies.
7) The processed data result is returned to the IDPEP.
8) The IDPEP provides the final results of the data operation to the data consumer.

6.4 Relationship with cloud computing reference architecture

[ITU-T Y.3502] specifies two functional components to support inter-cloud computing, also known as peer service integration (see clause 9.2.5.1.4 of [ITU-T Y.3502]) and peer service management (see clause 9.2.5.3.9 of [ITU-T Y.3502]). [ITU-T Y.3516] identifies an inter-cloud specific extension to the functional components of [ITU-T Y.3502] that are part of integration, security systems, operational support system (OSS) and business support system (BSS) (see clause 8 of [ITU-T Y.3516]). This Recommendation is based on the functions defined in [ITU-T Y.3502] and [ITU-T Y.3516] on inter-cloud computing and does not define or extend any new functions. This Recommendation focuses on data management in the inter-cloud environment based on the establishment of a relationship (pattern) among multiple peer CSPs, including peering, federation and intermediary, which are defined in [ITU-T Y.3511].

7 Functional requirements for inter-cloud data policy

This clause provides the functional requirements for inter-cloud data policy derived from the use cases described in Appendix I.

7.1 Data policy language

It is recommended that the CSP support inter-cloud data policy to satisfy data processing and usage.

It is recommended that the CSP support the DPL to annotate (tagging) cloud workloads.

It is recommended that the CSP support inter-cloud data annotation (tagging) in order to realize the CSC request.

7.2 Inter-cloud data policy administration point

It is recommended that the CSP support the IDPAP to administer data policies in inter-cloud.

7.3 Inter-cloud data policy information point

It is recommended that the CSP support the IDPIP to store the data policy provided by the CSC in inter-cloud.

7.4 Inter-cloud data policy decision point

It is recommended that the CSP support the IDPDP to enforce the data policy on the basis of information collected by the IDPEP about data processing and usage among peer CSPs in inter-cloud.

7.5 Inter-cloud data policy enforcement point

It is recommended that the CSP support the IDPEP to implement the data policy decision of the IDPDP in the inter-cloud environment.

It is recommended that the CSP support the IDPEP to collect information about data processing and usage among peer CSPs in inter-cloud and deliver this information to the IDPDP.

7.6 Inter-cloud data policy monitoring

It is recommended that the CSP support real-time data policy monitoring in inter-cloud to fulfil the data policy provided by the CSC.

7.7 Inter-cloud dynamic data policy management

It is recommended that the CSP support dynamic data policy management in inter-cloud to fulfil the data policy provided by the CSC.

7.8 Inter-cloud autonomic data policy management

It is recommended that the CSP support autonomic data policy management in inter-cloud to fulfil the data policy provided by the CSC.

7.9 Inter-cloud cognitive data policy management

It is recommended that the CSP support cognitive data policy management in inter-cloud to fulfil the data policy provided by the CSC.

8 Functional requirements for inter-cloud data isolation and protection

This clause provides the functional requirements for inter-cloud data isolation and protection derived from the use cases described in Appendix I.

8.1 Datasets placement policies among different CSPs

It is recommended that CSPs support dataset placement policies for data-intensive applications in geographically distributed data centres.

NOTE 1 – The conditions of placement policy include, but are not limited to, the time cost of data transmission, storage space, network performance and dataset dependencies.

NOTE 2 – Dataset placement policies themselves lie outside the scope of this Recommendation. For example, in some specific scenario, because the same set of raw data needs to be accessed by many CSCs, duplication/splitting can be selected as part of the dataset placement policies.

8.2 Data movement regulation across geographical borders

It is recommended that the CSP identify the different data movement regulations once the data needs to flow across geographical borders and provides the solution, if necessary and possible.

It is recommended that the CSP support the mechanisms to monitor the validity of the data movement regulations at geographical borders and provides the negotiation, if necessary and possible.

9 Functional requirements for inter-cloud data management

This clause provides the functional requirements for inter-cloud data management derived from the use cases described in Appendix I.

9.1 Inter-cloud data use policies

It is required that the CSP support data use policy in order to realize a CSC request.

It is recommended that the CSP integrate and validate services from multiple CSPs as an aspect of inter-cloud data use policy.

It is recommended that the CSP support inter-cloud data classification in order to realize a CSC request.

9.2 Secure data management of the SaaS replication model in inter-cloud

It is required that the CSP provide functionalities of data integrity management to check whether the data is identical to that of other CSPs.

It is recommended that the CSP provide to CSCs secure application program interfaces (APIs) to access SaaS securely.

9.3 Secure data management of the SaaS partition model in inter-cloud

It is required that the CSP provide functionalities for data identity management for software logic to find appropriate data and avoid data duplication among SaaSs.

It is recommended that the CSP provide cloud storage support data encryption functionalities to protect data.

9.4 Secure data management of the SaaS data partition model in inter-cloud

It is required that the CSP provide merging functionalities to incorporate new data into an already existing dataset.

It is recommended that the CSP provide functionalities for integrated key management among CSPs so that encryption/decryption SaaS data can merge.

10 Security considerations

Security aspects for consideration within the cloud-computing environment, including inter-cloud computing, are addressed by security challenges for CSPs as described in [ITU-T X.1601], which analyses security threats and challenges, and describes security capabilities that could mitigate these threats and meet the security challenges.

Appendix I

Use case of inter-cloud data management

(This appendix does not form an integral part of this Recommendation.)

This appendix includes inter-cloud data management-related use cases from which the corresponding functional requirements are derived.

I.1 Use case template

The use cases developed in this appendix adopt the format in Table I.1 for better readability and convenient material organization.

Table I.1 – Use case template table

Title	The title of the use case.
Description	Scenario description of the use case.
Roles	Roles involved in the use case.
Figure (optional)	Figure to explain the use case, but not mandatory.
Pre-conditions (optional)	The necessary pre-conditions that should be achieved before starting the use case.
Post-conditions (optional)	The post-conditions that will be carried out after the termination of current use case.
Derived requirements	Requirements derived from the use cases, whose detailed description is presented in the dedicated clause.

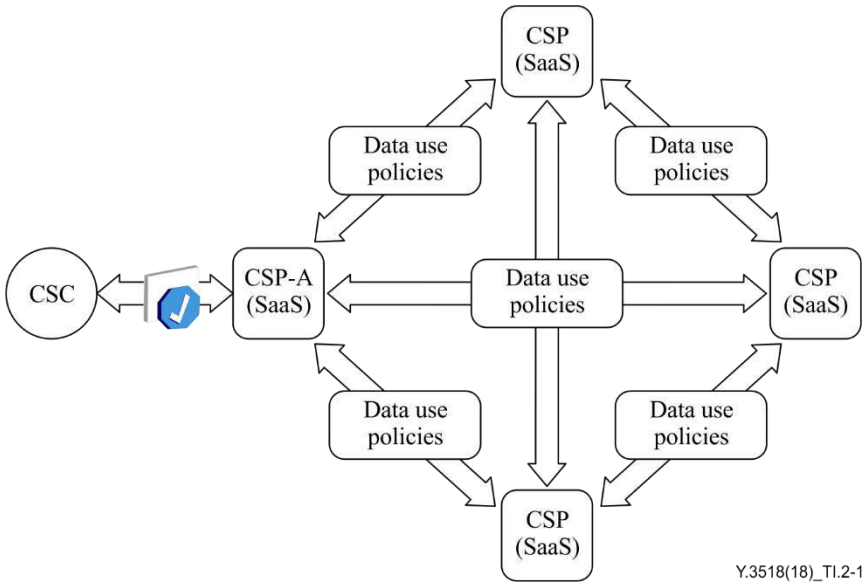
I.2 Use case of data use policies in inter-cloud

This use case illustrates data use policies aspect in inter-cloud. The inter-cloud federation pattern used to illustrate the use case is an example only.

Table I.2 – Data use policies in inter-cloud

Title	Data use policies in inter-cloud
Description	The CSC requests SaaS, which operates its data in specific countries. The CSP-A (SaaS) acts in an inter-cloud federation pattern among CPSs (SaaS) and becomes the contact point for the CSC. The CSP-A (SaaS) determines and validates appropriate data use policies or principles that allow exchange and operational use of CSC data among the inter-cloud federation. If the CSP (SaaS) operates out of specific countries, CSC data is not exchanged.
Roles	CSC, CSP (SaaS).

Table I.2 – Data use policies in inter-cloud

Figure (optional)	
Pre-conditions (optional)	The CSPs (SaaS) forms an inter-cloud federation pattern.
Post-conditions (optional)	The CSPs (SaaS) implement data use policy in their management system.
Derived requirements	Inter-cloud data use policies (refer to clause 9.1).

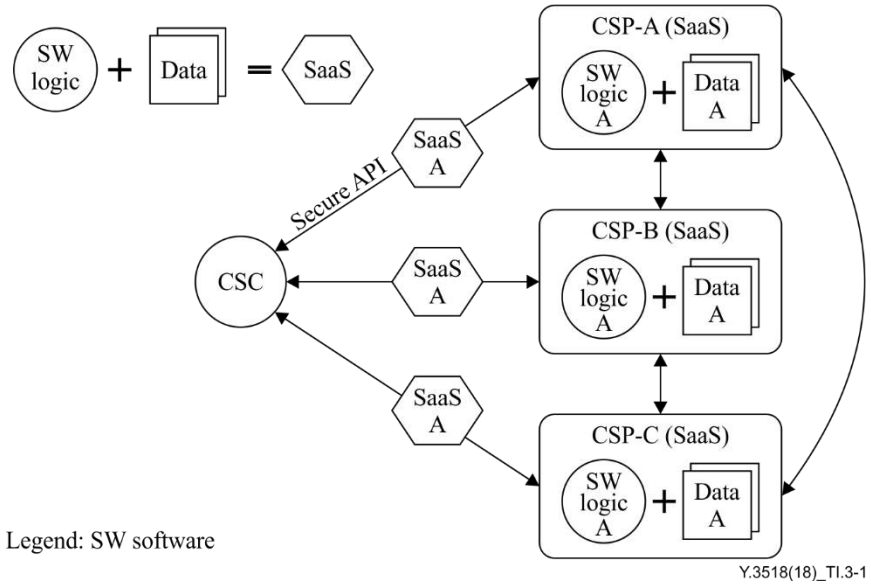
I.3 Use case of secure data management of the SaaS replication model in inter-cloud

This use case illustrates secure data management of the SaaS replication model in inter-cloud. The inter-cloud federation pattern used to illustrate the use case is an example only.

Table I.3 – Secure data management of the SaaS replication model in inter-cloud

Title	Secure data management of the SaaS replication model in inter-cloud
Description	The SaaS replication model, deployed on multiple CSPs, that combines software logic and data into one service enables the user to get evidence of the integrity of the result among multiple CSPs in order to guarantee that an operation performed in a cloud system has not been tampered with by the CSP or attackers.
Roles	CSC, CSP (SaaS)

Table I.3 – Secure data management of the SaaS replication model in inter-cloud

Figure (optional)	
Pre-conditions (optional)	The CSPs form an inter-cloud federation pattern.
Post-conditions (optional)	
Derived requirements	Data integrity among CSPs (see clause 9.2) Secure APIs (see clause 9.2)

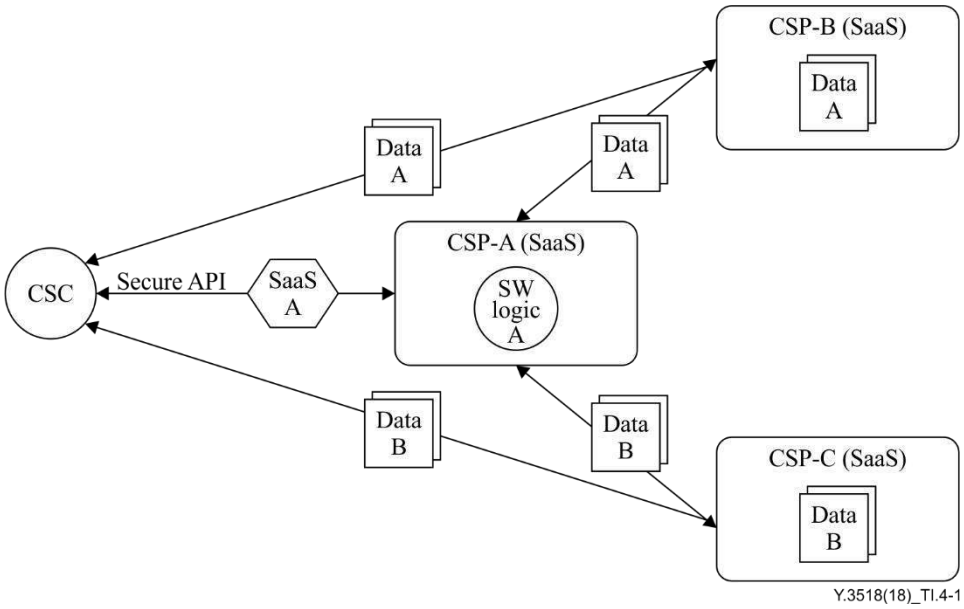
I.4 Use case of secure data management of the SaaS partition model in inter-cloud

This use case illustrates secure data management of the SaaS partition model in inter-cloud. The inter-cloud federation pattern used to illustrate the use case is an example only.

Table I.4 – Secure data management of the SaaS partition model in inter-cloud

Title	Secure data management of the SaaS partition model in inter-cloud
Description	This case separates software logic and data, and deploys them on each CSP to consider any inadvertent data breach during execution of cloud services in third party CSPs. This case considers data protection from malicious CSP threats. For example, the software logic is deployed on CSP-A and data A, B are stored on reliable cloud storage providers, CSP-B and CSP-C, respectively; the CSP-A provides the SaaS securely using data A and B stored on CSP-B and CSP-C.
Roles	CSC, CSP (SaaS)

Table I.4 – Secure data management of the SaaS partition model in inter-cloud

Figure (optional)	
Pre-conditions (optional)	The CSPs (SaaS) form an inter-cloud federation pattern.
Post-conditions (optional)	
Derived requirements	Unique data identity management (see clause 9.3) Data encryption in cloud storage (se clause 9.3)

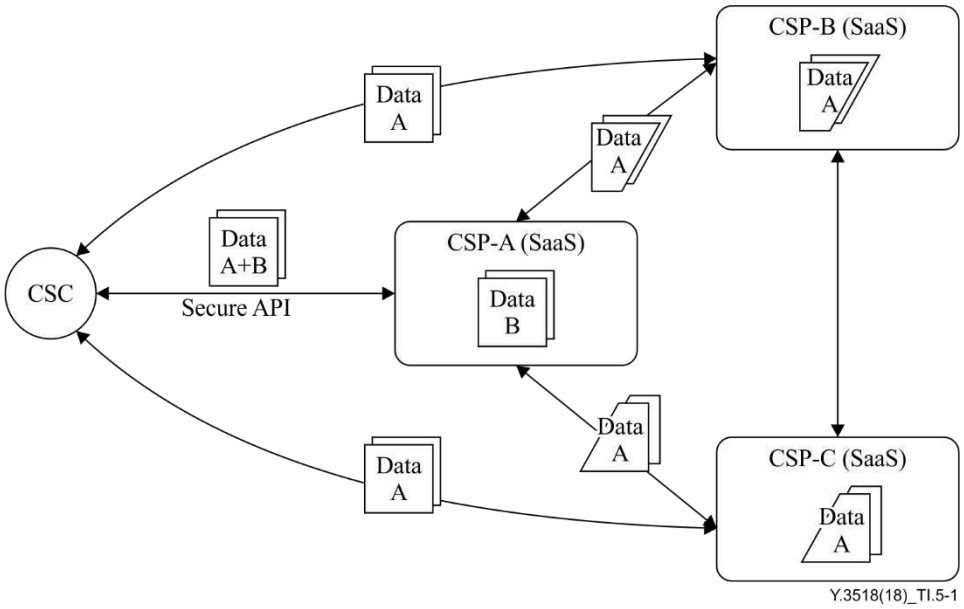
I.5 Use case of secure data management of the SaaS data partition model in inter-cloud

This use case illustrates secure data management of the SaaS data replication model in inter-cloud. The inter-cloud federation pattern used to illustrate the use case is an example only.

Table I.5 – Secure data management of the SaaS data partition model in inter-cloud

Title	Secure data management of the SaaS data partition model in inter-cloud
Description	This case partitions data and distributes fine-grained fragments of data to distinct clouds. None of the CSPs involved gains access to all the data, which safeguards data confidentiality. Data is partitioned by two methods according to data type. In unstructured data (e.g., picture, document), data can be partitioned using cryptographic data splitting. In database or structured data [e.g., extensible markup language (XML) data, log], data can be partitioned by distributing different parts of the data to different cloud service providers (CSP-A, CSP-B and CSP-C).
Roles	CSC, CSP (SaaS)

Table I.5 – Secure data management of the SaaS data partition model in inter-cloud

Figure (optional)	
Pre-conditions (optional)	The CSPs (SaaS) form an inter-cloud federation pattern.
Post-conditions (optional)	
Derived requirements	Merging technologies for encrypted data (see clause 9.4) Integrated key management (see clause 9.4)

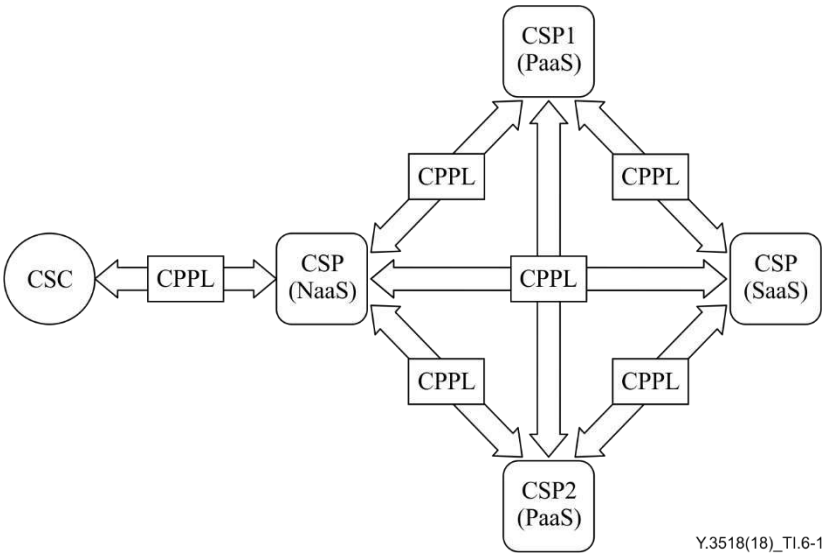
I.6 Use case of data policy language

This use case illustrates inter-cloud data annotation, processing and usage aspects between CSC and CSP or between CSPs. The inter-cloud federation pattern used to illustrate the use case is an example only.

Table I.6 – Data policy language

Title	Data policy language
Description	A CSP (NaaS) offers access to Internet (service) over virtual home gateway (vHGW) facilities using network functions virtualization (NFV) and software-defined networking (SDN) technologies. The CSP (NaaS) forms an inter-cloud federation pattern with a group of peer CSPs [here CSPs (PaaS) and CSP (SaaS)] to optimize its own resources and leverage area of service availability. The CSP (NaaS) uses a data policy language to annotate, process and use vHGW data in the inter-cloud environment. The CSP (NaaS) monitors service (here access to Internet) to ensure that particular key performance indicators (KPIs) are respected (e.g., energy efficiency, resource optimization, performance). In the case of a given KPI cross threshold, the service (here access to Internet) is automatically reallocated among members of the federation that respect data policy determined by the CSP (NaaS).
Roles	CSC, CSP (NaaS), CSP (PaaS), CSP (SaaS)

Table I.6 – Data policy language

Figure (optional)	 CPPL: compact privacy policy language
Pre-conditions (optional)	The CSP (NaaS), CSPs (PaaS) and CSP (SaaS) form an inter-cloud relationship to optimize their own resources and leverage area of service availability.
Post-conditions (optional)	The CSP (NaaS) establishes service chaining (here vHGW) between the CSC (PaaS) and CSP (SaaS). The CSP (NaaS) uses data policy language. The CSP (NaaS) reallocates service (here access to Internet) between CSPs in the federation if KPIs drop below threshold (e.g., energy efficiency, resource optimization).
Derived requirements	Data policy language (see clause 7.1)

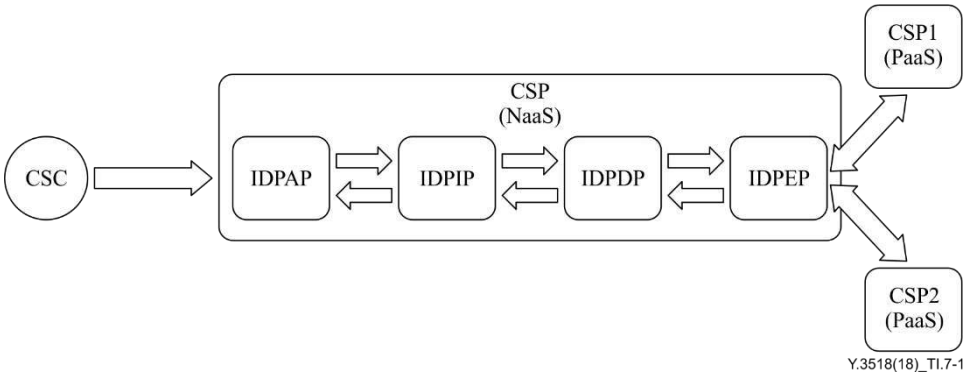
I.7 Use case of CSC data policy implementation in inter-cloud

This use case illustrates inter-cloud data policy processing and usage aspects between CSC and CSP or between CSPs. The inter-cloud intermediary pattern used to illustrate the use case is an example only.

Table I.7 – CSC data policy implementation in inter-cloud

Title	CSC data policy implementation in inter-cloud
Description	The CSP (NaaS) offers access to Internet (service) over virtual home gateway (vHGW) facilities using network functions virtualization (NFV) and software-defined networking (SDN) technologies. The CSP (NaaS) is involved in an inter-cloud intermediary pattern with two peer CSPs (PaaS), i.e., CSP1 (PaaS) and CSP2 (PaaS). The CSP (NaaS) respects data policy related to vHGW data in the inter-cloud environment. The CSP (NaaS) uses inter-cloud data policy management to process and use inter-cloud data. The CSP (NaaS) lets the CSC provide data policy related to CSC workloads passing into the inter-cloud environment. The IDPAP acts as access control for CSC data policies. The data policies are stored at the IDPIP. The IDPDP collects information about available resources and corresponding policies of peer CSPs to be able to decide which CSP can process and use vHGW data. The IDPEP establishes the service (here vHGW) between the CSP (NaaS) and one of CSP1 (PaaS) and CSP2 (PaaS) selected by the DPDP. The IDPEP is responsible for monitoring the inter-cloud environment and fulfilment of CSC data policy. In the case of violation, the IDPEP triggers the IDPDP to establish the service (here vHGW) between the CSP (NaaS) and other CSPs, which fulfils the CSC data policy.
Roles	CSC, CSP (NaaS), CSP1 (PaaS), CSP2 (PaaS)

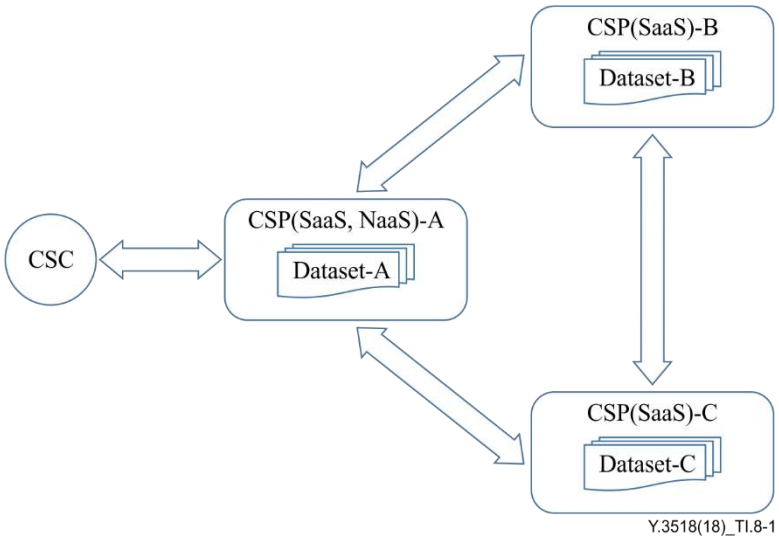
Table I.7 – CSC data policy implementation in inter-cloud

Figure (optional)	
Pre-conditions (optional)	The CSP (NaaS) has an inter-cloud relationship with two CSPs (PaaS), i.e., CSP1 (PaaS) and CSP2 (PaaS). The CSP (NaaS) respects data policy.
Post-conditions (optional)	The CSP (NaaS) supports inter-cloud data policy management. The IDPAP acts as access control for the CSC data policy and delivers policies to the IDPIP. The IDPIP stores data policies provided by the CSC. The IDPDP selects the policy on the basis of collected information about data processing and usage among peer CSPs. The IDPDP decides which CSP processes and uses vHGW data. The IDPEP implements decisions of the IDPDP in the inter-cloud environment.
Derived requirements	Inter-cloud data policy administration point (see clause 7.2) Inter-cloud data policy information point (see clause 7.3) Inter-cloud data policy decision point (see clause 7.4) Inter-cloud data policy enforcement point (see clause 7.5) Inter-cloud data policy monitoring (see clause 7.6) Inter-cloud dynamic data policy management (see clause 7.7) Inter-cloud autonomic data policy management (see clause 7.8) Inter-cloud cognitive data policy management (see clause 7.9)

I.8 Use case of data placement policies for data-intensive applications in the inter-cloud environment

This use case illustrates data placement policies for data-intensive applications in inter-cloud. The inter-cloud federation pattern used to illustrate the use case is an example only.

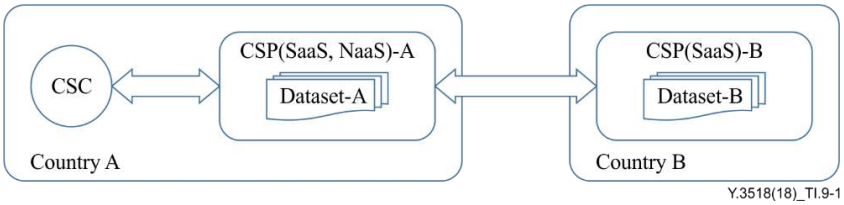
Table I.8 – Data placement policies for data-intensive applications in the inter-cloud environment

Title	Data placement policies for data-intensive applications in the inter-cloud environment
Description	Data-intensive applications are widely used in an increasing number of fields, e.g., high-energy physics, bioinformatics and astronomy. There are several challenges if the datasets required by this kind of application, including already existing data, intermediate data and final data, should be placed in the inter-cloud environment. Therefore, it is essential for federated CSPs to negotiate an appropriate placement policy for the different datasets. The placement policy conditions include, but are not limited to, the time cost of data transmission, storage space, network performance and data dependencies. The following aspects are described as the illustrations. – The transmission of data among different CSPs is inevitable. On one hand, the data scale is huge and the bandwidth limited; on the other, sometimes, there are several datasets limited to location in some specific CSP based on application logic. Consideration of how to reduce the time cost of data movements is required. – There are dependencies among these different datasets placed in different CSPs. Consideration of how to maintain these dependencies is required in order to improve calculation efficiency.
Roles	CSC, CSP (SaaS), CSP (NaaS, SaaS)
Figure (optional)	
Pre-conditions (optional)	The CSPs form an inter-cloud federation pattern. The datasets need placement in different CSPs. There are dependencies among these datasets.
Post-conditions (optional)	
Derived requirements	Dataset placement policies among different CSPs (see clause 8.1)

I.9 Use case of data regulation across different countries in the inter-cloud environment

This use case illustrates data regulation across different countries in the inter-cloud. The inter-cloud peering pattern used to illustrate the use case is an example only.

Table I.9 – Data regulation across different countries in the inter-cloud environment

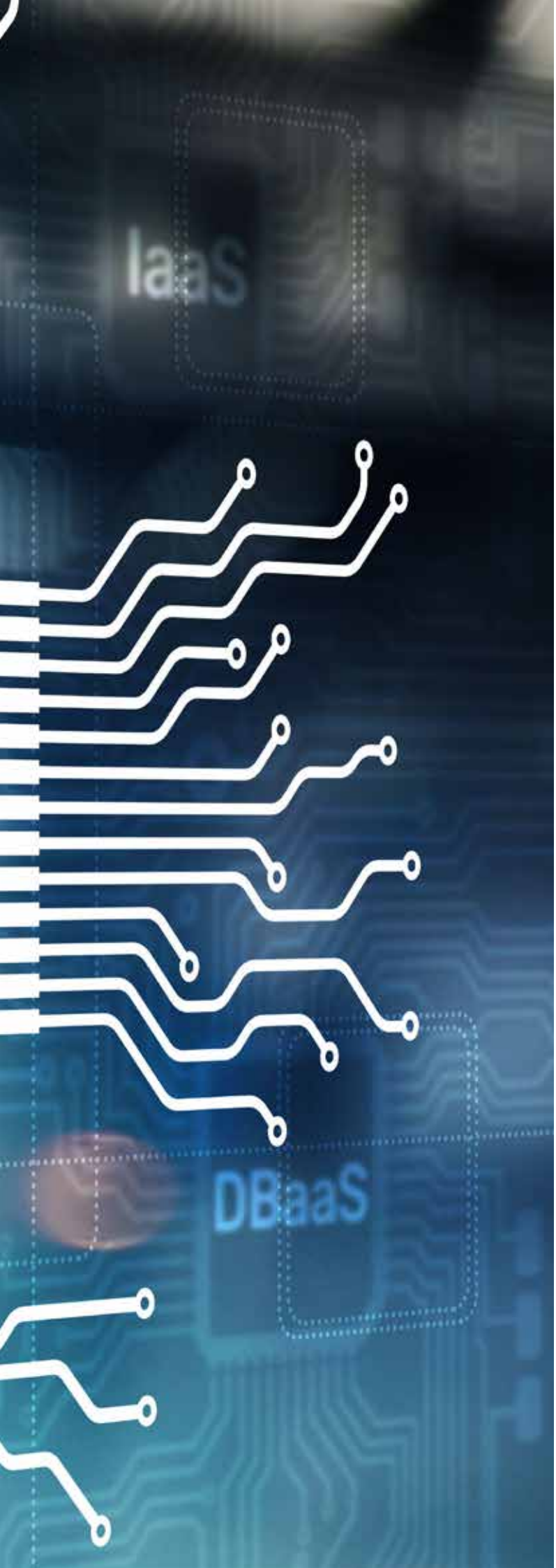
Title	Data regulation across different countries in the inter-cloud environment
Description	With the development of industrial globalization, data movement across geographical borders in the inter-cloud environment is increasingly frequent. However, data movement regulation varies significantly in different counties in several aspects, e.g., data ownership, privacy protection, law application and jurisdiction, as well as international trade rules. Therefore, the CSP needs to identify the various data movement regulations once data needs to flow across geographical borders and provide the solution, if necessary and possible. For example, when the CSC requests SaaS service requiring datasets located separately in country A and country B, CSP-A acts in an inter-cloud federation pattern among CSPs and becomes the contact point for the CSC. CSP-A needs to monitor the validity of the data movement regulation of country B and negotiate between country A and country B, if necessary and possible.
Roles	CSC, CSP (SaaS), CSP (NaaS, SaaS)
Figure (optional)	
Pre-conditions (optional)	The CSPs form an inter-cloud federation pattern. The data needs to flow across borders of countries that have different data movement regulations.
Post-conditions (optional)	
Derived requirements	Data movement regulation across geographical borders (see clause 8.2)

Bibliography

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014), *Information technology – Cloud computing – Overview and vocabulary.*

[b-ISO/IEC 19944] International Standard ISO/IEC 19944:2017, *Information technology – Cloud computing – Cloud services and devices: Data flow, data categories and data use*.


SaaS
XaaS
PaaS



3.

XaaS


DaaS

Requirements for desktop as a service

Recommendation ITU-T Y.3503

(05/2014)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Summary

As one of cloud computing service categories, desktop as a service (DaaS) provides cloud service customers with desktop functions remotely delivered by cloud service providers. Recommendation ITU-T Y.3503 introduces the concept of DaaS, and describes general and functional requirements. To derive those requirements relevant use cases are also presented.

Keywords

Desktop as a service, DaaS, virtual desktop, virtual desktop infrastructure.

Table of Contents

1 Scope

This Recommendation provides use cases, general requirements and functional requirements for desktop as a service (DaaS).

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1601] *Recommendation ITU-T X.1601 (2014), Security framework for cloud computing.*

[ITU-T Y.3501] Recommendation ITU-T Y.3501 (2013), *Cloud computing framework and high-level requirements.*

[ITU-T Y.3510] Recommendation ITU-T Y.3510 (2013), *Cloud computing infrastructure requirements.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 cloud service customer [ITU-T Y.3501]: A person or organization that consumes delivered cloud services within a contract with a cloud service provider.

3.1.2 cloud service provider [ITU-T Y.3501]: An organization that provides and maintains delivered cloud services.

3.1.3 hypervisor [ITU-T Y.3510]: A type of system software that allows multiple operating systems to share a single hardware host.

3.1.4 virtual machine [b-DMTF OVF]: The complete environment that supports the execution of guest software.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 DaaS client: A physical device and associated software running on the device that collectively enables a cloud service user to access desktop as a service (DaaS).

3.2.2 desktop as a service (DaaS): A cloud service category in which the capabilities provided to the cloud service customer are the ability to build, configure, manage, store, execute and deliver users' desktop functions remotely.

3.2.3 virtual desktop: An environment for accessing end user's desktop functions remotely.

NOTE – Examples of end user's desktop functions can include desktop interface functions for applications, data access functions for multimedia data, and control functions for input/output (I/O) devices.

3.2.4 virtual desktop infrastructure (VDI): A desktop as a service (DaaS) solution enabling the hosting of a desktop operating system within a virtual machine.

NOTE – In this Recommendation, VDI means that the virtual machine hosting the desktop operation system is running in a cloud computing environment.

3.2.5 virtual desktop template: A representation of a set of system configuration and application parameters with an option of including customer personalization, and other desired attributes.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

3D	Three Dimensional
3G	Third Generation
CPU	Central Processing Unit
CSC	Cloud Service Customer
CSP	Cloud Service Provider
CRM	Customer Relationship Management
DaaS	Desktop as a Service
DCN	Data Communication Network
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DTLS	Datagram Transport Layer Security
ERP	Enterprise Resource Planning
FEC	Forward Error Correction
GPS	Global Positioning System
HD	High Definition
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
I/O	Input/Output
IT	Information Technology
LAN	Local Area Network
OS	Operating System
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
QoE	Quality of Experience
RAM	Random Access Memory
SLA	Service Level Agreement
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VDI	Virtual Desktop Infrastructure
VM	Virtual Machine
VPN	Virtual Private Network

5 Convention

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

In the body of this Recommendation and its annexes, the words shall, shall not, should, and may sometimes appear, in which case they are to be interpreted, respectively, as is required to, is prohibited from, is recommended, and can optionally. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative are to be interpreted as having no normative intent.

6 Introduction to desktop as a service (DaaS)

DaaS is defined as a cloud service category in which the capabilities provided to the cloud service customer (CSC) are the ability to build, configure, manage, store, execute and deliver users' desktop functions remotely. With DaaS, the user experience is achieved through a user interface, which is presented on a DaaS client over the network. Figure 6-1 shows the conceptual view of DaaS.

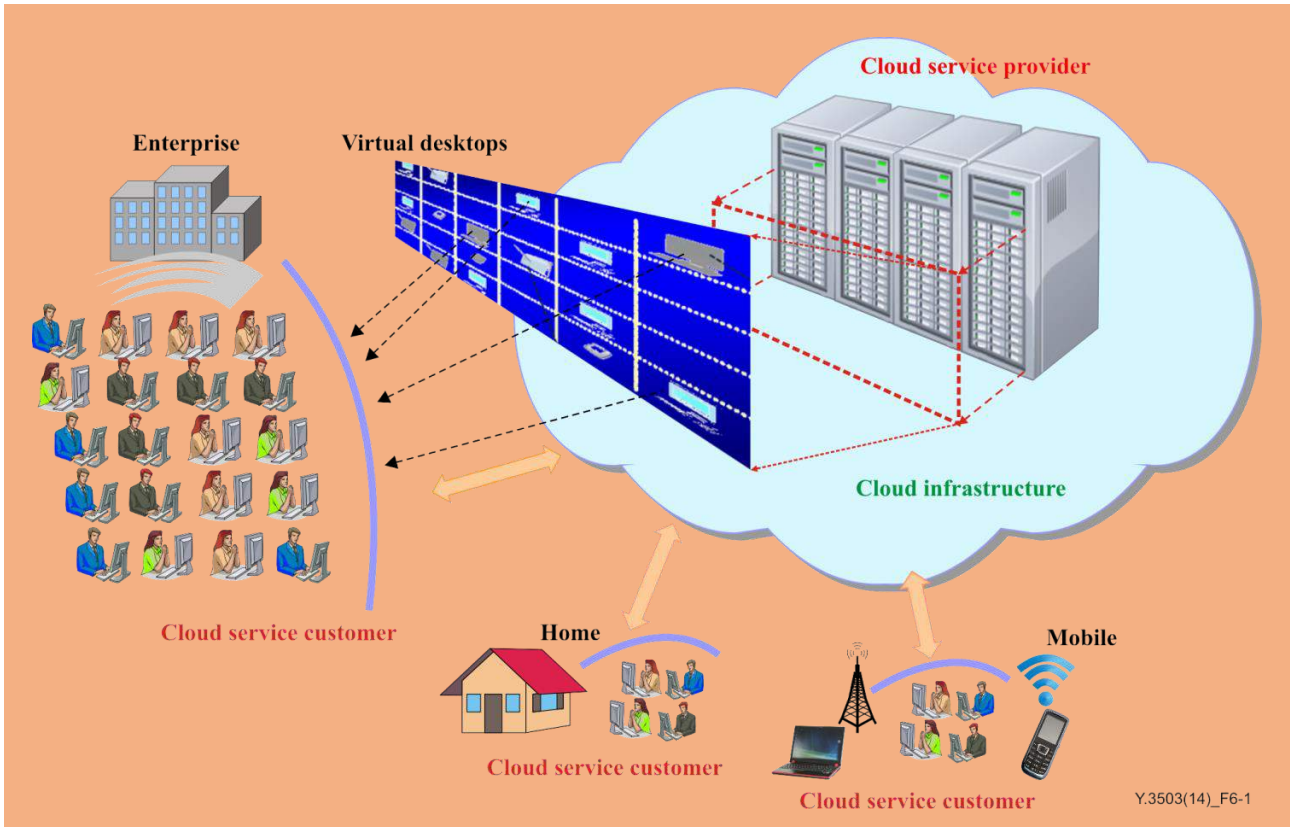


Figure 6-1 – Conceptual view of DaaS

Instead of maintaining and running a desktop operating system and applications on CSC devices, servers of a cloud service provider (CSP) located in the cloud are used to execute the instances of users' virtual desktops. This allows a party (e.g., an organization) to run end user's operating systems and applications, and keep their data in the cloud computing environment.

Based on application streaming and virtualization technologies, CSCs can access the virtual desktop environment through cloud infrastructure.

A few technologies can be used for providing services of the DaaS like virtual desktop infrastructure (VDI) and web-based solutions with various delivery protocols such as the virtual desktop delivery protocol and the web-based delivery protocol shown in Figure 6-2.

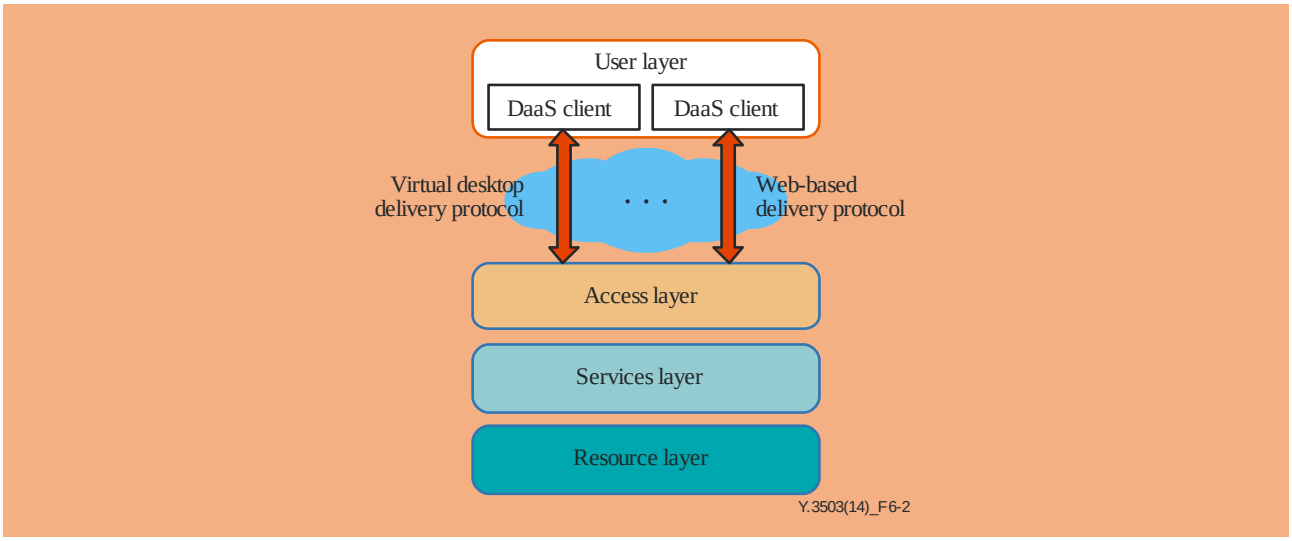


Figure 6-2 – DaaS delivery solutions

VDI supports the users' virtual desktop and recreates it in an environment hosted on a remote system. A virtual desktop is executed for each user from the server side. Users access this environment remotely through DaaS clients, with all virtual desktop associated processing. A virtual desktop delivery protocol is used to deliver the virtual desktop.

In the web-based DaaS solution, a web-based server invokes application services from different servers and aggregates them to build a virtual desktop service. The web-based DaaS solution relies on cloud services provided through the use of web oriented technologies, i.e., based on the hypertext transfer protocol (HTTP), hypertext markup language (HTML) and the new features supported by HTML5 [b-W3C-HTML5].

6.1 Main advantages of DaaS

The main advantages of DaaS [b-ITU-T FGCC1] are:

- **Enhanced management and security**: Since all desktop applications actually run in a CSP server, they are more secure than if they were installed on each user's DaaS client since the CSP can focus more on security aspects.
- **Lower total cost of ownership**: By placing emphasis on the data centre rather than on individual user devices, DaaS promotes longer hardware life. Organizations or enterprises seeking to avoid additional costs can switch part of their information and communication technology infrastructure from capital expenditure to operating expenditure, as they now pay for virtual desktops. Also, decoupling the desktop operating system from the hardware permits the use of cost-effective user's devices.
- **Preservation of user experience**: DaaS allows for a rich user experience by enabling the possible choice among multiple operating systems and their customization. Conversely, shared service environments offer a user experience that may compromise between application compatibility and user customization.
- **Separation of CSP and CSC responsibilities**: DaaS allows separation between the responsibilities of the CSP and the CSC. The CSP is responsible for the infrastructure of virtual desktops delivery (i.e., servers, storage, virtualization software, etc.), while the virtual desktops (e.g., operating system (OS), application packaging, user profiles, etc.) is under the CSC responsibility.

6.2 General configuration for DaaS

Figure 6-3 shows the general configuration environment for DaaS logical components. The environment is based on a traditional client-server model and mainly consists of a DaaS client, a connection manager, a resource pool, a virtualization infrastructure and a virtual desktop delivery. Detailed interaction among these DaaS logical components are described in clause 6.3.

NOTE 1 – Relationship between DaaS logical components and the cloud computing reference architecture in [b-ITU-T FGCC2] is described in Appendix I. Further study of the DaaS architecture is needed to map the DaaS logical components to the cloud computing reference architecture.

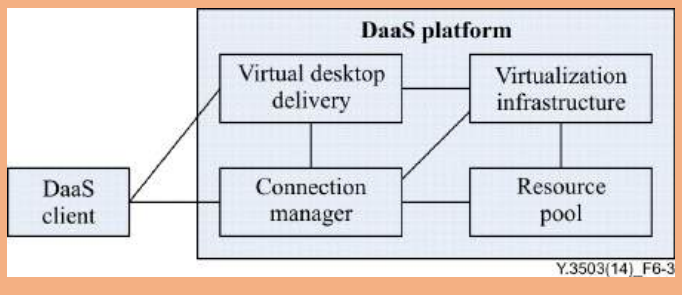


Figure 6-3 – General configuration for DaaS

The main logical DaaS components, shown in Figure 6-3, are as follows:

- DaaS client

  DaaS users can be provided with their virtual desktop remotely through their DaaS clients. To access a DaaS platform, DaaS users can employ one of the methods among dedicated software, general-purpose web browser and firmware depending on the type of DaaS client. More detailed information regarding DaaS clients is provided in Appendix II.

  NOTE 2 – Depending on the type of DaaS client, when the DaaS client is booted up, it starts a log in procedure to a corresponding virtual desktop with access information such as its identification, password and IP address. In case of termination of the corresponding virtual desktop, the DaaS client recognizes it and begins a log out procedure which includes turning off the virtual machine (VM) or the DaaS client.

- Connection manager

  This logical component is responsible for connecting a DaaS user to an available and suitable virtual desktop. The connection manager's tasks include:

  – user authentication and licence verification to validate the user and the user's application;
  – assignment of a virtual desktop;
  – coordination of a delivery protocol to be used between a DaaS client and a DaaS platform; and
  – allocation of necessary storage.

  In addition, the connection manager is responsible for load balancing and managing the number of users per DaaS platform, reconnecting a user to the virtual desktop.

  The connection manager uses the resource pool and the virtualization infrastructure to allocate the required resources such as computing, network and storage in virtualization infrastructure.

- Resource pool

  Resource pool is an abstraction of software resources such as OS, applications and user profiles. The software resources can be loaded from the resource pool to given resources in the virtualization infrastructure. A resource pool can offer provisioning information regarding the software resources on request by a connection manager.

  NOTE 3 – A user profile can contain individual information about hardware configuration (i.e., central processing unit (CPU), random access memory (RAM), I/O), used OS, selected applications and user computing environment information (e.g., display resolution and Internet access means).

- Virtualization infrastructure

  The main role of the virtualization infrastructure is to support hardware and software resources and create virtual resources (e.g., VMs). The virtualization infrastructure can use a virtualization function, called a hypervisor, to manage hardware resource efficiently. A hypervisor can abstract physical hardware resources and assign them dynamically to a virtual desktop. In this case, the end user's application runs on the virtual desktops provided by the virtualization infrastructure. The virtualization infrastructure supports high availability features (e.g., multiple VMs are created from the same VM template) with pre-defined configuration parameters.

- Virtual desktop delivery

  This component is responsible for encapsulation and delivery of either access to an entire information system environment, or the environment itself to a remote DaaS client through the network. A protocol for virtual desktop delivery provides the communication channels between the DaaS client and the DaaS platform in order to transfer all the interaction information. The interaction information includes display information, control and configuration information, monitoring information, etc.

  DaaS can be serviced by either a personalized virtual desktop or by a virtual desktop from a shared pool. In the case of a personal virtual desktop, there is a one-to-one mapping between a virtual desktop and a cloud service user. Each user is assigned a virtual desktop that can be personalized and customized. These changes are available to the user each time that user logs on to his or her personal virtual desktop. For a shared virtual desktop pool, a single OS image is replicated across many VMs and users can reuse a single VM over time. As users connect to the shared virtual pool, they are dynamically assigned a virtual desktop. A shared virtual pool allows for uniformed experience across all end users, while combined with simplified administration means.

6.3 Interaction between DaaS components

To illustrate the DaaS operation concepts based on Figure 6-3, the various steps of an example interaction for DaaS are shown as follows:

- A DaaS client accesses a connection manager through a security protocol (such as secure shell or transport layer security) and the connection manager validates the user with a user-ID and associated password.
- The connection manager identifies a corresponding user profile and, in order to assign appropriate virtual resources in the virtualization infrastructure, a provisioning operation helps the connection manager to allocate the virtual resources that satisfies the user's hardware configuration and is optimal to the computing environment.
- If there are no proper virtual resources, the connection manager requests the virtualization infrastructure to create such virtual resources according to the hardware configuration requested by the user or a pre-defined hardware configuration.
- After such virtual resources are assigned or created, the connection manager applies the user profile, including installation of OS and applications, to construct a virtual desktop.
- A connection to deliver a corresponding virtual desktop is created in the virtualization infrastructure and the information of the connection is dispatched to the connection manager.
- The connection manager sends the connection information to the DaaS client and the DaaS client connects to the virtual desktop in the virtualization infrastructure.
- The DaaS client communicates with the virtual desktop through the network using a delivery protocol for the virtual desktop.
- When a DaaS user terminates a virtual desktop service, the DaaS client executes a log out operation without loss of user data.
- During the log out operation, the connection manager updates the modified user profile in a user profile pool to keep the most recent information, and releases the VM resources.

7 DaaS general requirements

The DaaS general requirements are described in [ITU-T Y.3501] as follows:

- Quality of experience (QoE);
- Fast boot-up time;
- Configurability of the virtual environment;
- Single sign-on access control.

Additional general requirements of DaaS derived from use cases (cf. Appendix III) include (but are not limited to):

- **Support for high-definition (HD) and three-dimensional (3D) applications**: DaaS can optionally support execution of HD applications on virtual desktops for CSCs.

  NOTE 1 – HD and/or 3D applications (e.g., high-definition 3D videos or games) are becoming one of the major user demands in the personal computing device market.
- **Extensible storage**: It is recommended that a CSP support the storage extension requested by a CSC.
- **Response time**: It is recommended that DaaS provide CSCs with acceptable QoE.

  NOTE 2 – Detailed relevant information on acceptable response time is described in Appendix IV.
- **High availability**: It is recommended that high availability in terms of delivery and operation of DaaS be assured by a CSP.
- **Resiliency to disaster**: In a case of a disaster, DaaS is recommended to provide and maintain an acceptable level of service.

  NOTE 3 – This includes preserving the system information and the users' data including their virtual desktop state such as power-on, power-off, suspend, etc.
- **Service continuity**: It is recommended that in case of temporarily unavailable resource access, a CSP provides the capability to preserve the state of the user session.
- **System scalability**: It is recommended that DaaS supports elastic scalability of:
  - Storage for DaaS user account information, virtual desktop environment settings, and active and inactive virtual desktop environments;
  - Processing and network capacity for the number of concurrent DaaS user connections and total DaaS users;
  - Underlying DaaS resources.
- **DaaS developer environments**: It is recommended to provide a developer environment for the service and contents regarding DaaS.
- **Diversity of DaaS client**: It is recommended that the CSP support a wide selection of DaaS clients.

  NOTE 4 – Examples of such DaaS clients are described in Appendix II.

8 DaaS functional requirements

8.1 Operation and management requirements

Operation and management requirements include:

- **Unified management interface**: It is recommended that the CSC be capable of deploying, configuring, managing and monitoring the DaaS through a unified management interface.
- **User account provisioning**: It is recommended that the CSP provide the method of operating and provisioning various types of accounts in accordance with CSC's characteristics based on the service level such as one-time usage and permanent account, types of virtual desktop environments, and allocating options for the virtual desktop environments.

  NOTE 1 – User account provisioning depending on the CSC types is described in Appendix V.

- **Virtual desktop lifecycle management**: It is required that the CSP support the full life cycle management of the virtual desktop, including set-up, test, delivery, use, maintenance, optimization, shutdown and deletion.
- **Support of virtual desktop template**: In order to achieve better delivery of DaaS, a desktop template can be optionally used for DaaS maintenance purposes.

  NOTE 2 – The virtual desktop template includes defining, publishing, verifying, revoking, deleting and other related operations.
- **User profile management**: It is required that the CSP manage the user profile information.
- **Server-side platform hardware resource maintenance**: It is required that the CSP maintain and allocate servers, storage, network and related hardware.
- **Service-related resource maintenance**: It is required that the CSP maintain DaaS service supporting applications and data, such as security auditing server, performance monitoring server, active directory, database, user configuration, file server, etc.
- **Status monitoring**: It is recommended that the current running status of virtualized resource be monitored to perform the change the status requested by a CSC.
- **System load monitoring**: In order to achieve an appropriate QoE, it is recommended that a CSP be capable of monitoring the system load to assign virtualized resources to a CSC.
- **Automated scriptable management interface**: It is recommended that the DaaS management solution be accessible through a consistent scripting interface.
- **Power management**: It can optionally be that the CSP is able to support the mechanism that monitors server's power and relevant usage in order to perform load balancing or save the power consumption in the server.
- **Accounting and charging**: It is recommended that the CSP collect accounting information based on computing power, network use, storage, memory and/or application licence fee. Accounting information is collected per service and per user. It is also recommended that the CSP provide a charging scheme based on the accounting information and charging information transparently.

  NOTE 3 – Depending on the implementation of DaaS, the charging scheme may not be needed.
- **Managing and operating pre-configured environments**:
  - It is recommended that the CSP manage and operate the pre-configured environments which are prepared after configuring the service information (such as server processing capacity, the prediction of concurrent users and the resources capacity, etc.).
  - It is recommended that the CSP provide the preconfigured environment without the loss of user functionality and the degradation of performance when service is requested.

  NOTE 4 – The pre-configured environments are the environmental files such as images of OS and applications, which reflect the CSC's requirements including operating environment, installed applications, user data and level of service. The pre-configured environments are prepared in advance with the related operations (e.g., generating, creating, reproducing and cloning, etc.) and supplied in their use during service execution.
- **Monitoring and controlling DaaS**: It is recommended to monitor and control the activities of a DaaS platform without impacting the performance of the DaaS platform.

  NOTE 5 – A software agent can be used to communicate with a kernel or a hypervisor in order to create and control VMs.
- **DaaS client capability**: It is recommended that virtualization infrastructure supports making use of any available DaaS client capability on the CSC's device as and when required by application programs running in virtual desktop.
- **User log management**: It is recommended that the CSP keep the connection log information for all CSCs and their event logs for further security and/or incident analysis.

8.2 DaaS platform-side functional requirements

The DaaS platform-side functional requirements include:

- **Maintaining DaaS user status**: It is required that the CSC be capable of reconnecting to virtual desktop in the same virtual desktop state as left.
- **Optimized adaptation for content type**: It is recommended that the DaaS client be optimized for the content type involved (e.g., each type of content is encoded with a codec that is tuned to best support the content and the codec configuration can be automatically changed based on the content type such as multimedia, images and text).
- **Isolation between virtual desktop functions**: It is required that the operation of the virtual desktop functions of one CSC should not be negatively impacted by the use of virtual desktop functions by other CSCs.
- **Graphic processing acceleration support**: In order to provide ability to DaaS clients to work with graphic-intensive software packages (such as 3D computer-aided design or compression) running on the server, it is recommended that the CSP provide the acceleration of graphic processing to DaaS clients.
- **Server-side rendering**: In order to provide a consistent user experience to a wide range of DaaS clients as well as to improve user experience, it is recommended that the local desktop be composed and rendered on the host before the resulting image is encoded and sent to the DaaS client.
- **Standard video codec support**: For applicable video content, it is recommended to support standard codecs, such as specified in [b-ITU-T H.264] or [b-ITU-T H.265].
- **Progressive encoding support**: For networks with limited bandwidth, in order to improve user experience in case of a network bottleneck, it is recommended to use progressive encoding.

  NOTE – Progressive encoding and rendering means that the image can be encoded and sent over several stages, and the image quality becomes progressively clearer at each stage.
- **CSC environment backup**:
  - It is recommended that the CSP backup and restore the allocated virtual machines with user environment in order not to lose user data.
  - It is recommended that the CSP should not degrade the service performance from the process of backing up and restoring.
- **Standard audio encoder support**: It is recommended to support standard audio encoders.

8.3 DaaS client-side functional requirements

The DaaS client-side functional requirements include:

- **Resource request**: It is recommended that the CSC be capable of configuring the system resources in its use (e.g., CPU, memory, storage and other devices) during service execution.
- **Support of DaaS client peripherals**: It is recommended that DaaS applications be able to use DaaS client peripherals.

  NOTE 1 – Examples of DaaS client peripherals include USB port, flash memory, global positioning system (GPS), camera, etc.
- **Video decoder support**: For rendering video content on client, it is recommended to support standard codecs, such as specified in [b-ITU-T H.264] or [b-ITU-T H.265] to decode encoded images.
- **Standard audio decoder support**: It is recommended to support standard audio decoders.
- **Synchronization between DaaS client and DaaS platform**: It is recommended that DaaS support synchronization of DaaS user state when the connection is established and terminated.

  NOTE 2 – DaaS user state include desktop background and layout, user interface preferences, current DaaS user timezone, etc.

8.4 DaaS platform-DaaS client interaction functional requirements

The functional requirements related to the interaction between DaaS platform and DaaS client include:

- **Dynamic configuration adaptation**: To improve network throughput, it is recommended that a DaaS client be able to dynamically determine its access network types and adapt its configuration (including the network protocols and display resolution) accordingly to ensure network connectivity and improve the user experience.
- **Standard transport protocol support**: It is required to use standard transport protocols (e.g., transmission control protocol (TCP) [b-IETF RFC 793] and user datagram protocol (UDP) [b-IETF RFC 768]) to deliver DaaS.
- **High latency environment**:
  - For applications and elements that are less sensitive to packet loss and only dependent on low latency and jitter (such as for desktop rendering, audio, video streaming, or communications), a loss-tolerant transport (e.g., UDP) can optionally be used for allowing immediate delivery with some packet loss, without any need to wait for retransmission of lost packets.
  - For those applications and elements where data reliability is important (e.g., for typing), it is recommended to use the standard transports available for this purpose that allows recovering from losses without retransmissions, such as forward error correction (FEC).

  NOTE 1 – DaaS is very sensitive to latency and jitter (variation in latency). For example, when DaaS users type text or move a mouse they need to see this appear almost immediately on their screens. For this reason, retransmission is often unacceptable as a mean of error recovery. This constraint on latency and jitter imposes the following DaaS-specific requirements when suffering from latency.
- **Fall-back to alternative transport**: When the standard transport protocol is not available, it is recommended that an automatic fall-back to the alternative protocol is implemented by the DaaS application. An example would be a fall-back from UDP to TCP.
- **DaaS client reconnection**: When there is no response from the DaaS platform to a service request from a DaaS client, it is required that the DaaS client send a reconnection request to the DaaS platform. If the reconnection fails, it is also required that a DaaS user be notified of loss of service.
- **Display redirection**: It is required that the CSP redirect display to a CSC immediately after the completion of the connection between a DaaS platform and a DaaS client.
- **Hybrid resource configuration**: It is recommended that resources in both a DaaS platform and a DaaS client be used simultaneously to achieve the best performance and the CSP support the ability to modify their configuration to improve the performance.

  NOTE 2 – Hybrid means that there can be various combinations of resource configuration between a DaaS client and a DaaS platform.

8.5 DaaS security requirements

- **Standard security protocols support**: It is recommended to use standard security protocols for content delivery protection for DaaS (e.g., secure socket layer (SSL) [b-IETF RFC 6101] and datagram transport layer security (DTLS) [b-IETF RFC 6347]).
- **Network separation**: It is recommended that DaaS provide policy-based separation between the DaaS client's local network, DaaS provided network and the public Internet network. This separation can be logical (e.g., virtual private network (VPN)) or physical as appropriate.

  NOTE – In addition to cloud-based resources, DaaS users may require access to local network resources (such as printers), or the public Internet.

9 Security considerations

It is recommended that the security requirements of [b-ITU-T Y.2201], [b-ITU-T Y.2701] and applicable X, Y and M series of ITU-T security Recommendations be taken into consideration, including access control, authentication, data confidentiality, communications security, data integrity, availability and privacy. It is also recommended that the security framework for cloud computing described in [ITU-T X.1601] be considered. [ITU-T X.1601] analyses security threats and challenges in the cloud computing environment, and describes security capabilities that could mitigate these threats and meet security challenges.

Appendix I

Relationship between DaaS logical components and the cloud computing reference architecture

(This appendix does not form an integral part of this Recommendation.)

This appendix provides the relationship between DaaS logical components, which are described in clause 6.2, and the cloud computing reference architecture [b-ITU-T FGCC2].

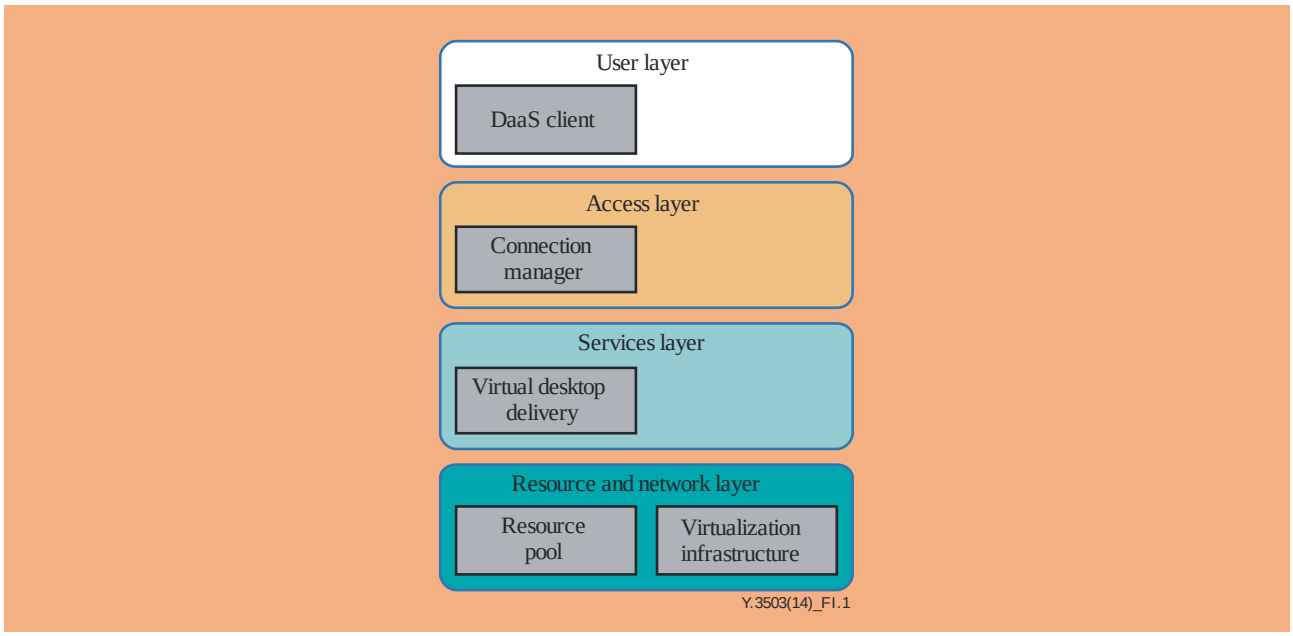


Figure I.1 – An example of location of DaaS logical components within the layers of the cloud computing reference architecture

Figure I.1 shows an example of the location of the DaaS logical components, which are related to layers in the cloud computing reference architecture.

Since the user layer provides the user interface between CSC and CSP, the DaaS client logical component can be related to this layer in that a DaaS CSC accesses the virtual desktop through this component.

The capability to provide the connection between DaaS CSCs and virtual desktops is the main role of the connection manager. This DaaS logical component corresponds to the access layer of the cloud computing reference architecture.

The virtual desktop delivery DaaS logical component facilitates the implementation of the virtual desktop by employing a delivery protocol. Therefore, this DaaS logical component is related to the services layer of the cloud computing reference architecture.

The resource pool and the virtualization infrastructure as DaaS logical components provide an abstraction of software and hardware resources. These two DaaS logical components are related with the resource and network layer of the cloud computing reference architecture.

Appendix II

DaaS client classification

(This appendix does not form an integral part of this Recommendation.)

DaaS users access their virtual desktops using networked DaaS clients, such as desktop computers, thin clients and mobile devices. Basically, most of these devices rely on computing power in DaaS platforms for all or a majority of their applications. Several ways to access virtual desktops from DaaS clients can be provided. Some DaaS clients support specific software dedicated to DaaS while some do not require specific software on the DaaS client and instead use a general web browser to interact with the DaaS platform. Still, some DaaS clients can directly connect without any software or browsers. Table II.1 shows the characteristics of various types of DaaS clients, including these access methods

Table II.1 – Characteristics of DaaS client

Categories	Personal computer	Thin client	Mobile device
Access method	Dedicated software web browser	Dedicated software Web browser	Dedicated software web browser
Network	Mainly wired	Mainly wired	Wireless
CPU	Performance-centric	Power-centric	Power-centric
RAM	Yes	Yes	Yes
Storage	Yes (Hard disk drive)	Yes/No (Flash memory)	Yes (Flash memory)

Appendix III

DaaS use cases

(This appendix does not form an integral part of this Recommendation.)

This appendix describes seven DaaS-related use cases in Tables III.1 to III.7.

Table III.1 – Office automation of development-oriented enterprise

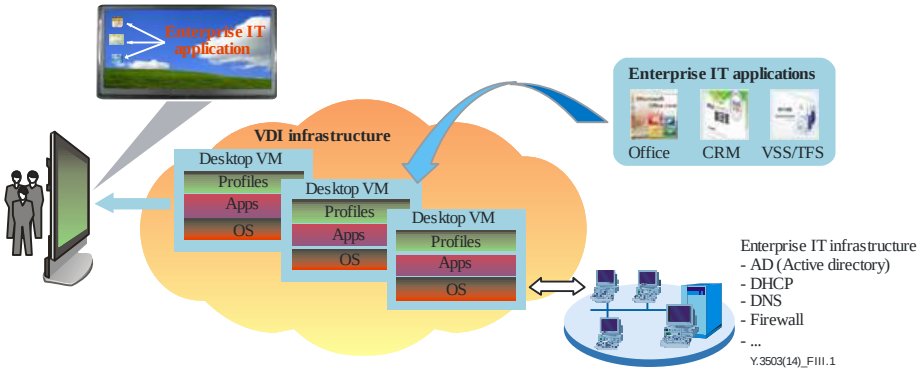
Legend	Use case
Use case title	Office automation of development-oriented enterprise
Use case description	In this scenario, the DaaS users access the enterprise applications and data hosted in virtual desktops which are created within a DaaS platform. Common applications of this type include online word processing, email, communication, co-operating development, etc. The sales staff also can view customer information and marketing records on the enterprise website. The DaaS platform interacts with traditional enterprise information and communication technology facilities to achieve many control tasks, for instance, using dynamic host configuration protocol (DHCP) to assign an IP address for thin client, leveraging internal domain name system (DNS) server to resolve local host names, and consulting authentication of user desktop sessions.
High-level figure describing the use case	
Derived requirements	– Single sign-on access control – QoE – Standard video codec support – Support of DaaS client peripherals – Standard security protocol support

Table III.2 – Customer service call centre

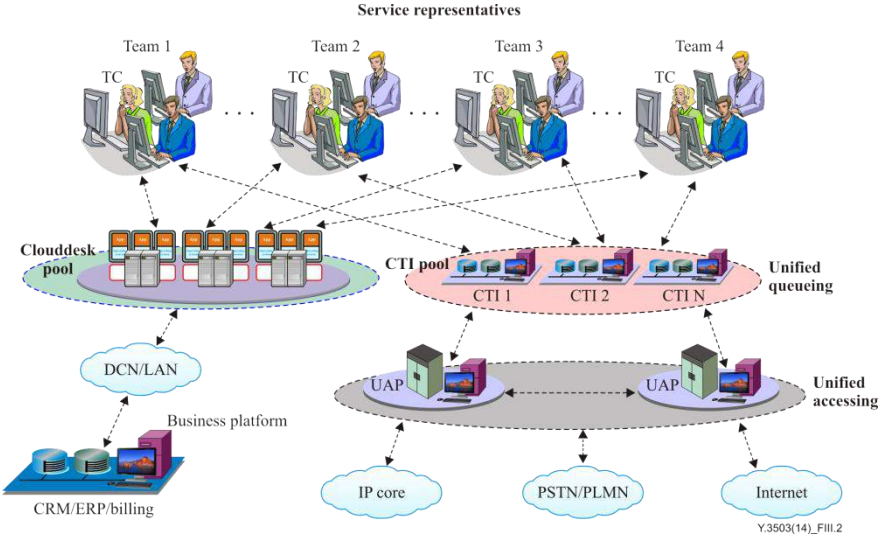
Legend	Use case
Use case title	Customer service call centre
Use case description	Virtual desktop pool supports distributed deployment model and can be deployed in the cloud computing infrastructure as a service (IaaS) resource pool with the dynamic stretching of resources. By adopting cloud computing technology (virtualization, distributed computing and storage, cluster, etc.) to consolidate queuing resource and desktop resources, unified phone call dispatching and delivery and maintenance of the desktop can be achieved in an intensive way.
High-level figure describing the use case	
Derived requirements	– Unified management interface – Automated scriptable management interface – Diversity of DaaS client

Table III.3 – Scenario of DaaS user

Legend	Use case
Use case title	Scenario of DaaS user
Use case description	Scenario of DaaS user is driven by a specific class of user. Common user types that benefit from DaaS are mobile workers, task workers (such as factory floor and call centre workers), contractor/offshore workers, and remote workers in branch offices. • Mobile workers: If an organization needs to support employees who are mobile, work from home or work from the road, a DaaS solution can enable employee productivity anywhere and increase effective user collaboration without compromising security. DaaS can offer secure access to desktops and applications over low-bandwidth connections without requiring new applications to be distributed to DaaS users. Employees will see a consistent set of applications and can access their own data regardless of location. If employees need access to a comprehensive desktop experience, they can be assigned a personal virtual desktop within the confines of the corporate data centre. This improves the DaaS offering available to users while keeping the environment securely managed. With the wide adoption of third-generation (3G) wireless networks, users are even more capable of experiencing a full-fidelity desktop remotely.

Table III.3 – Scenario of DaaS user

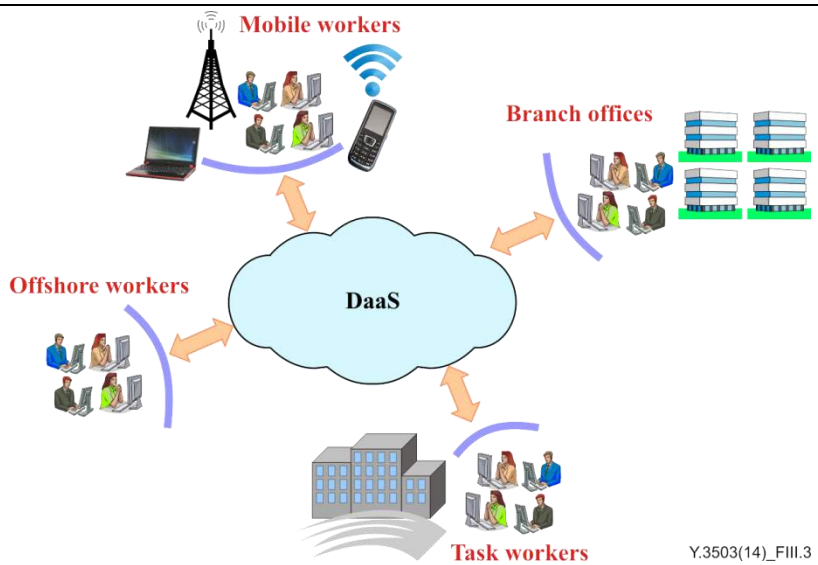
Legend	Use case
	• Task workers: If an organization includes structured task workers, such as in call centres and retail branches, DaaS can provide a more cost-effective and productive user experience because these user roles do not typically need access to multiple applications to complete business processes. Additionally, there are situations when the location is simply not capable of supporting a fully functioning client computer; instead, thin-client solutions are more applicable. The same experience can be provided even if the client computer is a legacy computer. This type of deployment can extend the reach of applications within the enterprise and is a valuable way to deliver the right business tools in a cost-effective way. • Contractor/Offshore workers: Many companies are leveraging workforce experience from around the world. Organizations will need to provide access to applications for users located both remotely and internationally. In order to provide access to resources while respecting corporate policies, providing a virtual desktop or virtual desktop pool becomes very attractive for organizations. This allows users to receive a first-class client on the network while allowing the organization to control where the virtual desktop is running, how the virtual desktop is accessed, how data is being run on the client computer and where data is stored. • Remote workers in branch offices: In an environment that relies on remote or branch offices, DaaS can provide enhanced capabilities to these sites and reduce the network bandwidth that the required applications use. For example, a bank might have essential financial software applications that would not be cost-effective to deploy and maintain in every branch. With DaaS, the software can be available at a central headquarters and accessed as needed by employees in different locations. A centralized-applications strategy often results in a reduction of application server infrastructure at various branches or locations, requiring much less maintenance and on-site support from the home office information technology (IT) staff.
High-level figure describing the use case	
Derived requirements	– Single sign-on access control – Service continuity – Diversity of DaaS client – Managing and operating pre-configured environment – Maintaining DaaS user status – CSC environment backup – Standard transport protocols support

Table III.4 – Local resource usage

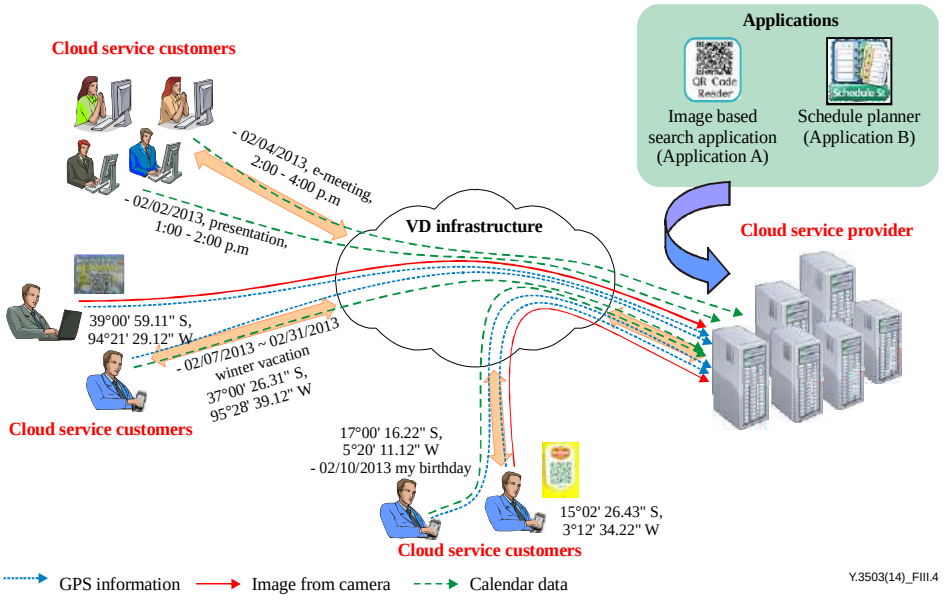
Legend	Use case
Use case title	Local resource usage
Use case description	In this scenario, an application hosted in a DaaS platform requires input from the local resources where a DaaS client is located, i.e., user terminal, to function properly. For instance, an image-based search application will require input from a camera on the terminal; the location based application may require GPS information from the GPS module running on the terminal; the schedule planner would require calendar data (meetings, task) from the terminal. For instance, Alice is using an application called "My locality" which provides a list of near-by attractions. This application makes use of GPS information, from the GPS module running in its host, to find the exact current user location. Since the application is being used remotely and hosted on the network, it needs the user terminal to provide its GPS information for the application to provide correct results (attractions near the user not near the server where the application is hosted). When Alice uses the application, local GPS data are sent to the server where they are used to provide correct results.
High-level figure describing the use case	
Derived requirements	– Support of DaaS client peripherals

Table III.5 – Service continuation for DaaS

Legend	Use case
Use case title	Service continuation for DaaS
Use case description	In this scenario, a consumer is using a particular DaaS. Due to network unavailability, the consumer gets disconnected from the DaaS platform. Later on and after network re-establishment, the consumer starts consuming the service from the same point where it got disconnected, enabling preservation of all user data and settings. Flow: • When a disconnected session is noticed, the DaaS platform identifies the related CSC and the virtual desktop. • The DaaS platform checks if user has opted for service continuity, i.e., no loss reconnection. • The DaaS platform saves the required data such as virtual machine data before releasing the resources. • On reconnection, the DaaS platform shall look for any saved data and reloads them before resuming the service.

Table III.5 – Service continuation for DaaS

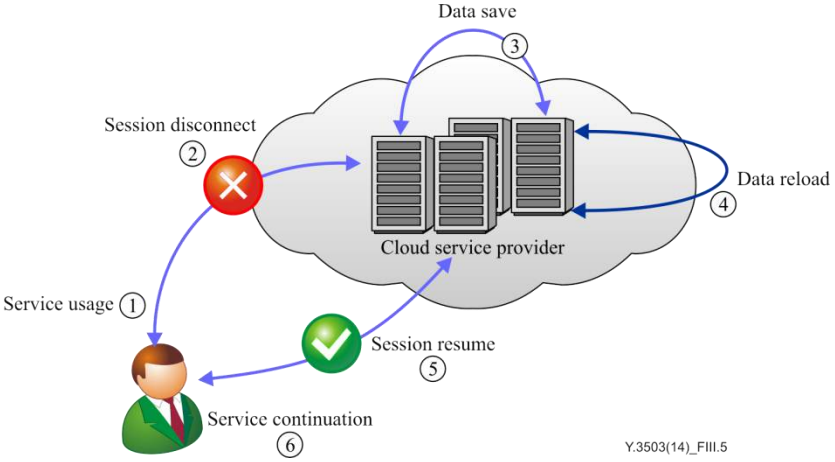
Legend	Use case
High-level figure describing the use case	
Derived requirements	– Resiliency to disaster – Service continuity – Monitoring and controlling DaaS – Maintaining DaaS user status – CSC environment backup – DaaS client reconnection – Display redirection

Table III.6 – Home application using DaaS

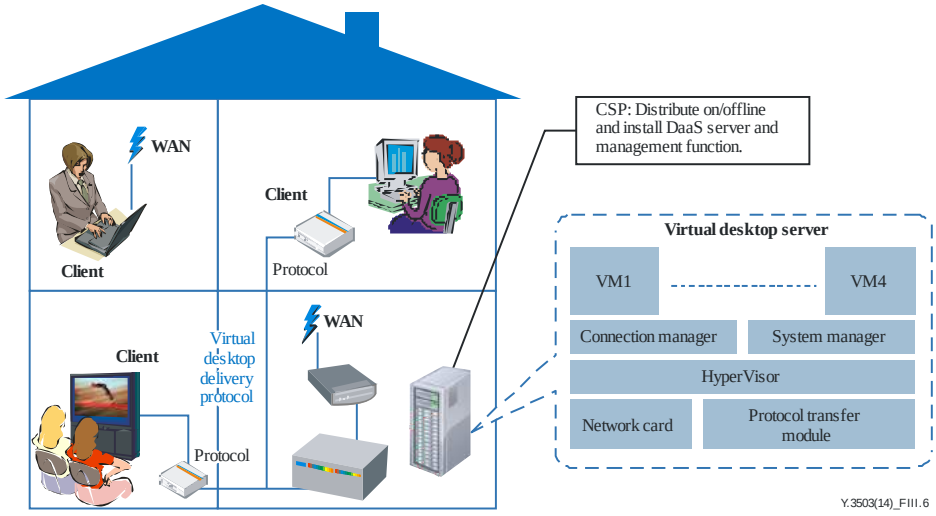
Legend	Use case
Use case title	Home application using DaaS
Use case description	CSCs access the home applications and data hosted in virtual desktops which are created within a DaaS platform in home. This type of service can support a computer for multi-users with own virtual desktops in small area. CSCs can access their own virtual machine with any DaaS clients through a delivery protocol for virtual desktops in home. Since CSC's access is taken in local area in this application, a certain access protocol can be adopted for the dedicated network or the dedicated DaaS client. CSP can distribute the package for server management and installation to support configuration functions by on-line or off-line ways.
High-level figure describing the use case	

Table III.6 – Home application using DaaS

Legend	Use case
Derived requirements	– Unified management interface – Diversity of DaaS client – Optimized adaptation for content type – Dynamic configuration adaptation – Support of DaaS client peripherals

Table III.7 – Charging scheme for DaaS

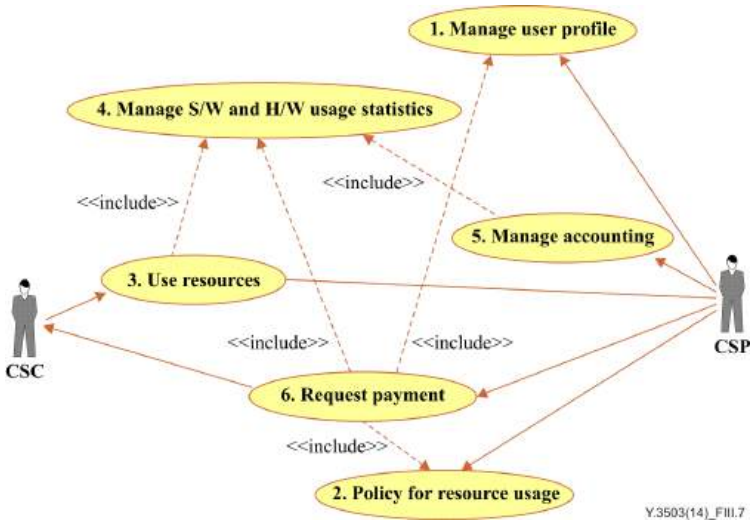
Legend	Use case
Use case title	Charging scheme for DaaS
Use case description	This use case depicts the case where charging functionality is required in DaaS. The purpose of this use case is to show various environments of CSCs that use common resources provided by the same CSP. There are two actors in this diagram: CSC and CSP; they provide software and hardware. • The CSP needs to manage DaaS user profiles including the types of users. (#1 in figure). • As, depending on the type of users, the rate for using resource can be offered differently, the CSP manages the policy for resource usage. (# 2 in figure). • The CSC uses resources (#3 in figure) and the CSP manages software and hardware usage statics (#4 in figure). • The CSP manages accounting (#5 in figure) by monitoring software and hardware usage statistics (use case 3). The CSC can use storage, CPU and memory as in IaaS, and whenever an application (software) runs on CSP. DaaS also provides storage, CPU and memory. The CSP needs to store accounting information of software and hardware usage whenever the usage occurs. • Considering user profile, software and hardware usage statistics, and the policy of resource usage to reflect different types of usage, the CSP produces bills and requests payment to CSCs (#6 in figure).
High-level figure describing the use case	

Table III.6 – Home application using DaaS

Legend	Use case
Derived requirements	– Accounting and charging – User account provisioning – User profile management – Server-side platform hardware resource maintenance – Service-related resource maintenance – Status monitoring – System load monitoring – Support for HD and 3D applications – Extensible storage – Resource request – User log management

Appendix IV

Value for response time limit

(This appendix does not form an integral part of this Recommendation.)

The response time is specified in clause 7 as a general requirement for DaaS. The value of the response time-limit is needed in order to meet the CSC's acceptable QoE.

This appendix only provides general information relevant to response time. However, the response time described in here is not specific to cloud computing and DaaS.

Figure IV.1 shows a response time model [b-Shneiderman].

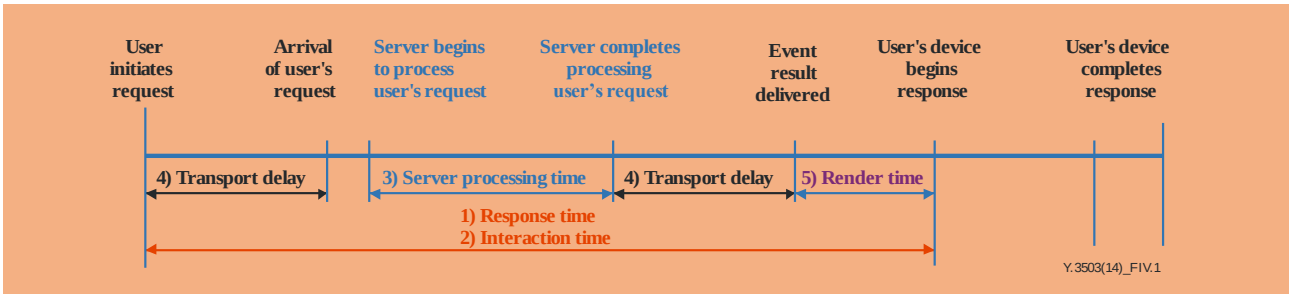


Figure IV.1 – Model of response time

As shown in Figure IV.1, the response time includes transport delays, server processing time and rendering time on a client as defined hereafter:

- Response time: An interval from the moment when user initiates an activity until that user's device begins to present its result on the display;
- Interaction time: The same as response time;
- Transport delay: An interval from the moment when user's request is sent until it is received by a server or the time from the moment a server sends;
- Server processing time: Operation time used by a server to process the user's request;
- Rendering time: Duration for generating an image with the received event results screen on the user's device.

Values for acceptable response times may differ depending on the use case, but experimental studies show that a user starts to be bored or interrupts if there is no response within one second [b-Tolia]. It seems common that users are intolerable if the reaction time takes more than one second.

As shown in Table IV.1 [b-Tolia], in the range from 150 ms to one second users become increasingly aware of the response time, and unhappy after one second.

Table IV.1 – Impact of interactive response time [b-Tolia]

Response time	Subjective impression
< 150 ms	Crisp
150 ms to one second	Noticeable to annoying
One to two seconds	Annoying
Two to five seconds	Unacceptable
Longer than five seconds	Unusable

Appendix V

Service provisioning based on CSC types in DaaS

(This appendix does not form an integral part of this Recommendation.)

This appendix describes the service provisioning based on the various types of cloud service customers. Also, several considerations of the overall service provisioning for DaaS according to the user accounting provisioning are described.

V.1 Types of cloud service customer

In DaaS, various types of CSC can exist and there are many types of service provisioning according to the type of CSC. Therefore, the classification of CSC is categorized as below:

- Classification based on service level – The CSC can be classified with the various types of service level agreement (SLA).
- Classification based on virtual desktop environment – The CSC can be classified depending on the types of virtual desktop environment. For example, some CSCs can be serviced with a virtual desktop with OS desktop in itself, and others can be serviced with a web application of virtual desktop. Also, this is related with the type of virtual desktop.
- Classification based on the allocation of the virtual desktop environment – A CSC can be served with the permanently allocated virtual desktop environment, while others can be served with a temporary virtual desktop in a virtual desktop pool.
- Classification based on the demand of resources – A CSC can be served with the virtual desktop environment of the predefined configuration or the pre-set virtual image, while others can be served with the virtual desktop environment using CSC manual configuration and resource management.

V.2 User account provisioning based on CSC types in DaaS

In clause V.1, the various types of CSC are classified. User account provisioning could be implemented in accordance with these types of CSC, and user account should also be provisioned in accordance with service provisioning in DaaS. In general, CSC can request the account in order to use a virtual desktop environment. CSC can be registered by an administrator on the CSP side or the CSC can register the account automatically. The types of user account provisioning for DaaS are listed below.

- Discretionary account provisioning – This account allows administrators to decide for themselves. This approach can be applied to the small office or home application.
- Self-service account provisioning – This account allows the CSC to participate in some aspects of the provisioning process in order to reduce the administrator's overhead and to quickly supply the virtual desktop environment to the CSC according to the manually requested resources (such as the number of CPU, amount of memory, amount of hard disk resources etc.).
- Workflow-based account provisioning – This account obtains the approvals from the designated approvers before CSC access. Also, this approach can supply the virtual desktop environments to the CSCs according to the service level with a prior approval.
- Automatic account provisioning – This requires every account to be added, using one same method, with a centralized management application or data by using the predefined procedures.

V.3 Service provisioning in DaaS

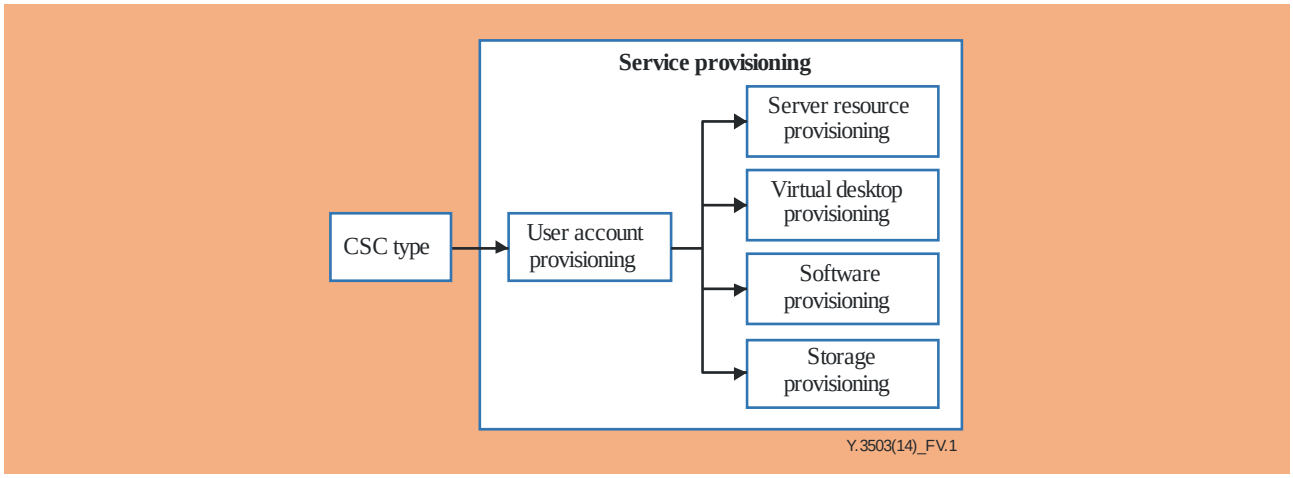


Figure V.1 – Service provisioning in DaaS system

As shown in Figure V.1, service provisioning is the design or modification of DaaS configuration to meet the various types of CSC. All types of CSC try to connect their virtual desktop environment with the client and the CSP provides the service in accordance with these types. Service provisioning consists of the following:

- Account provisioning: It makes and manages the CSC account with regard to CSC type.
- Server and resource provisioning: It supplies or manages hardware resources that are requested from the CSC.
- Virtual desktop provisioning: It generates, supplies and manages the virtual desktop environment to be allocated to the CSC.
- Software provisioning: It installs, manages or updates the software in the DaaS platform and virtual desktop environment.
- Storage provisioning: It manages and backs up offline files of virtual machine, user data and other storage-related files related to virtual desktop environment.

Bibliography

[b-ITU-T H.264] Recommendation ITU-T H.264 (2014), *Advanced video coding for generic audiovisual services*.

[b-ITU-T H.265] Recommendation ITU-T H.265 (2013), *High efficiency video coding*.

[b-ITU-T Y.2201] Recommendation ITU-T Y.2201 (2009), *Requirements and capabilities for ITU-T NGN*.

[b-ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

[b-ITU-T FGCC1] ITU-T Focus Group on Cloud Computing Technical Report (2012), *Part 1: Introduction to the cloud ecosystem: definitions, taxonomies, use cases and high-level requirements.*

[b-ITU-T FGCC2] ITU-T Focus Group on Cloud Computing Technical Report (2012), *Part 2: Functional requirements and reference architecture.*

[b-IETF RFC 768] IETF RFC 768 (1980), *User Datagram Protocol*.

[b-IETF RFC 793] IETF RFC 793 (1981), *Transmission Control Protocol*.

[b-IETF RFC 6101] IETF RFC 6101 (1996), The *Secure Sockets Layer (SSL) Protocol Version 3.0*.

[b-IETF RFC 6347] IETF RFC 6347 (2012), *Datagram Transport Layer Security Version 1.2*.

[b-DMTF OVF] DMTF Standard DSP0243 (2009), *Open virtualization format specification*.

[b-W3C-HTML5] W3C, *A vocabulary and associated APIs for HTML and XHTML*, Available at http://www.w3.org/TR/html5/.

[b-Shneiderman] Ben Shneiderman (1984), "*Response Time and Display Rate in Human Performance with Computers*", ACM Computing Survey, Vol. 16, pp. 265-285.

[b-Tolia] Niraj Tolia, David G. Andersen, and M. Satyanarayanan (2006), "*Quantifying Interactive User Experience on Thin Clients*", Computer, Vol. 39, Issue. 3, pp. 46-52.


SAAS
PAAS
Cloud
Computing
IAAS
DAAS

Desktop-as-a-Service

Functional architecture for Desktop as a Service

Recommendation ITU-T Y.3504

(06/2016)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Summary

Recommendation ITU-T Y.3504 describes Desktop as a Service (DaaS) functions and functional architecture for DaaS. This Recommendation also describes the relationship between the DaaS functional architecture and the cloud computing reference architecture.

Keywords

DaaS functional architecture, DaaS functions, Desktop as a Service, virtual desktop.

Table of Contents

1 Scope

This Recommendation provides functional architecture for desktop as a service (DaaS) to specify the detailed functions and their relationships based on the general and functional requirements of [ITU-T Y.3503]. It addresses the following subjects:

– DaaS functions;

– DaaS functional architecture;

– mapping DaaS functional architecture to the cloud computing reference architecture.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing*.

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), *Information technology – Cloud computing – Reference architecture*.

[ITU-T Y.3503] Recommendation ITU-T Y.3503 (2014), *Requirements for desktop as a service*.

[ITU-T Y.3510] Recommendation ITU-T Y.3510 (2016), *Cloud computing infrastructure requirements*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 cloud service customer [b-ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

3.1.2 cloud service provider [b-ITU-T Y.3500]: Party which makes cloud services available.

3.1.3 DaaS client [ITU-T Y.3503]: A physical device and associated software running on the device that collectively enable a cloud service user to access Desktop as a Service (DaaS).

3.1.4 Desktop as a Service [ITU-T Y.3503]: A cloud service category in which the capabilities provided to the cloud service customer are the ability to build, configure, manage, store, execute, and deliver users' desktop functions remotely.

NOTE – Examples of end user's desktop functions can include desktop interface functions for applications, data access functions for multimedia data, and control functions for input/output (I/O) devices.

3.1.5 hypervisor [ITU-T Y.3510]: A type of system software that allows multiple operating systems to share a single hardware host.

3.1.6 virtual desktop [ITU-T Y.3503]: An environment for accessing end user's desktop functions remotely.

3.1.7 virtual machine [b-DMTF OVF]: The complete environment that supports the execution of guest software.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CCM-F	Client Connection Management Function
CN-F	Connection Negotiation Function
CPC-F	Client Peripheral Connection Function
CPU	Central Processing Unit
CSC	Cloud Service Customer
CS-FS	Client Support Functions
CSP	Cloud Service Provider
CSU	Cloud Service User
DaaS	Desktop as a Service
DB	Database
DPP-F	Delivery Protocol Processing Function
FC	Functional Component
GPU	Graphic Processing Unit
HA-F	High Availability for DaaS Function
H/W	Hardware
IAM-F	Infrastructure Access Management Function
ID	Identification
I/O	Input/Output
IP	Internet Protocol
MAC	Media Access Control
MC-F	Monitoring and Controlling virtual desktop resource Function
OS	Operating System
OPM-F	Operational Policy Management for DaaS Function
PA-F	Provisioning and Allocation of virtual desktop Function
PE-F	Performance Enhancement for virtualization platform Function
PM-F	Power Management of virtual desktop resource Function
PV-F	Platform Virtualization Function
QoS	Quality of Service
RA-F	Resource Assignment Function
RAD-F	virtual desktop Resource Allocation and Distribution Function
SCUE-F	Service Continuity for User Environment Function
SC-F	Service Connection Function
UAM-F	User Access Management Function
UAPM-F	User Account and Profile Management Function
VDCD-FS	irtual Desktop Connection and Delivery Functions

VDRM-FS Virtual Desktop Resource Management Functions

VI-FS Virtualization Infrastructure Functions

VM Virtual Machine

5 Conventions

Throughout this Recommendation, the term "DaaS user" is to be understood as equivalent to "cloud service user (CSU)".

6 Relationship between DaaS logical components and DaaS functions

There are five DaaS logical components in Recommendation [ITU-T Y.3503]:

1) DaaS client;
2) connection manager;
3) resource pool;
4) virtualization infrastructure;
5) virtual desktop delivery.

NOTE – The relationship between the DaaS logical components and the cloud computing reference architecture in [ITU-T Y.3502] is described in Appendix I.

In DaaS, a connection manager is configured to establish connections to a DaaS client and manage these connections. Virtual desktops in the virtualization infrastructure are provided to DaaS users through virtual desktop delivery. The resource pool is provisioned or configured to assign optimum resources to virtual desktops for the DaaS clients. These DaaS logical components are realized by the following DaaS functions:

– virtualization infrastructure support functions: These functions support DaaS in terms of virtualization infrastructure with resource pool;
– virtual desktop connection and delivery functions: These functions configure, provision, and deliver virtual desktops in connection manager and virtual desktop delivery;
– virtual desktop resource management functions: These functions manage resources in resource pool for virtual desktops;
– DaaS client **support functions**: These functions support DaaS from a DaaS client's perspective.

Table 6-1 shows the relationship between DaaS logical components in [ITU-T Y.3503] and DaaS functions in this Recommendation.

Table 6-1 – Relationship between DaaS logical components and DaaS functions

DaaS logical components [ITU-T Y.3503]	DaaS functions This Recommendation
Virtualization infrastructure	Virtualization infrastructure support (see clause 7.1)
Connection manager	Virtual desktop connection and delivery (see clause 7.2)
Virtual desktop delivery	
Resource pool	Virtual desktop resource management (see clause 7.3)
DaaS client	DaaS client support (see clause 7.4)

7 DaaS functions

7.1 Virtualization infrastructure support

Virtualization infrastructure support functions provide the abilities to:

– offer abstracting hardware resources (see clause 7.1.1);

– allocate resources to a virtual desktop resource assignment function (see clause 7.1.2);

– improve the performance in terms of a DaaS platform (see clause 7.1.3);

– supply the interfaces to access the virtualization infrastructure (see clause 7.1.4).

7.1.1 Platform virtualization

Providing a separate virtual desktop environment for each DaaS user is a main role of the platform virtualization function. This function:

– performs abstracting hardware resources in order to assign them to a virtual desktop efficiently;

NOTE – Abstracting hardware resources has different approaches, e.g., operating-system-level virtualization and hypervisor which are configured to accommodate one or more virtual machines above hardware;

- operating-system-level virtualization is a virtualization method where the input/output (I/O) management part of a base operating system (OS) allows for multiple isolated user space instances, instead of just one. Such instances may look like a virtual desktop environment from the point of view of its DaaS users. (E.g., container based approach);
- a hypervisor is a type of system software that allows multiple OSs to share a single hardware host [ITU-T Y.3510]. It is classified into two types depending on the installation on a host machine. In the one type, hypervisors are installed and run directly on the host machine's hardware like an OS. The other type is described such a way that hypervisors are installed on an existing operating system OS of the host machine and run just as other applications do.

– coordinates invocations on central processing unit (CPU), memory, disk, network and other resources through the platform OS. Since the platform OS takes care of all the hardware, this function supports the hardware compatibility;

– consolidates multiple platforms into the pool of physically separated hardware resources;

– isolates virtual desktops not to affect the operation of a platform itself or any other virtual desktops;

– constructs the multiple systems for DaaS such as server, storage and network to serve different DaaS users.

7.1.2 Resource assignment

The resource assignment function:

– allocates the software and hardware resources to a virtual desktop;

NOTE 1 – Software resources include OS image, disk image, applications, templates and profile, etc. Hardware resources include all hardware in virtualization infrastructure such as CPU, memory, storage which is the separated space to store a user's own data and network, etc.

– provides resource interfaces to assign the hardware resources to a virtual desktop;

NOTE 2 – Resource interface includes virtual or physical device driver, virtual I/O interface and API etc.

– operates when creating virtual desktops and operates when a DaaS user requests resource changes. All resources for DaaS are managed through resource pooling. These pooled resources are prepared and managed to be provided quickly from the pre-configured environment to a DaaS user.

7.1.3 Performance enhancement for virtualization platform

The performance enhancement for virtualization platform function:

– utilizes graphic processing acceleration which uses rendering resources in both a DaaS platform and a DaaS client simultaneously;

NOTE 1 – Rendering resources include CPU, graphic processing unit (GPU) and software resources for rendering, etc. To reduce the delays in delivering high-definition display, graphic processing acceleration also adopts hardware-based compression and decompression units in a DaaS platform and a DaaS client, respectively. A DaaS platform can be also configured with vGPU.

– employs in-memory virtual desktop which is created, stored and managed on main memory to provide high-speed processing to a DaaS user. This virtual desktop environment, in main memory, is backed up when a DaaS platform is turned off and restored from backup storage with non-volatile characteristics when a DaaS platform is turned on due to the volatile characteristics of memory. In order for virtual desktop environments to be managed on small-size memory, the de-duplicated image is adopted;

NOTE 2 – the de-duplicated image in the main memory is converted to a read/write command which is transferred in blocks to the actual read/write command on the accessible main memory address.

– uses caching which is used to increase the loading rate of the virtual desktop environment at the creation step of the virtual desktop. One pre-configured virtual desktop environment (especially, OS or disk image) on shared storage is converted into copy-on-write file format stored in a memory cache and allocated to the virtual desktop;

– optimizes the delivery protocol from the created multiple paths for different DaaS user's services to improve network performance.

7.1.4 Infrastructure access management

There are three ways to access virtualization infrastructure in DaaS:

1) access for the resource allocation by provisioning;

2) access for virtual desktop over delivery protocol by a DaaS client;

3) access for the management of DaaS platforms by administrators.

Infrastructure access management function:

– grants access to the virtualization infrastructure after confirming the access authority;

– connects to the virtualization infrastructure through the interface of resource, which is allocated according to the user account and cloud service customer (CSC) type;

NOTE – Virtualization infrastructure for DaaS utilizes various cloud infrastructures from different cloud service providers (CSPs) or an individual platform owned by one CSP. Interface in this function refers to both cases.

– transmits operating commands on the virtual desktop to access the selected resources;

– maintains, changes and deletes the access authority of infrastructure which has already been established from a user request;

– applies to the separated access authorities of each resource in the infrastructure individually.

7.2 Virtual desktop connection and delivery

Virtual desktop connection and delivery functions:

– perform a delivery protocol (see 7.2.1 delivery protocol processing function);
– connect virtual desktops for a DaaS user (see 7.2.2 client connection management function);
– validate a DaaS user with user authentication (7.2.3 user access management function);
– establish a virtual desktop for a DaaS user (7.2.4 provisioning and allocation function).

7.2.1 Delivery protocol processing

The delivery protocol processing function:

– provides the communication channels through the network for exchanging information between the DaaS client and the DaaS platform;

NOTE 1 – Examples of exchanged information by the delivery protocol processing function are virtual desktop's display, video and audio data, events of input devices (e.g., mouse, keyboard), and events of other DaaS client peripherals.

– transmits virtual desktop environments to the DaaS client after the coordination process performed by the client connection management function (see clause 7.2.2) and the connection to the virtual desktop by the DaaS client with the virtual desktop access information;

NOTE 2 – Virtual desktop access information includes the information for connecting virtual desktop such as internet protocol (IP) address, URI, port number of the DaaS platform, port number of assigned virtual desktop, and password for secure connection.

– redirects virtual desktop's graphic display to a DaaS client;
– provides the compressed display to decrease the network bandwidth for high resolution and dimension display data;
– transmits video/audio data encoded and decoded with standard codec for each applicable video/audio content;
– determines connection negotiation results based on monitoring information received from the connection negotiation function (see clause 7.4.2) and the monitoring and controlling virtual desktop resource function (see clause 7.3.1);

NOTE 3 – Connection negotiation result includes screen resolution, compression rate of video and audio, transmission rate of display, and kind of video and audio codec.

– uses standard security protocols in order to protect the content exchanged between a DaaS client and a DaaS platform.

7.2.2 Client connection management

The client connection management function:

– establishes a connection to a DaaS client after DaaS user's authentication related with the user access management function (see clause 7.2.3);
– identifies CSC types (e.g., allocated user, pooled user, multi-virtual machine (VM) user) which were previously assigned from CSU's account information;

NOTE 1 – The allocated user uses its own allocated virtual desktop persistently and has its own permanent virtual desktop by adopting a pre-set method and a manual method.

NOTE 2 – The pooled user has a non-persistent virtual desktop for one-time use only. When the user terminal, divided as the pooled user is logged off from the operation server, the virtual desktop used by the user terminal is deleted. When the user terminal accesses the operation server again, a new virtual desktop is allocated to the user terminal. The operation server does not store a personal profile of the user when the access of the user terminal of the pooled user is released.

NOTE 3 – The multi-VM user is allowed to use multiple virtual desktops.

NOTE 4 – CSU's account information is registered by an administrator at the portal of a DaaS platform or the administrator's terminal to approve a DaaS user's prior permission. This information includes CSC type, user name, e-mail, telephone number, social security number and employee identification (ID), etc. This information can be maintained and provided using database (DB), active directory, or lightweight directory access protocol.

– identifies the user profile managed by the user profile management function (see clause 7.3.2) if a DaaS user has already been registered;
– coordinates with different virtualization infrastructures according to a delivery protocol, in some cases the client connection needs to be customized according to dedicated infrastructure;
– sends virtual desktop access information and/or other formats like a customized access connector software, access connection plugins in a browser to a DaaS client to proceed with client connection;
– performs connection monitoring for any type and reconnection with the connection monitoring if a DaaS client is disconnected; it also guarantees both security and quality of service (QoS) of the delivered DaaS service based on the connection;
– validates the license of the user's applications of virtual desktops.

7.2.3 User access management

The user access management function:

– validates a DaaS user with CSU's access information in logon procedure;

NOTE 1 – CSU's access information is registered at the portal of a DaaS platform or a DaaS user's terminal. This information includes ID, password, and other check items for authority. This information can be used in login procedure.

NOTE 2 – For a DaaS user who accesses DaaS for the first time, an administrator prepares CSU's access information for the DaaS user's logon procedure in advance in the user account and profile management function (see clause 7.3.2).

– accesses the user account and profile management function (see clause 7.3.2) for each DaaS client according to CSC types, the information may be used to authorize access, establish connections with DaaS-specific protocol/connection;
– notifies the result of a client connection to a DaaS client to give guides to access a DaaS platform and requests the client connection to the client connection management function (see clause 7.2.2) after validating a DaaS user, the access can be achieved through a dedicated connector software or through a web browser and plugin supporting DaaS-specific protocol;
– supports differentiated permissions according to CSC types;

NOTE 3 – The permissions are classified into authority of administration, resource access, and service access.

– supports secure access through a security protocol (such as secure shell or transport layer security) and technical access depending on the type of DaaS client such as the dedicated software, general-purpose web browser;
– maintains logs such as the date and time of the user log-on and log-off, the type of DaaS client, the location of the DaaS client, and the service usage, etc.

7.2.4 Provisioning and allocation of virtual desktop

The provisioning and allocation function:

– prepares hardware and software resources for a virtual desktop corresponding with CSU's account information, load-balancing or allocation policy;
– configures a DaaS platform with a virtual desktop delivery protocol and resource pool for virtual desktop environments;

NOTE 1 – This function involves the following processes:

- the provision for a DaaS client configured to receive the allocation of a virtual desktop;
- the provision for a connection manager to control a type of a virtual desktop to be allocated according to CSU's account and access information;
- the provision for a DaaS Platform to be selected among platforms in the datacentre or server farm on which the virtual desktop is allocated.

– configures a pre-configured virtual desktop environment (such as an OS image and a user disk image) and stores it to share for convenience and speed of the configuration;
– installs and updates software in a pre-configured virtual desktop environment as well as a DaaS platform;
– deploys a DaaS platform which scales up, down, and out including redundancy;

NOTE 2 – If a heterogeneous virtualization infrastructure is adopted, this function deploys it and prepares a new pre-configured environment compared with the previous user environment.

– determines operating status of a DaaS platform and a virtual desktop according to CSC type;

NOTE 3 – Based on the operating status, this function assigns a previously allocated virtual desktop, a temporary allocated virtual desktop, or a newly created virtual desktop on the optimum DaaS platform according to CSU's account information.

NOTE 4 – The optimum DaaS platform has best-efforts performance from the monitoring of server power or performance among DaaS platforms.

– identifies CSC type and service catalogue.

7.3 Virtual desktop resource management

Virtual desktop resource management functions:

– monitor and control states of virtual desktop resources (see clause 7.3.1 monitoring and controlling virtual desktop resource function);
– manage user accounts and profiles in terms of administrators and DaaS users (see clause 7.3.2 user account and profile management function);
– offer a virtual desktop and other resources to a DaaS user in a timely manner (see clause 7.3.3 virtual desktop resource allocation and distribution function);
– establish operational policy (see clause 7.3.4 operational policy management for DaaS function);
– offer high availability (see clause 7.3.5 high availability for DaaS function);
– supply management of power consumption (see clause 7.3.6 power management of virtual desktop resource function).

7.3.1 Monitoring and controlling virtual desktop resource

In the monitoring and controlling virtual desktop resource function, monitored and controlled targets for DaaS are mainly virtualization infrastructure and virtual desktops. Monitoring information is classified into static and run-time data.

NOTE 1 – The exchanged monitoring information is communicated through a protocol between a monitoring target and virtualization infrastructure. A software agent or daemon activated in virtualization infrastructure is used to gather monitoring information which is stored as a form of database or other file formats. This database is normally accessible by other functions.

The monitoring and controlling virtual desktop resource function:

– monitors the information of virtualization infrastructure to gather by event processing during running DaaS;

NOTE 2 – The monitoring information of virtualization infrastructure is as follows:

- basic information of virtualization infrastructure: machine's host name, machine type;
- hardware (H/W) resource for virtualization infrastructure: total memory space, the number of CPUs, total storage space, machine's IP address, media access control (MAC) address, the availability for performance enhancement, estimated power;
- virtualization related resource: hypervisor information, the number of currently running virtual desktops, the supported maximum number of virtual desktops, supported OSs.

– monitors the information for each virtual desktop to gather by event processing;

NOTE 3 – The monitoring information of virtual desktops is as follows:

- basic information of a virtual desktop: virtual desktop ID, OS type, hypervisor type, current status;
- H/W resource for virtual desktop: assigned memory space, the assigned number of CPUs, assigned storage space, virtual desktop's IP address, virtual desktop's MAC address, accessible port number, performance enhancement factor.

– monitors the run-time information of virtualization infrastructure and virtual desktop. This monitoring information is dynamically monitored at run-time and usually checked periodically;
NOTE 4 – The run-time information includes CPU utilization, memory utilization, storage utilization, network utilization, etc.

– performs the controls by a DaaS user and an administrator.
NOTE 5 – Following are the controls at both sides:
- DaaS user's controls: virtual desktop state controls such as on, create, reset, pause, resume, and off:
  – on/off: turn on or turn off a virtual desktop;
  – create: make a new virtual desktop;
  – reset: reboot the OS of a virtual desktop;
  – pause/resume: pause the OS maintaining a connection and resume the OS from a pause status;
  – delete: elimination of a virtual desktop.
- administrator's controls: virtual desktop state controls, resource modification (CPU change, memory change, storage change, adding/deleting USB, network selection etc.), virtual desktop migration.

7.3.2 User account and profile management

CSU's accounts are separated into two types as follows:

1) administrative account for an administrator who has the authority to control and manage a system;
2) general user account combined with CSC types such as service level, the type of virtual desktop, the authority of resource utilization, and the virtual desktop persistence user or not. See [ITU-T Y.3503].

The user account and profile management function:

– classifies each CSC type and clarifies the service catalogue since different DaaS users have their own accounts and profiles;
– manages CSU's accounts and profiles to guarantee correct access to their resources;
– maintains CSU's account information and provides it to the user access management function (see clause 7.2.3);
– maintains types of profiles such as virtual desktop user profile and virtual desktop hardware profile in order to build and maintain DaaS user's individual virtual desktop environments;
NOTE 1 – Virtual desktop user profile consists of desktop preferences and the CSU's application settings, etc.
NOTE 2 – Virtual desktop hardware profile includes the specific hardware configuration information to be allocated to a DaaS user and the information for booting-up procedure, etc.
NOTE 3 – Since virtual desktop hardware profile depends on physical hardware in virtualization infrastructure, the physical hardware information from hypervisor or platform is collected and stored.
– generates profiles from CSU's account information or the pre-configured virtual desktop environment (such as virtual desktop user profile or template). These generated profiles are bound to CSU's accounts and are reflected in a corresponding virtual desktop;
– saves profiles whenever they are changed;
NOTE 4 – For a particular CSC type (such as non-persistence), this function does not save the profile. In this case, this function provides new profiles whenever a DaaS user connects a virtual desktop.
– prepares and provides new virtual desktop user profiles and hardware profiles by comparing physical hardware information with the pre-configured environment.

7.3.3 Virtual desktop resource allocation and distribution

The virtual desktop resource allocation and distribution function is manually accessed by an administrator or dynamically operated by the operational policy management function (see clause 7.3.4). The virtual desktop resource allocation and distribution function:

– receives the resource usage from the monitoring and controlling virtual desktop resource function (see clause 7.3.1) and provides an administrator or a resource scheduler with the analysis of resource usage statically or dynamically;

NOTE – This analysis includes the resource usage state, resource usage pattern, and modification history, etc. A resource scheduler requests the resource distribution to virtualization infrastructure based on the analysis of resource usage.

– determines resources to be allocated to or released from a virtual desktop, respectively, through the interface of the resource assignment function (see clause 7.1.2);

– provides the interfaces to allocate and distribute the resources for the pre-configured virtual desktop environment when a virtual desktop is created or changed;

– applies the operational policy dynamically or manually from the operational policy management function (see clause 7.3.4);

– allocates and distributes resources dynamically to a virtual desktop according to the operational policy (such as setting the threshold of resource usage) when its resources are insufficient or overloaded;

– modifies or reallocates resources to satisfy the performance of a virtual desktop from a DaaS user's request.

7.3.4 Operational policy management for DaaS

The operational policy management for DaaS function:

– establishes DaaS user's group policies according to CSC types and user accounts;

NOTE 1 – These polices are reflected in the individual user account related with a virtual desktop user profile and a pre-configured environment.

– establishes a group policy to apply to the virtualization infrastructure or virtual desktops which use the same operational policy;

NOTE 2 – If a DaaS user utilizes similar applications, tasks and usage patterns, they are grouped and assigned to the same virtualization infrastructure with sharing resources.

NOTE 3 – A DaaS user's usage pattern is the information about a DaaS user's average usage of resources (e.g., CPU, memory, network and disk) from the monitoring information for a certain period. The virtualization infrastructure with DaaS user's similar tasks and usage patterns can improve performance by the caching process to provide a virtual desktop when the virtual desktop performs the similar tasks running on it.

– establishes a policy of the limitation or the arbitration for resource usage to prohibit the performance degradation from the assignment of excessive resources;

NOTE 4 – In order to satisfy different DaaS user's requirements, different operational policies are reflected in each resource (such as an application policy, a network plolicy, other resource policies).

– requests the reallocation of insufficient resources, when some resources are needed more for some CSC types;

NOTE 5 – During this process, this function detects which resources are dominantly used from a DaaS user's usage pattern according to a DaaS user's tasks.

– provides a policy to assign the DaaS platforms on which a virtual desktop is running;

NOTE 6 – This function considers the physical distance on the network from a DaaS user to a DaaS platform and sets the policy on the shortest path. Otherwise, this function considers power consumption or utilization of the platform according to the weighted resource usage or the number of virtual desktops operated in one platform and sets the policy on the lowest utilization rate or the fewest number of virtual desktops. Also, if DaaS users perform similar tasks and requests specific virtual desktop by CSC type, this function considers the allocation of the pre-classified groups.

– gathers information on the platform power consumption or utilization according to the weighted resource usage from the power management function (see clause 7.3.6);

NOTE 7 – The weighted resource usage mean which resources are heavily used as usual; the platform power consumption is estimated by the sum of these usages.

– performs the scheduling from the policies about a DaaS user's usage pattern and power consumption in virtualization infrastructure;

– sends a policy to the allocation function (see clause 7.2.4) to select the virtualization infrastructure to operate a virtual desktop;

– establishes a backup policy which covers types and frequency of backing up the virtual desktop enviorment to prepare for a system disaster;

– provides user interfaces for established policies which are established and applied dynamically or manually by the administrator.

7.3.5 High availability for DaaS

For high availability, DaaS adopts platform clustering which includes connection manger and virtualization infrastructure to maintain the seamless DaaS user's connection in a failure occurrence situation. The high availability for DaaS function:

– detects a system failure by confirming states among DaaS platforms;

– ensures DaaS users have a stable running environment in terms of delivery and operation of virtual desktops;

– sets up the redundancy for the client connection management function (see clause 7.2.2) to perform failover with minimum downtime and connection continuity;

NOTE 1 – The redundancy for the client connection management function (see clause 7.2.2) includes the duplication by active-active form or active-standby form. In order not to lose the DaaS user's connection, CSU's account and access information (such as DB, license or active directory) are duplicated or mirrored.

– configures the failover to redundancy for virtualization infrastructure;

NOTE 2 – The redundancy for virtualization infrastructure (such as the redundant server on active state for virtual desktop environments) is configured to perform failover for minimizing downtime. It helps to allocate a virtual desktop by load balancing or migrating a virtual desktop to the activated server to a DaaS client when the failure occurs on the server to which the virtual desktop is allocated, by providing a service without the loss of the user environment.

– saves the user's environment during a certain time and backs up and restores it on a local disk or on shared storage, thus preventing the loss of the user environment.

7.3.6 Power management of virtual desktop resource

The power management of virtual desktop resources function manages the power consumption of a DaaS platform with virtual desktop resources. This function:

– monitors the power consumption and the related performance factors of a virtual desktop and each resource in a DaaS platform;

– calculates the variation of power consumption and performance of a virtual desktop or a DaaS platform by collecting monitoring information;

– supports other functions for the provisioning and allocation of virtual desktop function (see clause 7.2.4) or the operational policy management for DaaS function (see clause 7.3.4).

7.4 Client support

Client support function:

– establishes a connection for a virtual desktop on the client side (see clause 7.4.1 service connection function);

– supports the optimized user interaction on a DaaS client (see clause 7.4.2 connection negotiation function);

– handles peripherals on a DaaS client (see clause 7.4.3 client peripheral connection function);

– guarantees that the virtual desktop service remains turned on (see clause 7.4.4 service continuity for user environment).

7.4.1 Service connection

The service connection function supports a DaaS client to establish a connection for virtual desktop service. This function:

– transmits CSU's access information to the user access management function (see clause 7.2.3) to verify a DaaS user;

– exchanges virtual desktop access information with the client connection management function (see clause 7.2.2) after user authentication;

– supports various types of DaaS clients such as personal computer, laptop computer, tablet computer, and thin client to access a virtual desktop;

– periodically sends the connection state of the DaaS client to the client connection management function (see clause 7.2.2) to monitor the client state for the preservation of the client connection. In case of a temporarily unavailable connection, the DaaS client notifies the connection state to a DaaS user;

– transmits the DaaS user's requests (i.e., additional resource, resources cancelling, and additional virtual desktop service) to the client connection management function (see clause 7.2.2);

– maintains a standard security connection to protect the content exchanged between a DaaS client and a DaaS platform.

7.4.2 Connection negotiation

The connection negotiation function considers two main factors for DaaS: network performance (e.g., network bandwidth or traffic information) between a DaaS client and a DaaS platform; and the client state of a DaaS client. Based on these two main factors, it supports the optimized user interaction on the DaaS client.

The connection negotiation function:

– gathers network performance information and the client state, and transmits them to a DaaS platform through a network;

NOTE 1 – The client state consists of static and dynamic information of a DaaS client such as specification of display, usage and specification of hardware resources (i.e., CPU, GPU, and memory), and user interaction methods supported on a DaaS client.

NOTE 2 – The static information is collected at the initial connection between a DaaS client and a DaaS platform after user verification. The dynamic information is collected periodically when the client is connected to the DaaS platform to use a virtual desktop service.

– allows a DaaS client to display with best-efforts resolution for client without delay;

– receives the negotiation results from a DaaS platform after the completion of a negotiation;

– reflects the negotiation results in a DaaS client.

7.4.3 Client peripheral connection

The client peripheral connection function:

– recognizes peripherals on a DaaS client when they are connected to the DaaS client;

– sends a connection request event to a DaaS platform according to the type of DaaS client;

NOTE 1 – When this function requests the connection of the peripheral, the DaaS platform executes a device driver on a virtual desktop to operate the client peripheral remotely on a DaaS client.

– transmits the control events (such as attachment and detachment) and data for the client peripherals to a DaaS platform through a delivery protocol;

– disconnects the peripheral on a DaaS client safely.

NOTE 2 – When a DaaS user want to disconnect a peripheral on the assigned virtual desktop, this function disconnects the peripheral on the virtual desktop through the removal control event of the peripheral on the DaaS platform.

7.4.4 Service continuity for user environment

The service continuity for user environment function provides a DaaS client with a reconnection to provide for the continuity of service against the network failure or any faults of a DaaS platform. This function:

– requests a reconnection to the client connection management function (see clause 7.2.2) in case of a connection failure in order to maintain continuous virtual desktop service;

– reconnects a virtual desktop running on a DaaS client with an available DaaS platform;

– saves the DaaS user states of the virtual desktop on the DaaS client;

NOTE – The DaaS user state includes data, working environments for a DaaS user, etc.

– synchronizes the saved user states of the virtual desktop on the DaaS client with user states of the virtual desktop on the DaaS platform when the DaaS client is reconnected to the DaaS platform.

7.5 Relationships among DaaS functions

Figure 7.1 depicts the summary of the relationships among the DaaS functions described in clause 7.1 through 7.4. Each link between two functions has related information.

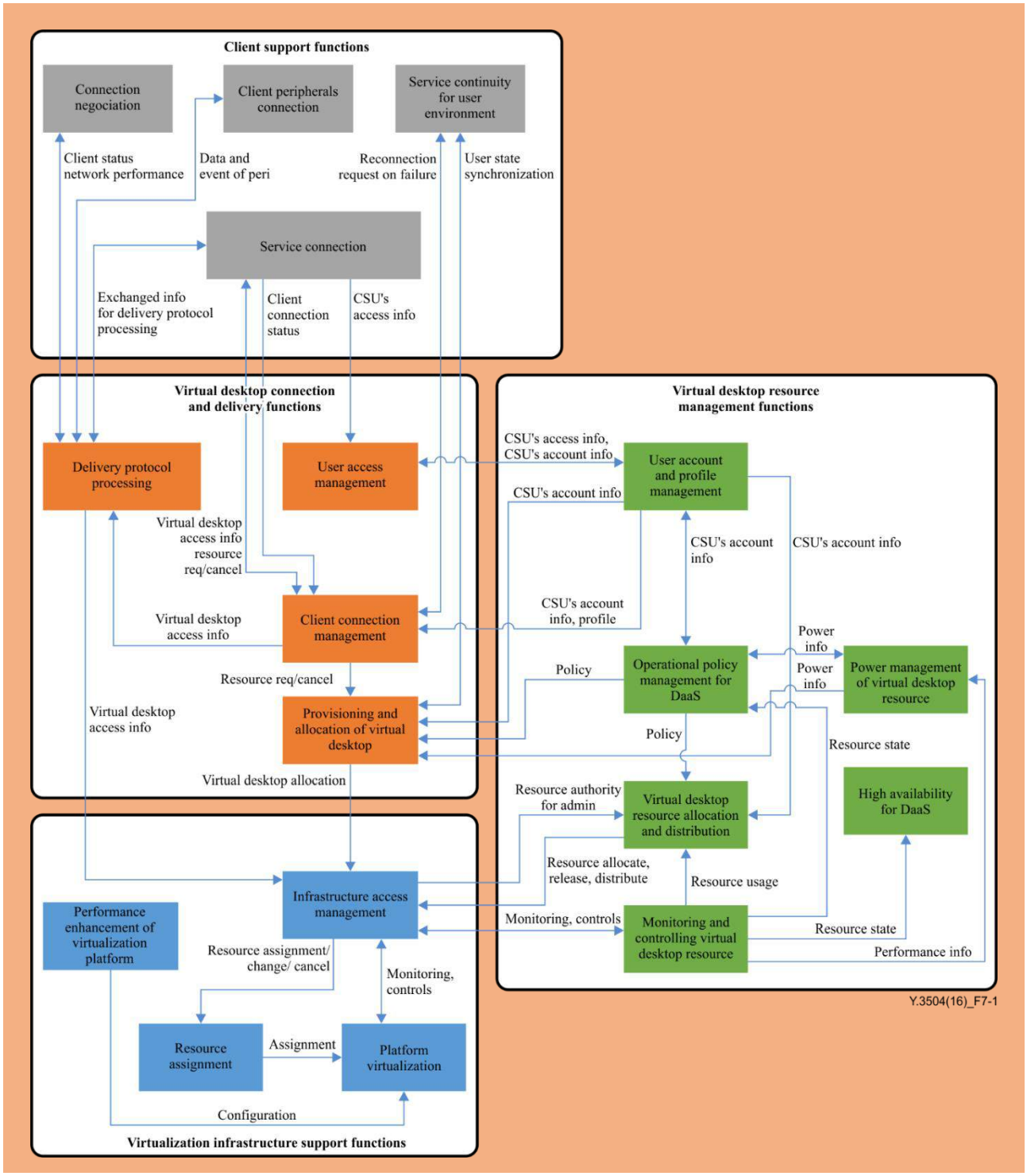


Figure 7-1 – Relationships among DaaS functions

8 Relationships between DaaS functions and functional components of cloud computing reference architecture

Figure 8-1 shows the mapping between the DaaS functions in clause 7 and the functional components in [ITU-T Y.3502].

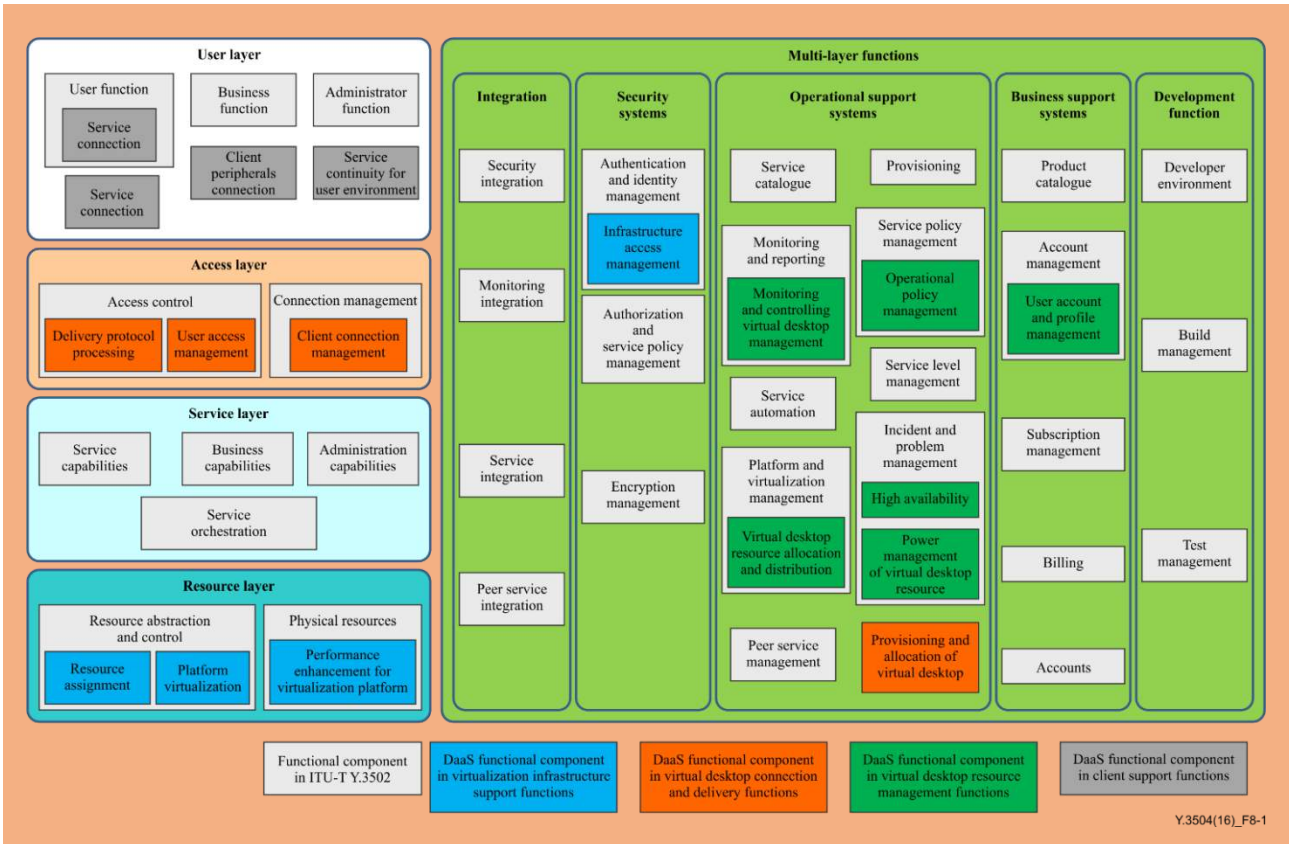


Figure 8-1 – Mapping between DaaS functions and functional components of cloud computing reference architecture

Among the 18 DaaS functions identified in clause 7, 14 of these can be mapped to functional components in [ITU-T Y.3502]. These mappings, in terms of the layering framework, are as follows:

– User layer:
  - user function: service connection function (see clause 7.4.1)

– Access layer:
  - access control functional component: delivery protocol processing function (see clause 7.2.1), user access management function (see clause 7.2.3)
  - connection management functional component: client connection management function (see clause 7.2.2)

– Resource layer:
  - resource abstraction and control functional component: resource assignment function (see clause 7.1.2), platform virtualization function (see clause 7.1.1)
  - physical resources functional component: performance enhancement for virtualization platform function (see clause 7.1.3)

– Multi-layer functions:
  - security systems functional component-authentication and identity management: infrastructure access management function (see clause 7.1.4)

- operational support systems functional component-monitoring and reporting: monitoring and controlling virtual desktop resource function (see clause 7.3.1)
- operational support systems functional component-service policy management: operational policy management for DaaS function (see clause 7.3.4)
- operational support systems functional component-platform and virtualisation management: virtual desktop resource allocation and distribution function (see clause 7.3.3)
- operational support systems functional component-incident and problem management: high availability for DaaS function (see clause 7.3.5), power management of virtual desktop resource function (see clause 7.3.6)
- business support systems functional component-account management: user account and profile management function (see clause 7.3.2)

There are four DaaS functions that are not mapped to any functional components in [ITU-T Y.3502]; they can be located in the layering framework as follows:

– User layer:
  - connection negotiation function (see clause 7.4.2), client peripheral connection function (see clause 7.4.3), service continuity for user environment function (see clause 7.4.4)

– Multi-layer functions:
  - operational support systems functional component: provisioning and allocation of virtual desktop function (see clause 7.2.4)

The detailed mapping is in Appendix II.

Since there are no reference points among functional components in [ITU-T Y.3502], it is necessary to adopt the grouping of DaaS functions in order to specify their reference points for convenience. Clause 9 explains the reference points based on four groups of DaaS functions as in Figure 7-1, i.e., client support functions, virtual desktop connection and delivery functions, virtual desktop resource management functions, and virtualization infrastructure functions.

9 DaaS functional architecture

9.1 Client support functions

The client support functions (CS-FS) have four functions including: connection negotiation function (CN-F), client peripheral connection function (CPC-F), service connection function (SC-F), and service continuity for user environment function (SCUE-F) as shown in Figure 9-1. The CS-FS interfaces with only the virtual desktop connection and delivery functions (VDCD-FS).

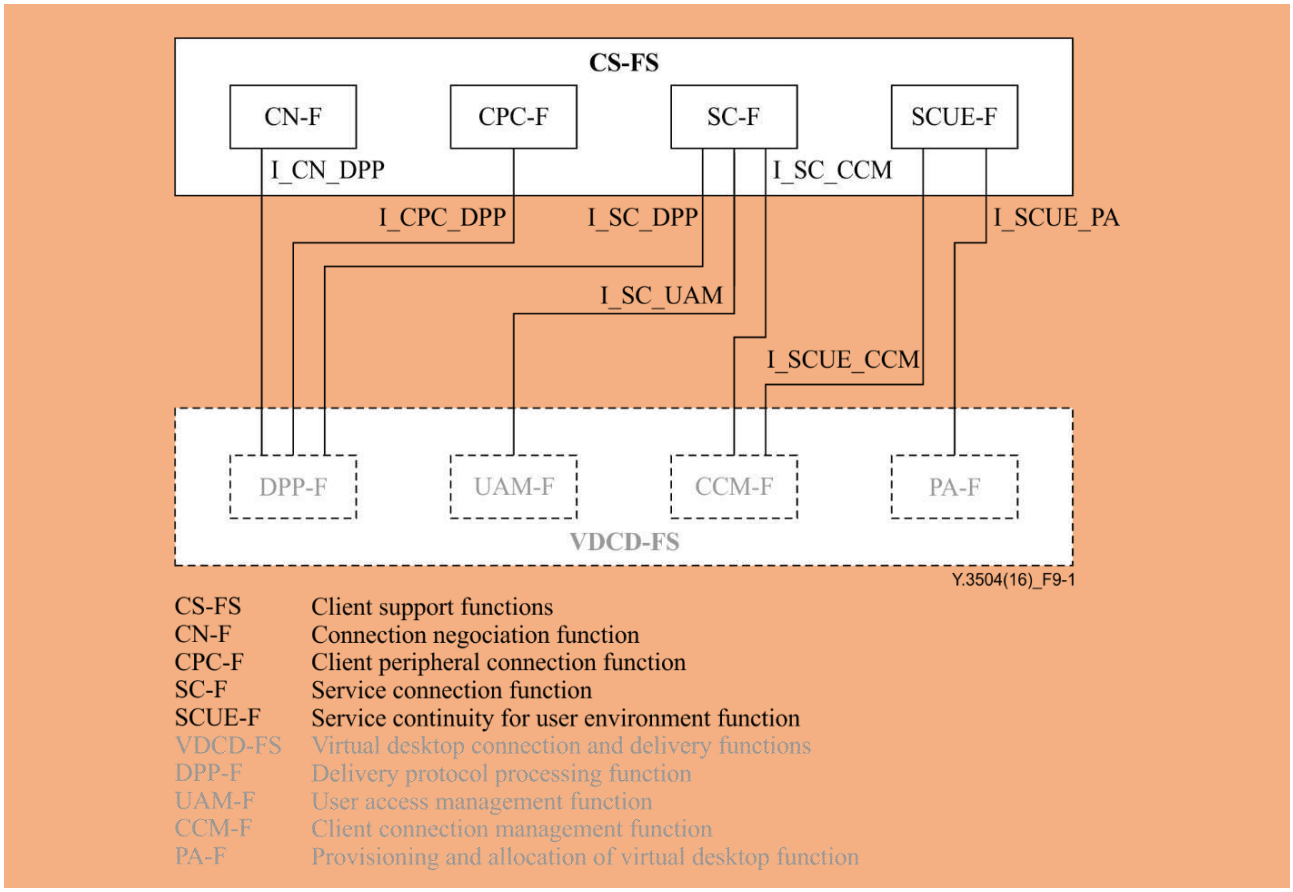


Figure 9-1 – Functions and reference points in CS-FS

9.1.1 Service connection function

The SC-F connects a virtual desktop in the CS-FS while the user access management function (UAM-F) and client connection management function (CCM-F) are the counterparts to the same operations in the VDCD-FS. The SC-F sends CSU's access information to the UAM-F through I_SC_UAM to perform user authentication. The SC-F exchanges the virtual desktop access information with the CCM-F through I_SC_CCM to connect a virtual desktop. In addition, the SC-F delivers the DaaS client's connection state and additional resource request/cancellation to the delivery protocol processing function (DPP-F) though I_SC_DPP. Detailed functional description for the SC-F is specified in clause 7.4.1.

9.1.2 Connection negotiation function

The CN-F provides the CS-FS with the user interaction by using negotiation results. The CN-F gathers network performance information and the DaaS client state, and delivers them to the VDCD-FS through I_CN_DPP. Consequently, the CN-F also receives the negotiation result from the DPP-F in the VDCD-FS thorough I_CN_DPP. Detailed functional description for the CN-F is specified in clause 7.4.2.

9.1.3 Client peripheral connection function

The CPC-F handles DaaS client's peripherals on a DaaS client. When the CPC-F recognizes the peripherals, all sorts of peripheral events (e.g., a connection and control events) are sent to the VDCD-FS though I_CPC_DPP. A detailed functional description for the CPC-F is specified in clause 7.4.3.

9.1.4 Service continuity for user environment function

The SCUE-F maintains the same user environment even on abnormal network state. When the network is disconnected, the SCUE-F requests the reconnection to the CCM-F through I_SCUE_CCM. And, the SCUE-F synchronizes the DaaS user's states between the CS-FS and the provisioning and allocation of virtual desktop function (PA-F) through I_SCUE_PA. A detailed functional description for the SCUE-F is specified in clause 7.4.4.

9.2 Virtual desktop connection and delivery functions

The VDCD-FS comprise DPP-F, UAM-F, CCM-F, and PA-F as shown in Figure 9-2. The VDCD-FS have three interfaces with other functional groups such as CS-FS, virtual desktop resource management functions (VDRM-FS), and virtualization infrastructure functions (VI-FS).

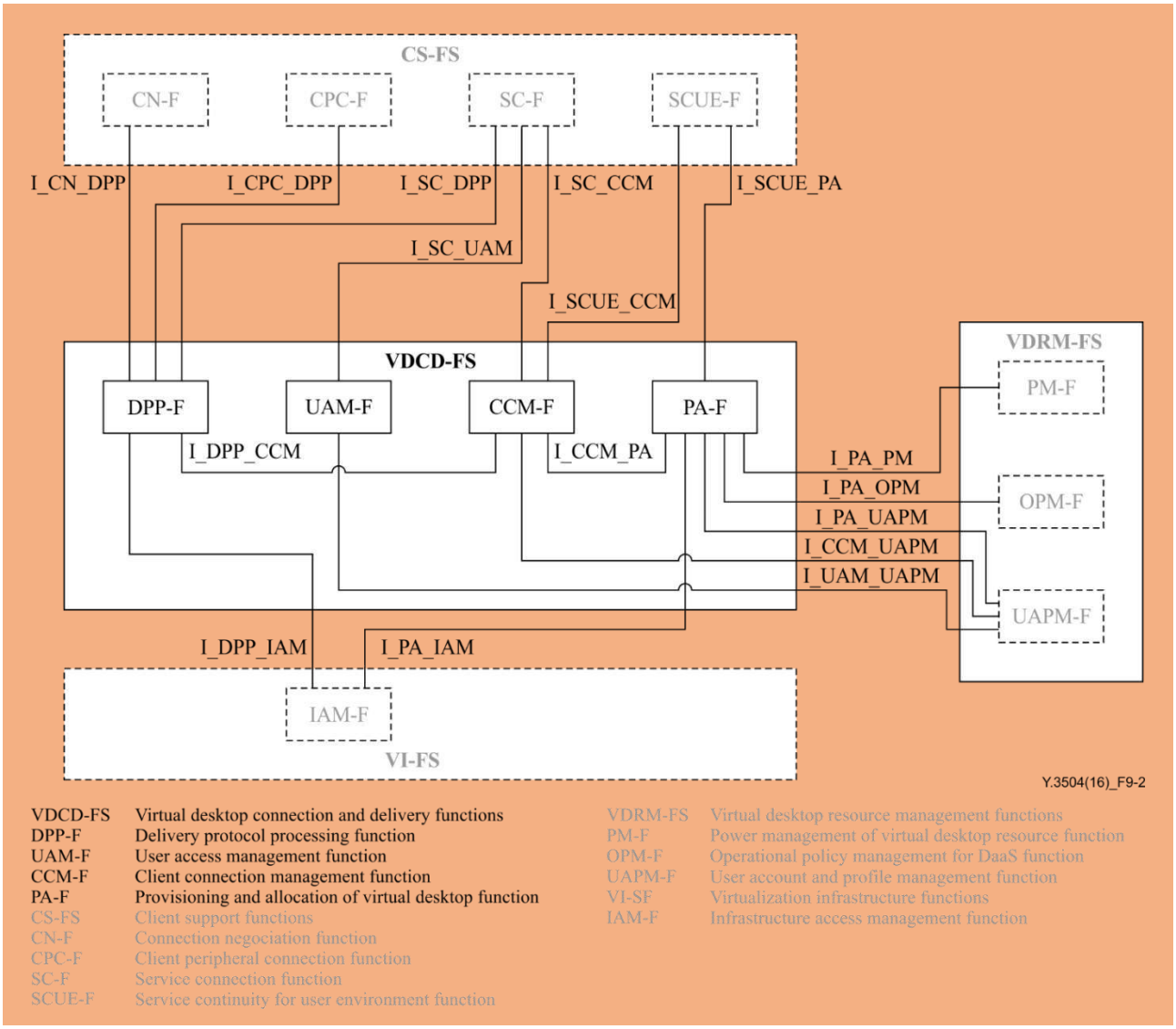


Figure 9-2 – Functions and reference points in VDCD-FS

9.2.1 Delivery protocol processing function

The DPP-F delivers the exchanged information to the SC-F through I_SC_DPP. The DPP-F communicates to the CN-F and the CPC-F to perform the connection negotiation and peripheral event through I_CN_DP and ICP_DP, respectively. Virtual desktop access information from the CCM_F on I_DP_CCM is forwarded to VI-FS through I_DPP_IAM. A detailed functional description for the DPP-F is specified in clause 7.2.1.

9.2.2 User access management function

For user authentication, the UAM-F validates a DaaS user with CSU's access information through I_SC_UAM and connects the user account and profile management function (UAPM-F) through I_UAM_UAPM with CSU's access information and CSU's account information. A detailed functional description for the UAM-F is specified in clause 7.2.3.

9.2.3 Client connection management function

The CCM-F delivers and verifies virtual desktop access information to CS-FS through I_SC_CCM. Virtual desktop access information from the SC-F is transferred to the DPP-F through I_DP_CCM. The CCM-F also

uses I_CCM_UAPM to refer to CSC types and profiles from the UAPM-F. A resource request/cancellation is delivered by I_SC_CCM and transferred to PA-F thorough I_CCM_PA. Additionally, the CCM-F receives the client connection state from the SC-F through I_SC_CCM to monitor virtual desktop connection and reconnection requests from the SCUE-F through I_SCUE_CCM against network failure. A detailed functional description for the CCM-F is specified in clause 7.2.2.

9.2.4 Provisioning and allocation of virtual desktop function

In order to configure the pre-configured virtual desktop environment or create new virtual desktops, the PA-F uses I_PA_PM, I_PA_OPM, and I_PA_UAPM to get power performance information, policies, and CSU's account information, respectively. After configuration of a virtual desktop, the PA-F allocates the virtual desktop using VI-FS through I_PA_IAM. The PA-F also synchronizes the DaaS user's state with the SCUE-F through I_SCUE_PA. Detailed functional description for the PA-F is specified in clause 7.2.4.

9.3 Virtual desktop resource management functions

The VDRM-FS are composed of monitoring and controlling virtual desktop resource function (MC-F), UAPM-F, virtual desktop resource allocation and distribution function (RAD-F) and operational policy management for DaaS function (OPM-F). VDRM-FS also includes high availability for DaaS function (HA-F) and power management of virtual desktop resource function (PM-F) for more effective management. Figure 9-3 shows VDRM-FS with two interconnections of VDCD-FS and VI-FS.

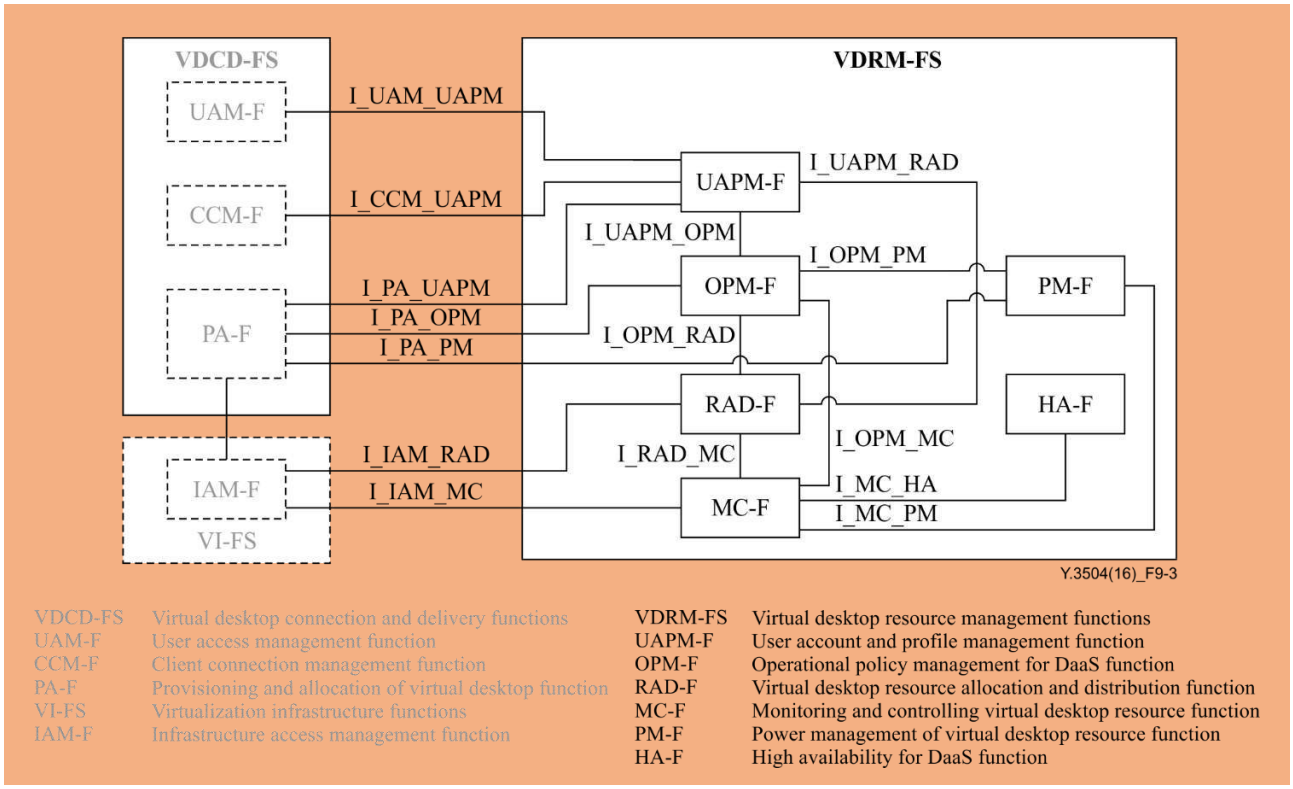


Figure 9-3 – Functions and reference points in VDRM-FS

9.3.1 Monitoring and controlling virtual desktop resource

The MC-F has the connection with virtualization infrastructure through I_IAM_MC to receive monitoring information or send the control commands from or to the infrastructure access management function (IAM-F). The MC-F is connected with the HA-F through I_MC_HA and with the OPM-F through I_OPM_PM for the resource state. The MC-F also sends monitoring information of resources and resource usages to the PM-F and RAD-F with I_MC_PM and I_OPM_MC, respectively. Detailed functional description for the MC-F is specified in clause 7.3.1.

9.3.2 User account and profile management

The UAPM-F creates CSU's account with CSU's access information through I_UAM_UAPM. The UAPM-F has two more reference points I_CCM_UAPM and I_PA_UAPM for authentication with CSU's account information and for the pre-configured environments and profiles, respectively. When RAD-F allocates and distributes resources, the UAPM-F provides CSU's account information on I_UAPM_RAD or I_UAPM_OPM. Detailed functional description for the UAPM-F is specified in clause 7.3.2.

9.3.3 Virtual desktop resource allocation and distribution

The RAD-F has a reference point of MC-F through I_RAD_MC with monitoring information to analyse resource usage. I_IAM_RAD enables the RAD_F to approach IAM-F and resource assignment function (RA-F) for resource assignment. A detailed functional description for the RAD-F is specified in clause 7.3.3.

9.3.4 Operational policy management for DaaS

The OPM-F has two reference points I_OPM_PM and I_OPM_MC to receive the performance or resource usage which is used to establish the policies. These policies are applied to PA-F with I_PA_OPM. A detailed functional description for the OPM-F is specified in clause 7.3.4.

9.3.5 High availability for DaaS

The HA-F has only the reference point with the MC-F through I_MC_HA in order to monitor the resource state for establishing the related policies. A detailed functional description for the HA-F is specified in clause 7.3.5.

9.3.6 Power management of virtual desktop resource

The PM-F collects performance information from the MC-F through I_MC_PM and transfers the power related information to the PA-F through I_PA_PM for efficient provisioning. A detailed functional description for the PM-F is specified in clause 7.3.6.

9.4 Virtualization infrastructure functions

The VI-FS has four functions including performance enhancement for virtualization platform function (PE-F), IAM-F, RA-F, and platform virtualization function (PV-F) as shown in Figure 9-4. The VI-FS provide the interfaces with the other two function groups, VDCD-FS and VDRM-FS.

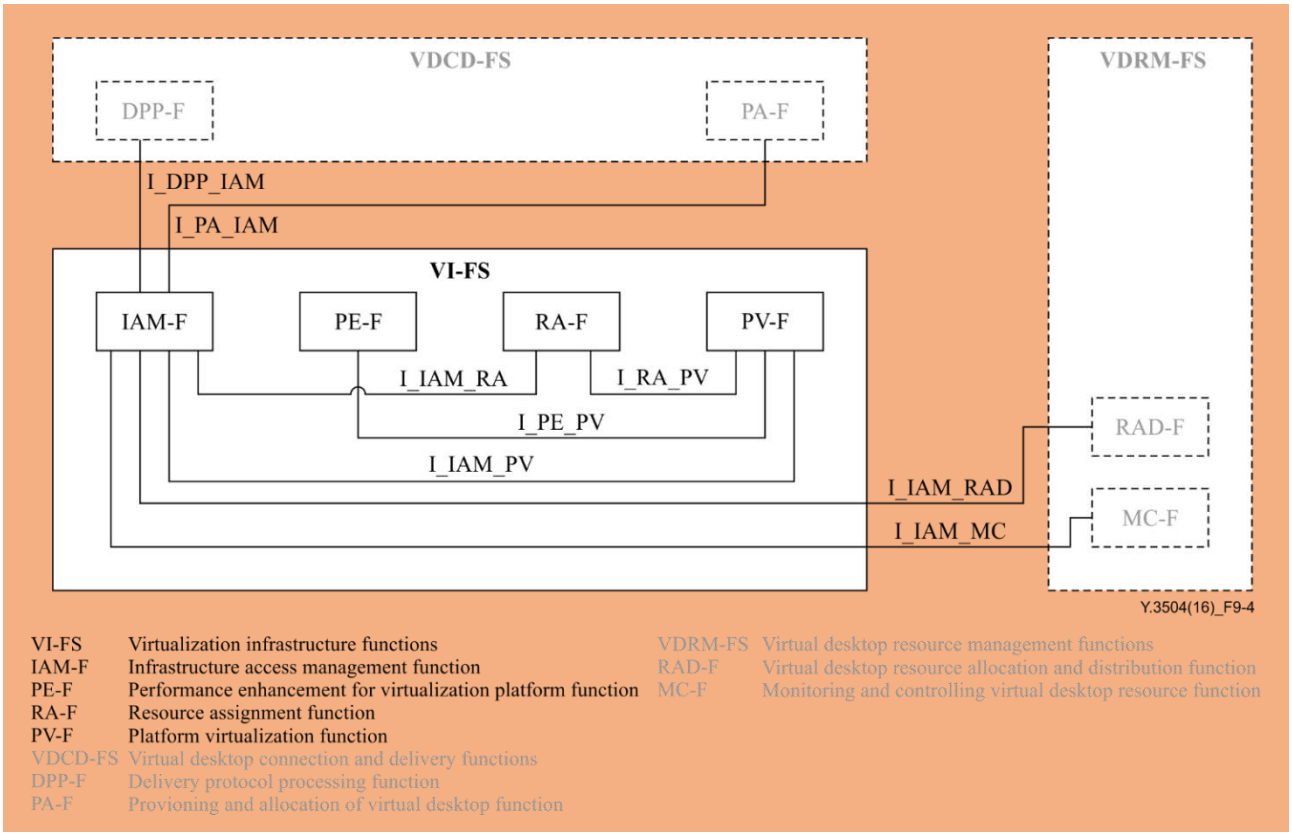


Figure 9-4 – Functions and reference points in VI-FS

9.4.1 Infrastructure access management function

The IAM-F approves virtual desktop resource allocation through I_PA_IAM and the virtual desktop access through I_DPP_IAM. The IAM-F authorizes resource access from the administrator in order for the RAD-F to allocate, release, change and distribute resources through the I_IAM_RAD. The IAM-F also sends the request for resource assignment, change and cancellation from the RAD-F to the RA-F through I_ IAM _RA. Finally, the IAM-F delivers monitoring information and controls through the I_IAM_MC. A detailed functional description for the IAM-F is specified in clause 7.1.4.

9.4.2 Performance enhancement for virtualization platform function

The PE-F enhances the performance of virtualization platform and virtual desktop. The PE-F configures virtualization platform or infrastructure with the PV-F through the I_PE_PV. A detailed functional description for the PE-F is specified in clause 7.1.3.

9.4.3 Resource assignment function

The RA-F receives the resource assignment which is sent through the IAM-F during the creation of a virtual desktop. The RA-F assigns the resources to the virtual desktop on the PV-F through I_RA_PV according to the request from the IAM-F. According to the resource change from the IAM-F, the RA-F re-assigns the resources to the PV-F through the I_RA_PV. A detailed functional description for the RA-F is specified in clause 7.1.2.

9.4.4 Platform virtualization function

The PV-F configures the DaaS platform according to the PE-F. The PV-F transmits the monitoring information and receives controls through I_IAM_PV. A detailed functional description for the PV-F is specified in clause 7.1.1.

9.5 Reference points

9.5.1 Reference points between CS-FS and VDCD-FS

The reference points between CE-FS and VDCD-FS are summarized as follows:

I_CN_DPP reference point between CN-F and DPP-F. The CN-F interacts with the DPP-F to handle connection negotiation through this reference point.

I_CPC_DPP reference point between CPC-F and DPP-F. The CPC-F interfaces with the DPP-F to exchange the peripheral events through this reference point.

I_SC_DPP reference point between SC-F and DPP-F. The SC-F requests or cancels additional resources through this reference point.

I_SC_UAM reference point between SC-F and UAM-F. The SC-F inputs the user authentication information to the UAM-F through this reference point.

I_SC_CCM reference point between SC-F and CCM-F. The SC-F and the CCM-F interact with each other to exchange virtual desktop access information through this reference point.

I_SCUE_CCM reference point between SCUE-F and CCM-F. The SCUE-F requests a reconnection to the CCM-F in case of network failure, through this reference point.

I_SCUE_PA reference point between SCUE-F and PA-F. The SCUE-F and PA-F perform the synchronization of a DaaS user's state through this reference point.

9.5.2 Reference points between VDCD-FS and VDRM-FS

I_UAM_UAPM reference point between UAM-F and UAPM-F. CSU's access information, CSU's account information, and CSC types are transferred through this reference point.

I_CCM_UAPM reference point between CCM-F and UAPM-F. CSC types and profiles are delivered from the UAPM-F to the CCM-F through this reference point.

I_PA_UAPM reference point between PA-F and UAPM-F. CSU's account information is delivered from the UAPM-F to the PA-F through this reference point.

I_PA_OPM reference point between PA-F and OPM-F. Operational policy information is delivered from the OPM-F to the PA-F through this reference point.

I_PA_PM reference point between PA-F and PM-F. Power information is delivered from the PM-F to the PA-F through this reference point.

9.5.3 Reference points between VDCD-FS and VI-FS

I_DPP_IAM reference point between DPP-F and IAM-F. Resource request/cancellation and virtual desktop access information are forwarded to IAM-F through this reference point.

I_PA_IAM reference point between PA-F and IAM-F. The PA-F delivers virtual desktop allocation information to IAM-F through this reference point.

9.5.4 Reference points between VDRM-FS and VI-FS

I_IAM_RAD reference point between IAM-F and RAD-F. The RAD-F accesses IAM-F to communicate with the RA-F.

I_IAM_MC reference point between IAM-F and MC-F. The MC-F accesses IAM-F to communicate with PV-F.

9.5.5 Reference points within VDCD-FS

I_DPP_CCM reference point between DPP-F and CCM-F. Virtual desktop access information from CCM-F is delivered to DPP-F through this reference point.

I_CCM_PA reference point between CCM-F and PA-F. The CCM-F bypasses resource request/cancellation to the PA-F through this reference point.

9.5.6 Reference points within VDRM-FS

I_UAPM_OPM reference point between UAPM-F and OPM-F. CSU's account information is communicated through this reference point.

I_UAPM_RAD reference point between UAPM-F and RAD-F. CSU'S account information is sent from UAPM-F to RAD-F though this reference point.

I_OPM_PM reference point between OPM-F and PM-F. The PM-F delivers the power performance to OPM-F to establish a policy through this reference point.

I_OPM_RAD reference point between OPM-F and RAD-F. Operational policy information is delivered from the OPM-F to the RAD-F through this reference point.

I_OPM_MC reference point between OPM-F and MC-F. The MC-F sends resource states to the OPM-F through this reference point.

I_RAD_MC reference point between RAD-F and MC-F. The MC-F sends resource usage to the RAD-F through this reference point.

I_MC_HA reference point between MC-F and HA-F. The MC-F sends resource states to the HA-F through this reference point.

I_MC_PM reference point between MC-F and PM-F. The MC-F sends monitoring information to the PM-F through this reference point.

9.5.7 Reference points within VI-FS

I_IAM_RA reference point between IAM-F and RA-F. The resource allocation and distribution is forwarded to the RA-F through this reference point.

I_PE_PV reference point between PE-F and PV-F. The configuration to enhance the performance of virtualization platform is sent to the PV-F through this reference point.

I_RA_PV reference point between RA-F and PV-F. The resource assignment is sent to the PV-F through this reference point.

I_IAM_PV reference point between IAM-F and PV-F. The monitoring information and controls are transmitted through this reference point.

10 Security considerations

Security aspects for consideration within DaaS are addressed by security challenges for CSPs and CSCs, as described in [ITU-T X.1601]. In particular, [ITU-T X.1601] analyses security threats and challenges, and describes security capabilities that could mitigate these threats and meet security challenges.

It is recommended that relevant security requirements of [b-ITU-T Y.2201], [b-ITU-T Y.2701] and applicable ITU-T X-series, ITU-T Y-series and ITU-T M-series of Recommendations be taken into consideration, including access control, authentication, data confidentiality, data retention policy, network security, data integrity, availability and privacy.

Appendix I

Relationship between DaaS logical components and cloud computing reference architecture

(This appendix does not form an integral part of this Recommendation.)

This appendix provides the relationship between DaaS logical components [ITU-T Y.3503] and cloud computing reference architecture in [ITU-T Y.3502].

The relationship between DaaS logical components and cloud computing reference architecture can be done in two steps.

The first step is the mapping between DaaS logical components and DaaS functions in clause 6. Based on clause 6, each corresponding functions of DaaS for the DaaS logical components in [ITU-T Y.3503] is described in Table 6-1.

The second step is the mapping between DaaS functions and functional components of cloud computing reference architecture. This mapping is described in Figure 8-1.

Therefore, the possible mapping between DaaS logical components and functional components in cloud computing reference architecture is shown in Figure I.1.

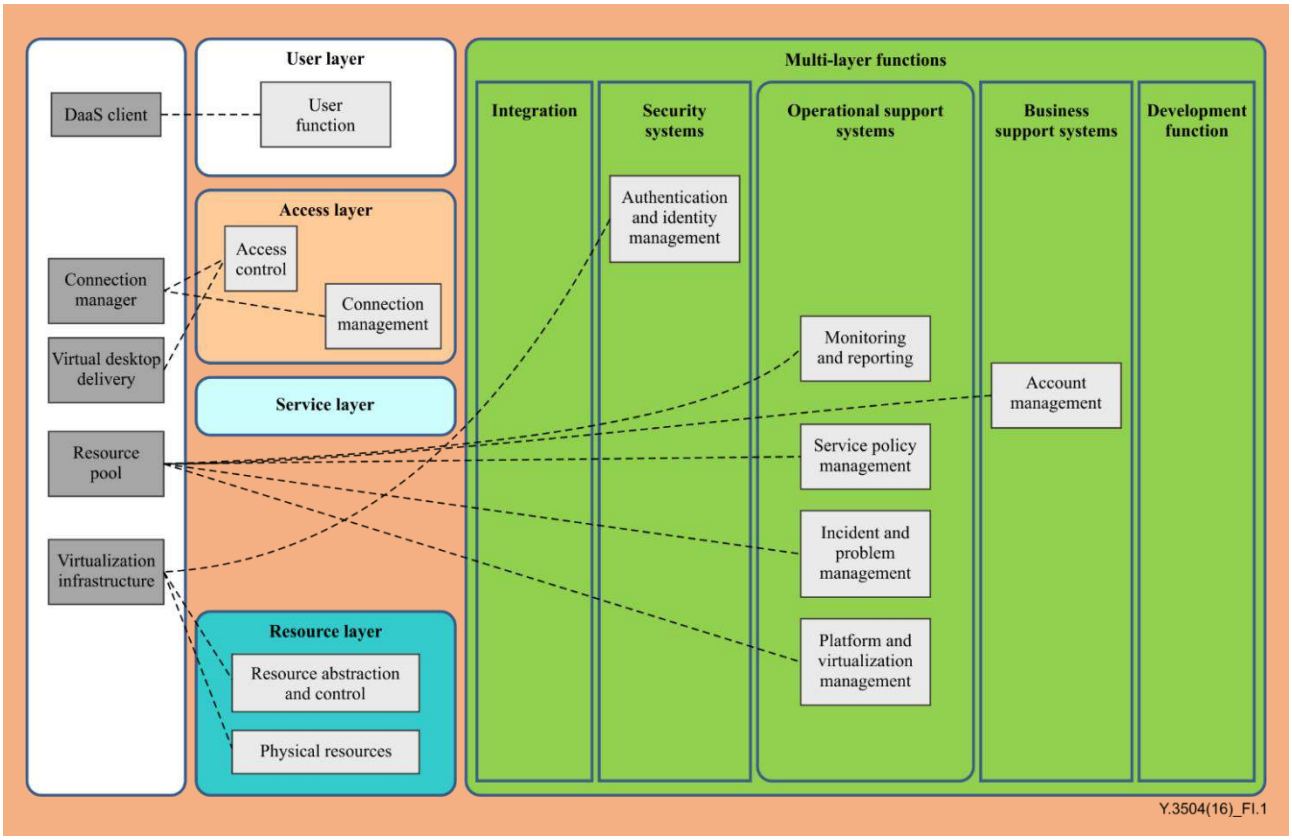


Figure I.1 – Relationship between DaaS logical components and cloud computing reference architecture

Appendix II

Relationship between DaaS functions and functional components in cloud computing reference architecture

(This appendix does not form an integral part of this Recommendation.)

Table II.1 provides the relationship between DaaS functions in clause 7 and functional components of cloud computing reference architecture defined in [ITU-T Y.3502] by enumerating all the related functional components corresponding to DaaS functions. The term "related functional components" in this appendix means that the description of the functional component in [ITU-T Y.3502] is similar to that of the DaaS function but does not mean that the functional component in [ITU-T Y.3502] can replace or cover for the DaaS function.

Table II.1 – Relationship between Clause 7 DaaS functions and ITU-T Y.3502 reference architecture

DaaS functions	Keywords or simple descriptions	Related functional components (FCs) in [ITU-T Y.3502]	Notes
Platform virtualization	Virtualization	Resource layer- Resource abstraction and control	Resource abstraction and control FC includes software elements such as hypervisors, virtual machines, virtual data storage, and time-sharing. Platform and virtualization management FC provides the capabilities for virtualizing the use of those resources (e.g., by means of hypervisors).
Resource assignment	Resource assignment	Resource layer- Resource abstraction and control	Resource abstraction and control FC provides access to the physical computing resources through software abstraction.
Performance enhancement for virtualization platform	Performance enhancement	Resource layer- Physical resources	Physical resources include hardware resources, such as computers (CPU and memory), networks (routers, firewalls, switches, network links and network connectors, storage components (hard disks) and other physical computing infrastructure elements.
Delivery protocol processing	Delivery of virtual desktop	Access layer- Service access	Delivery of virtual desktop means access of service. Service object is a virtual desktop in DaaS.
Client connection management	Coordinating delivery protocol Connection monitoring, reconnections	Access layer- Connection management	Connection management FC provides enforcement of QoS policies regarding the traffic from and/or to the user layer. This is related with connection monitoring, reconnection on the DaaS side.
User access management	Validating a DaaS user Support secure access	Access layer- Access control	Validating a DaaS user and secure access are tightly associated with the access control FC and the authentication and identity management FC.
Provisioning and allocation of virtual desktop	Preparing SW, HW resource Configure the pre-configured virtual desktop environment	None	There is no FC specialized in virtual desktop matters as the provisioning function in [ITU-T Y.3502] is for service.

Table II.1 – Relationship between Clause 7 DaaS functions and ITU-T Y.3502 reference architecture

DaaS functions	Keywords or simple descriptions	Related functional components (FCs) in [ITU-T Y.3502]	Notes
	(OS, disk, profile image) Deploying DaaS platforms Selecting DaaS platform to assign virtual desktop		
Infrastructure access management	Access I/F to infra (admin, DaaS user) Managing access authority	Security systems- Authorization and security policy management	This FC provides capabilities for the control and application of authorization for users to access specific capabilities or data. This FC is somewhat related with the infrastructure access management in that they cover authorization, but DaaS focuses on authority for resource access.
Monitoring and controlling virtual desktop resource	Monitoring infra and virtual desktop	Operational support systems- Monitoring and reporting	In the monitoring and reporting FC, the part of monitoring resources is similar to that on the DaaS side.
User account and profile management	Service catalogues CSU account info (CSC type name, id) Profile (HW configuration, SW)	Business support systems- Account management	Account management FC includes contracts, subscriptions, entitlements, and service pricing. This FC is partially related with UAPM-F in that it covers service catalogues, CSC type, and contracted HW/SW, but this does explain all of this function.
Virtual desktop resource allocation and distribution	Analysis of resource usage to admin Resource allocation, releasing Reallocating resources by a DaaS user request	Operational support systems- Platform and virtualization management	The resources are typically organized into resource pools with key characteristics: • standardized hardware componentry and configuration • readily expandable through the addition of new hardware capacity • automated shifting of resources as workload needs change • reduce and/or eliminate downtime through movement of workloads and data between resources • manage resource consumption based on goals
Operational policy management for DaaS	Group policy based on CSC types and user account Resource reallocation policy DaaS platform allocation policy	Operational support systems- Service policy management	Policies can include business, technical, security, privacy and certification policies that apply to cloud services and their usage by cloud service customers.

Table II.1 – Relationship between Clause 7 DaaS functions and ITU-T Y.3502 reference architecture

DaaS functions	Keywords or simple descriptions	Related functional components (FCs) in [ITU-T Y.3502]	Notes
High availability for DaaS	Detecting failure Redundancy set up Backup and restore virtual desktop environment Load balance VM auto migration	Operational support systems- Incident and problem management	This FC is for capturing incident or problem reports and managing those reports through to resolution; the main role of the HA-F is to detect failure and manage it.
Power management of virtual desktop resource	Calculating power consumption	Operational support systems- Incident and problem management	Power management in DaaS is partly related with platform and virtualization management FC and incident and problem management in that the function can deal with workload matters and prepare the incident by exceptional power consumption.
Service connection	Supporting various type of DaaS clients DaaS client connection status info Additional resource request Security connection	User layer- User function	User function FC supports the service user to access and use cloud services. Service connection is responsible for the connection between a virtual desktop and a DaaS user on the client side, so this FC is related with the SC-F. However, this is not enough to cover specific operations of the function.
Connection negotiation	Gathering and delivering network performance info and client status info Receiving the negotiation result info	None	There is no specific FC to treat the connection negotiation on the client side.
Client peripheral connection	Peripheral connection Controlling event of peripheral	None	There is no specific FC to treat DaaS client's peripherals.
Service continuity for user environment	Reconnection Request on fault Off-line synchronization	None	There is no specific FC to treat DaaS client's connection on the client side.

Bibliography

[b-ITU-T Y.2201] Recommendation ITU-T Y.2201 (2011), *Requirements and capabilities for ITU-T NGN*.

[b-ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014), *Information technology – Cloud computing – Overview and vocabulary*.

[b-DMTF OVF] DMTF Standard DSP0243 Version 1.0.0 (2009), *Open virtualization format specification*.

Cloud computing – Functional requirements of Network as a Service

Recommendation ITU-T Y.3512

(08/2014)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Summary

Recommendation ITU-T Y.3512 describes the concept of Network as a Service (NaaS) and its functional requirements. It provides typical use cases of NaaS and specifies the functional requirements of three aspects, ranging from NaaS application, NaaS platform and NaaS connectivity which are based on the corresponding uses cases and cloud capabilities types.

Keywords

Cloud computing, Network as a Service, NaaS, NaaS application, NaaS connectivity, NaaS platform.

Table of Contents

1 Scope

This Recommendation provides use cases and functional requirements of Network as a Service (NaaS), one of the representative cloud service categories. This Recommendation covers the following:

– High-level concept of NaaS;

– Functional requirements of NaaS;

– Typical NaaS use cases.

This Recommendation provides use cases and functional requirements of NaaS application, NaaS platform and NaaS connectivity.

NOTE – General requirements of NaaS can be found in [ITU-T Y.3501].

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1601] Recommendation ITU-T X.1601 (2014), *Security framework for cloud computing*.

[ITU-T Y.3011] Recommendation ITU-T Y.3011 (2012), *Framework of network virtualization for future networks*.

[ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014), *Information technology – Cloud computing – Overview and Vocabulary*.

[ITU-T Y.3501] Recommendation ITU-T Y.3501 (2013), *Cloud computing framework and high-level requirements*.

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), *Information technology – Cloud computing – Reference architecture*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 application capabilities type [ITU-T Y.3500]: Cloud capabilities type in which the cloud service customer can use the cloud service provider's applications.

3.1.2 cloud capabilities type [ITU-T Y.3500]: Classification of the functionality provided by a cloud service to the cloud service customer, based on resource used.

NOTE – The cloud capabilities types are application capabilities type, infrastructure capabilities type and platform capabilities type.

3.1.3 cloud computing [ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

3.1.4 cloud service [ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.5 cloud service category [ITU-T Y.3500]: Group of cloud services that possess some common set of qualities.

NOTE – A cloud service category can include capabilities from one or more cloud capabilities types.

3.1.6 cloud service customer [ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

3.1.7 cloud service provider [ITU-T Y.3500]: Party which makes cloud services available.

3.1.8 cloud service user [ITU-T Y.3500]: Natural person, or entity on their behalf, associated with a cloud service customer that uses cloud services.

3.1.9 Communications as a Service (CaaS) [ITU-T Y.3500]: Cloud service category in which the capability provided to the cloud service customer is real time interaction and collaboration.

NOTE – CaaS can provide both application capabilities type and platform capabilities type.

3.1.10 infrastructure capabilities type [ITU-T Y.3500]: Cloud capabilities type in which the cloud service customer can provision and use processing, storage and networking resources.

3.1.11 logically isolated network partition [ITU-T Y.3011]: A network that is composed of multiple virtual resources which is isolated from other LINPs.

NOTE – Term "logically isolated", which is the counter concept of "physically isolated", means mutual exclusiveness of the subjects (e.g., network partition, in this case), while the original subjects may be physically united/shared within the common physical constraints.

3.1.12 Network as a Service (NaaS) [ITU-T Y.3500]: Cloud service category in which the capability provided to the cloud service customer is transport connectivity and related network capabilities.

NOTE – NaaS can provide any of the three cloud capabilities types.

3.1.13 platform capabilities type [ITU-T Y.3500]: Cloud capabilities type in which the cloud service customer can deploy, manage and run customer-created or customer-acquired applications using one or more programming languages and one or more execution environments supported by the cloud service provider.

3.1.14 tenant [ITU-T Y.3500]: Group of cloud service users sharing access to a set of physical and virtual resources.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 service chain: An ordered set of functions that is used to enforce differentiated traffic handling policies for a traffic flow.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

BGP Border Gateway Protocol

BoD Bandwidth on Demand

BSS Business Support System

CaaS Communications as a Service

CDN Content Delivery Network

CPE Customer Premises Equipment

CSC Cloud Service Customer

CSP Cloud Service Provider

CSU	Cloud Service User
DNS	Domain Name System
DPI	Deep Packet Inspection
EPC	Evolved Packet Core
GW	Gateway
HQ	Headquarter
IaaS	Infrastructure as a Service
IDE	Integrated Development Environment
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPS	Intrusion Protection System
IPsec	IP security
L2	Layer 2
L3	Layer 3
LAN	Local Area Network
LINP	Logically Isolated Network Partition
MAC	Medium Access Control
MEF	Metro Ethernet Forum
MEN	Metro Ethernet Network
MPLS	Multi-Protocol Label Switching
NaaS	Network as a Service
NNI	Network-to-Network Interface
NOS	Network Operating System
OSS	Operations Support System
QoE	Quality of Experience
QoS	Quality of Service
P2P	Peer-to-Peer
PaaS	Platform as a Service
PoP	Point of Presence
SaaS	Software as a Service
SAL	Software Abstraction Layer
SDN	Software Defined Networking
SLA	Service Level Agreement
SSL	Secure Socket Layer
UNI	User-to-Network Interface
vCDN	virtual Content Delivery Network
vDPI	virtual Deep Packet Inspection
vEPC	virtualised Evolved Packet Core

vFW	virtual Firewall
vRouter	virtual Router
VDI	Virtual Desktop Infrastructure
VM	Virtual Machine
VoIP	Voice over IP
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
WAN	Wide Area Network

5 Conventions

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

In the body of this Recommendation and its annexes, the words shall, shall not, should, and may sometimes appear, in which case they are to be interpreted, respectively, as is required to, is prohibited from, is recommended, and can optionally. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative is to be interpreted as having no normative intent.

6 General description

6.1 Networking challenges in cloud computing

There are several challenges to build an efficient and reliable network application and infrastructure to provide cloud services. Having both compute, storage and network capabilities may face the following challenges:

- Coordination of compute and storage virtualization with network capabilities

  Compute and storage performance challenges in cloud computing systems are successfully solved using virtualization as a core technique. Server virtualization introduced virtual machines' (VMs) dynamic and static migration, which imposes demands on the networking environments. Network is expected to provide suitable and flexible support for highly variable cloud applications, when they run inside complex and diverse system architecture. In such system it is possible to provide the compute and storage resources, but it is also expected to dynamically provide the necessary networking support required to assure overall system performance, reliability and quality of service (QoS) demands.

- Harmonized control of heterogeneous network technologies

  Due to the increasing geographical distribution of cloud computing systems several network technologies can be utilised to assure end-to-end connectivity. It is expected that support of efficient control mechanisms for heterogeneous network technologies be provided.

- On-demand reconfiguration

  Cloud computing system allows for dynamic computing and storage resources reconfiguration or migration to meet the changing requirements. It is desirable that networks provide on-demand reconfiguration to satisfy the requirements of cloud services, e.g., change of bandwidth, modification of network topology or addition of new network elements.

6.2 High-level concept of NaaS

As defined in [ITU-T Y.3500], Network as a Service (NaaS) is a category of cloud services in which the capability provided to the cloud service customer (CSC) is transport connectivity and related network capabilities in order to solve the challenges mentioned above. NaaS services are divided into NaaS application service, NaaS platform service and NaaS connectivity service. In particular, NaaS connectivity service is an "infrastructure capabilities type" service limited to networking resources.

The high-level concept of NaaS using the layering framework defined in [ITU-T Y.3502] is illustrated on Figure 6-1.

NaaS can provide any of the three cloud capabilities identified in [ITU-T Y.3500] as follows:

- **NaaS application**: application capabilities type of service where NaaS CSC can use network applications provided by NaaS cloud service provider (CSP). These network applications are considered and used as a virtual network functions provided by NaaS CSP. This includes any network function for either fixed or mobile or both core and access as well as for control and forwarding planes network elements. Examples of NaaS applications include virtual router, virtual content delivery network (vCDN), virtualised evolved packet core (vEPC) and virtual firewall (vFW).

  In this category, CSP offers a set of interfaces for network functionalities.

- **NaaS platform**: platform capabilities type of service where NaaS CSC can use the network platform provided by NaaS CSP. The NaaS platform offers one or more software execution environments and one or more programming languages to deploy, manage and run customer-created or customer-acquired network applications. Such network applications can be created or acquired by CSC as self-implemented network services. Network applications can implement various network functionalities or services, e.g., router, firewall, load balancer, as well as groups of network functionalities. Groups of network applications and functionalities can form an integrated network solution.

  In this category, CSP offers a programmable environment for network functionalities that can be employed by cloud service customer or cloud service partner software.

- **NaaS connectivity**: infrastructure capabilities type of service where NaaS CSC can provision and use networking connectivity resources provided by NaaS CSP. This includes for example flexible and extended virtual private network (VPN), bandwidth on demand (BoD), etc. NaaS can provide basic networking functionalities such as connectivity, using whatever physical, logical or virtual networking capabilities the CSP chooses to offer. There is often a desire to offer more than IP networking. For example, a CSC may wish for elastic, on-demand control of optical networks, or even for access to dark fibre using photonic switching.

  In this category, CSP offers network connections between two or more endpoints, which may include additional network functionalities.

  NOTE 1 – The creation, control, management and removal of NaaS connectivity is performed as a cloud service.

  NOTE 2 – NaaS typically provides "bearer" connectivity of raw data without regard to the type of data carried between endpoints. Services that are specific to a type of carried data, such as telephony, voice over IP (VoIP), video conferencing, and instant messaging, are typically categorised as Communications as a Service (CaaS).

  NOTE 3 – The endpoints of NaaS connectivity can reside either within the NaaS service interface itself, in another cloud service, in a non-cloud service or at a traditional network endpoint.

NaaS services can be utilized by both cloud and non-cloud services.

Network capabilities can be delivered through any combination of the three types of cloud capabilities. In particular, network capabilities could support cloud computing in aspects of interconnection of the CSP and the CSC, topology and route related functionality to share topologies, discovery related functionality to perform other services needed by inter-cloud related activities as well as other functionalities related to monitoring, protection, verification, etc.

Network functionality can be provided as a composite NaaS service where the NaaS service consists of more than one network functionality services. Hierarchically nested NaaS composite services can also be provided. Composite NaaS services could apply for different NaaS capabilities types provided to CSC according to the performance objectives expressed in the service level agreement (SLA).

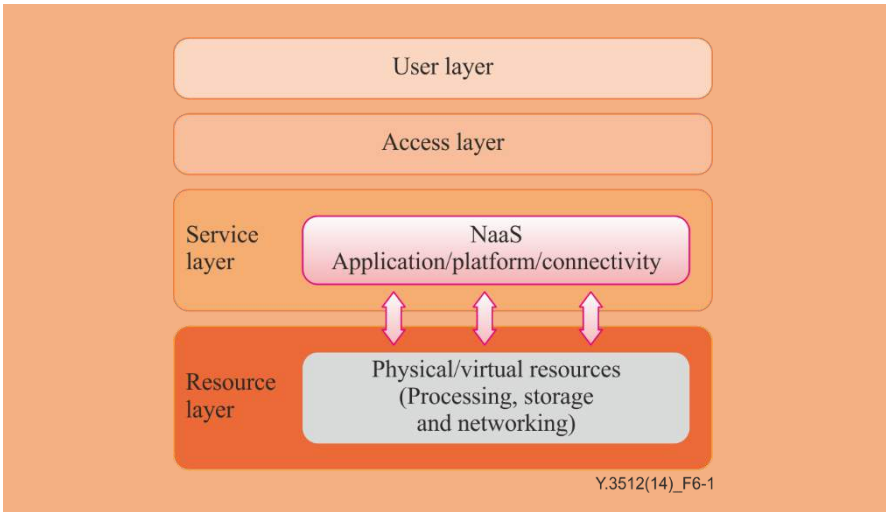


Figure 6-1 – High-level concept of NaaS

Appendix II provides NaaS use cases in which the three cloud capabilities types (i.e., application, platform and infrastructure capabilities) are provided to the CSC.

Appendix III provides considerations on the CSP's network related activities.

NOTE 4 – Regarding the network connectivity, one important difference between Infrastructure as a Service (IaaS) and NaaS is that IaaS is a cloud service category that is offered in only one flavour of cloud capability type, and that is infrastructure capabilities type [ITU-T Y.3500]. However, NaaS is a cloud service category that can be offered in all three cloud capabilities types.

7 Functional requirements of NaaS application

This clause provides requirements of NaaS application derived from the use cases described in Appendix II.

7.1 Performance

– NaaS application performance is recommended to be manageable to satisfy the CSC's needs.

– It is recommended that NaaS CSP monitors the utilization and delivery performance of NaaS application.

– NaaS application is recommended to be provided to the CSC according to the performance objectives expressed in the SLA.

7.2 Operation and management

– The operation of NaaS application is required to be manageable and deterministic in accordance with the CSP operational policies.

– It is recommended that each NaaS application be managed by NaaS CSP efficiently and automatically, complying with the CSP's common framework of service management and service operation management.

– It is recommended the NaaS CSP provide the CSC with an efficient management solution of provisioned NaaS applications allowing to integrate the management of the provisioned NaaS applications into the CSC's network operation environment.

7.3 Service chain

– It is recommended that NaaS CSP provides mechanisms allowing for the chaining of NaaS applications, e.g., the required NaaS applications components and associated order.

7.4 Multiple IP addresses

– It is recommended that NaaS application support multiple IP addresses on a network interface when it delivers network appliance functions (such as firewalls, load balancers).

NOTE – This requirement is also applicable to NaaS platform and NaaS connectivity.

8 Functional requirements of NaaS platform

This clause provides requirements of NaaS platform derived from the use cases described in Appendix II.

8.1 Programmable NaaS platform

– It is recommended that NaaS CSP supports deployment of network applications on NaaS platform by both the CSP and the CSC.

– It is recommended that NaaS platform provides hardware or software modules specialized for network function acceleration.

– It is recommended that NaaS platform assures and indicates performance available to the CSC's applications which are running on it.

– It is recommended that NaaS platform service provides a modular software framework to select and integrate networking functions, security functions and third party applications.

– It is recommended that NaaS CSP provides platform support for the CSC to manage (e.g., install, upgrade or uninstall) CSC owned modules.

– It is recommended that NaaS platform provides network enablers for the CSC to initiate (e.g., design, build, manage) and operate the flexible, scalable, functionally expandable networks.

– It is recommended that NaaS platform provides a unified control and management function over distributed NaaS platforms for the CSC to change, move, or remove network enablers between NaaS platforms.

8.2 Dynamic and flexible network services composition and steering

– It is recommended that NaaS CSP steers the CSC's traffic via service chain which is dynamically and flexibly composed by customized sequences of NaaS applications on the NaaS platform according to the CSC's specific service logic.

8.3 Isolation of service chains for tenants

– NaaS CSP can optionally support isolation of service chains for tenants, combining different network services, implemented on the NaaS platform.

8.4 Flexible scaling of NaaS platform

– It is recommended that NaaS CSP assures flexible scaling of the resources assigned to the NaaS platform to achieve performance objectives of the network services and applications implemented on the Naas platform.

NOTE – This requirement is to meet the changes in services or applications utilization caused by e.g., growth of traffic, change in number of users, adding new services, implementing new applications.

8.5 Integration of software applications

– It is recommended that NaaS CSP supports integration of software applications deployed on the NaaS platform by either the CSP or the CSC, or both, to allow building of the combined solutions.

9 Functional requirements of NaaS connectivity

This clause provides requirements of NaaS connectivity derived from the use cases described in Appendix II.

9.1 Common control mechanism for NaaS connectivity

– It is recommended that the NaaS connectivity control mechanism provided by the NaaS CSP supports the negotiation of connectivity parameters (such as interface characteristics, connection endpoints, IP version support, QoS, L3/L2VPN type, connectivity extension approach (e.g., clause 10 of [b-IETF RFC 4364], routing information (e.g., border gateway protocol (BGP) route target).

– It is recommended that NaaS CSP provides a common NaaS connectivity control mechanism allowing identified NaaS connectivity to be provided in a secure and QoS guaranteed manner.

– It is recommended that the NaaS connectivity control mechanism is able to cope with potentially different CSC identification schemes used on the NaaS CSP side and on the connected endpoint.

– NaaS CSP can optionally provide isolated connectivity for the network tenants.

9.2 Unified SLA for multiple optimized networks

– It is recommended that NaaS CSP provides network connectivity services using unified SLA for CSC's management of multiple optimized networks in order to simplify and unify the control and management of networks.

NOTE – This mechanism allows the CSP to create and add new features to their networks to provide high quality services which can meet CSC's differentiated requirements.

– It is recommended that composite NaaS services policy should be expressed in the SLA.

NOTE 1 – NaaS service can be a composite service, where the service consists of more than one NaaS service.

NOTE 2 – This requirement is also applicable to the NaaS application and the NaaS platform.

9.3 Leveraging transport networks dynamically

– It is recommended that NaaS CSP leverages transport networks dynamically from multiple choices of physical and virtual networks for the purpose of providing network connectivity services, such as recovery, BoD, QoS guarantee, etc.

NOTE – The transport networks can be heterogeneous in terms of technology and administrative domain.

9.4 Unified network control mechanism

– It is recommended that NaaS CSP provides a unified control mechanism for the end-to-end NaaS connectivity given to a CSC.

NOTE – NaaS connectivity could be provided either by multiple heterogeneous networks or by a network employing one or more NaaS platforms or applications, which perform(s) network functions.

9.5 Elastic network reconfiguration

– It is recommended for the CSP to provide the elastic network reconfiguration in order to match the computing and storage elasticity and to maintain service continuity.

9.6 Seamless and end-to-end solution of bandwidth allocation

– It is recommended that NaaS CSP provides seamless and end-to-end solution of bandwidth allocation independent of network technology and architecture.

9.7 Symmetric or asymmetric capacity

– It is recommended that NaaS CSP provides symmetric or asymmetric network link capacity based on the CSC's demand.

9.8 Optimized and fine-grained traffic engineering

– It is recommended that NaaS CSP provides the CSC with fine-grained view on usage of network resources.

– It is recommended that NaaS CSP collects near real time utilization metrics and topology data from its own network equipment.

– It is recommended that NaaS CSP controls the network resource allocation by reconfiguring network profiles as well as properties (e.g., topology, bandwidth) in response to dynamically changing traffic demands.

– NaaS CSP can optionally provide centralized traffic management to achieve optimized traffic engineering.

9.9 Coexistence with legacy network services and functions

– It is recommended that NaaS CSP avoids or mitigates possible performance and flexibility impacts when introducing new network connectivity services.

– It is recommended that NaaS CSP supports coexistence of new network connectivity services with legacy systems.

9.10 Centralized control view and abstraction view of resources

– NaaS CSP can optionally support logically centralized management and control view of the network resources.

– NaaS CSP can optionally provide to the CSC an abstraction view of the underlying network resources.

9.11 CSC limited control of services

– It is recommended that NaaS CSP provides to the CSC appropriate services control in order to respond to the time-sensitive performance requirements, including bandwidth quantities, maximum latencies and other QoS parameters.

9.12 Logically isolated network partition

– NaaS CSP can optionally implement logically isolated network partition (LINP).

NOTE – LINP is described in [ITU-T Y.3011]. See clause 3.1.14.

9.13 Overlay network mechanism

– NaaS connectivity can optionally support virtual overlay networks on top of the physical underlay network.

9.14 Overlapped private IP addresses

– It is recommended that NaaS CSP allows different CSCs to use their own private IP addresses even when the subnet addresses are overlapped.

9.15 Interworking among different VPN solutions

– It is recommended that NaaS CSP supports interworking among different VPN technologies.

9.16 VPN connection in mobile environment

– It is recommended that NaaS CSP supports VPN connectivity in mobile environment.

9.17 Connection to NaaS CSP's network through public Internet

– It is recommended that NaaS CSP allows the CSC to connect to the NaaS CSP through the public Internet.

10 Security considerations

Security aspects for consideration within cloud computing environments, including NaaS, are addressed by security challenges for the CSPs, as described in [ITU-T X.1601]. In particular, [ITU-T X.1601] analyses security threats and challenges, and describes security capabilities that could mitigate these threats and meet security challenges.

Appendix I

Development methodology of NaaS functional requirements and architecture

(This appendix does not form an integral part of this Recommendation.)

Considering the standardization methodology and conventional study sequence, the abstractions of functional entities and their mutual interactions are based on the functional requirements and the corresponding use cases analysis, which form a standardization body together. Therefore, it is required to progress NaaS functional requirements and architecture according to the following steps and priorities.

Step 1: Use cases and functional requirements of NaaS which are included in Appendix II and clauses 7-9, respectively, of this Recommendation. Note that all the functional requirements are derived from the corresponding use cases.

Step 2: Functional architecture of NaaS should be based on this Recommendation.

Additionally, the general requirements of NaaS are described in [ITU-T Y.3501].

Appendix II

Use cases of NaaS

(This appendix does not form an integral part of this Recommendation.)

This appendix includes three types of NaaS use cases: NaaS application related use cases, NaaS platform related use cases and NaaS connectivity related use cases. Each type of NaaS use case is further divided into general and detailed use cases.

II.1 Use case template

The use cases developed in Appendix II should adopt the following unified format for consistent readability and convenient material organization.

Title	Title of the use case
Description	Scenario description of the use case
Roles	Roles involved in the use case
Figure (optional)	Figure to explain the use case, but is not mandatory
Pre-conditions (optional)	The necessary pre-conditions that should be achieved before starting the use case.
Post-conditions (optional)	The post-condition that will be carried out after the termination of current use case.
Derived requirements	Requirements derived from the use cases, whose detailed descriptions are presented in the dedicated clauses.

II.2 NaaS applications related use cases

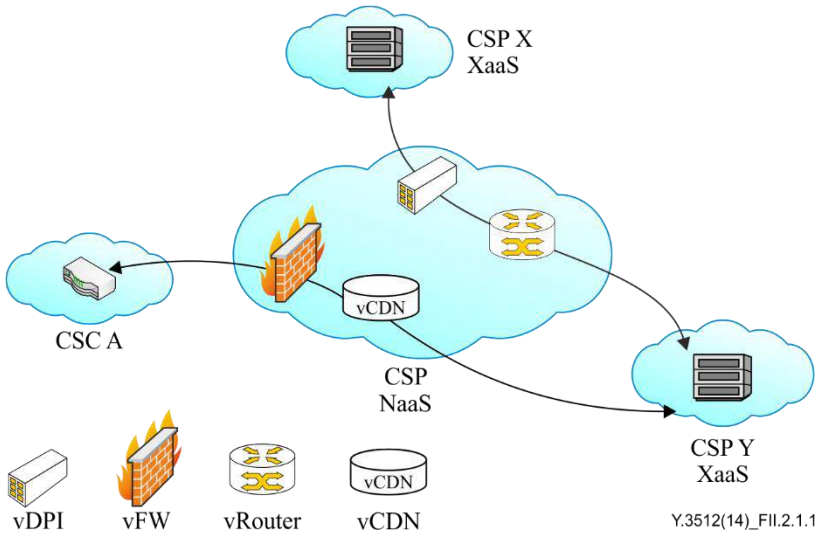
This clause provides description of use cases related where NaaS CSC can provision and use network applications.

NOTE – In the following clauses, XaaS represents any categories of cloud services such as Software as a Service (SaaS), Platform as a Service (PaaS), IaaS, CaaS, etc.

II.2.1 General use cases

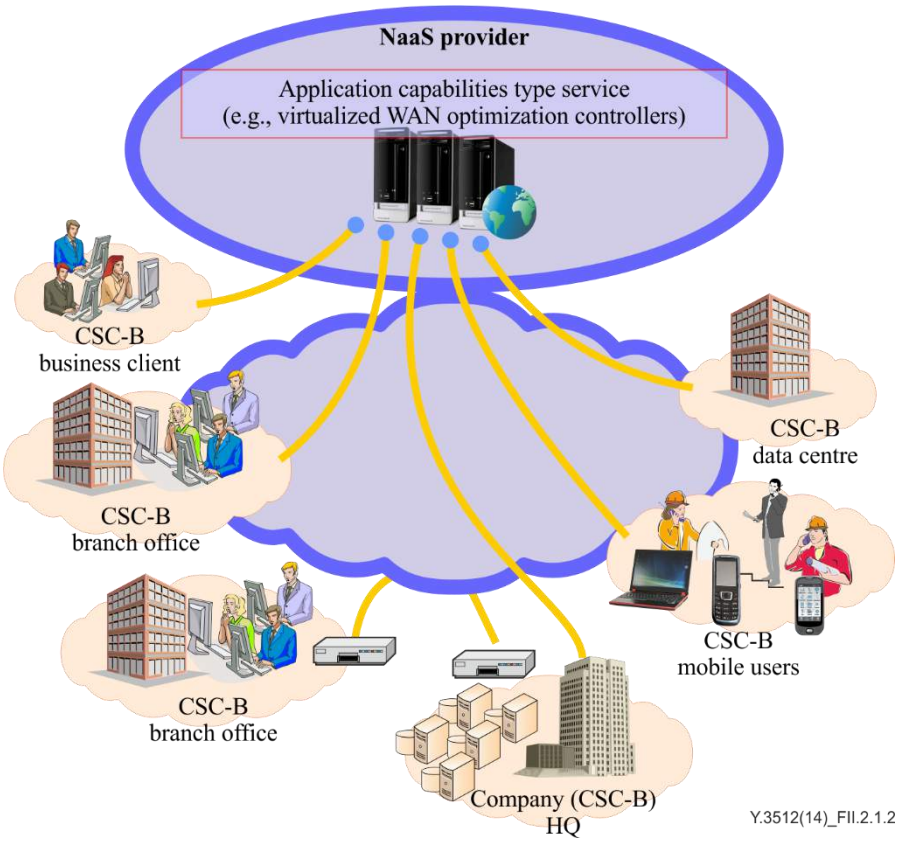
II.2.1.1 General NaaS application use case

Name	General NaaS application use case
Description	A XaaS CSC or XaaS CSP uses the network applications (e.g., virtual DPI (vDPI), vFW, vCDN) provided by NaaS CSP. These network applications can be chained by NaaS CSP.
Roles	CSC, CSP

Figure	 NOTE – Virtual router (vRouter) can also be applicable to NaaS connectivity.
Pre-conditions (optional)	– There is connectivity between XaaS CSC A and XaaS CSP Y. – There is connectivity between XaaS CSP X and XaaS CSP Y. – Either the XaaS CSP or the CSC requests a network application (vFW, vCDN, vDPI, vRouter etc.) to be chained with the connectivity.
Post-conditions (optional)	– NaaS CSP offers network applications for the XaaS CSC/CSP over existing network connectivity.
Derived requirements	– On-demand virtual network application – Scalable network application – Chain of network applications – QoS-guaranteed applications – Secure network applications – Resilient network applications – Multiple IP addresses (refer to clause 7.4) NOTE – The first six requirements belong to general requirements of NaaS which are provided in [ITU-T Y.3501].

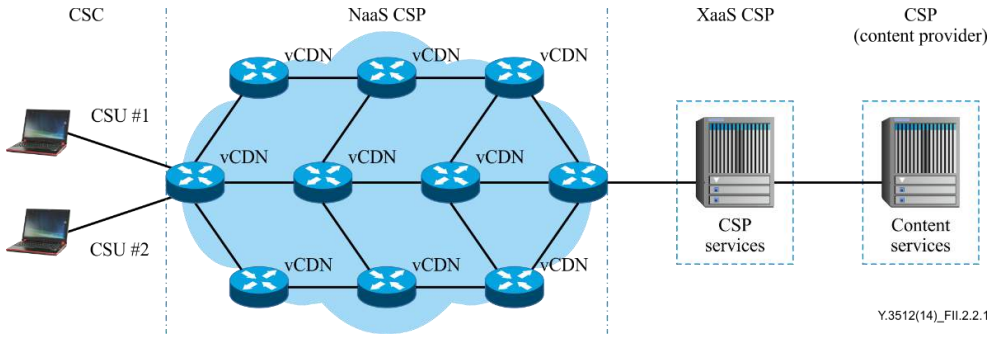
II.2.1.2 NaaS application use case for application provision

Title	NaaS application use case for application provision
Description	Assume that company CSC-B looks for NaaS application services to benefit from key characteristics of the cloud computing services. As an example, the company wants to accelerate network traffic saturated with business applications. Wide area network (WAN) optimization is very crucial for the success of its business applications. CSC-B wants usage-based deployment of WAN optimizations and flexible feature support on-demand. Traditional WAN optimization appliance devices cannot fulfil those requirements, in particular, in terms of total cost of ownership and deployment elasticity. NaaS CSP needs to provide virtual WAN acceleration solution to CSC-B, coping with its dynamic business needs.
Roles	CSP, CSC

Figure (optional)	
Pre-conditions (optional)	CSC-B needs to accelerate network traffic saturated with business applications.
Post-conditions (optional)	CSC-B used virtual WAN acceleration solution provided by NaaS CSP to satisfy the dynamic business needs.
Derived requirements	– On-demand self-service – Multi-tenancy – Resource pooling – Rapid elasticity and scalability – Measured service – Performance assurance and monitoring – Co-existence and compatibility with CSC's legacy network equipment – Interoperability support for management and orchestration – Security and resilience – Performance (refer to clause 7.1) – Operation and management (refer to clause 7.2) NOTE – The first nine requirements belong to general requirements of NaaS which are provided in [ITU-T Y.3501].

II.2.2 Detailed use cases

II.2.2.1 NaaS platform use case for cloud CDN

Title	NaaS platform use case for cloud content delivery network (CDN)
Description	Content provider acting as CSC stores the content in the data centre and monitors the usage of the content. When the usage of the content reaches certain level of popularity or if according to some predictions content provider expects a growth of popularity in a defined period of time, e.g., video transmission of a sport event, content provider creates a virtual CDN to temporarily move the content from the data centre to the network (vCDN). XaaS CSP receives the content from the content provider (which can itself create a distribution service). Content is delivered to the cloud service users (CSUs) from XaaS CSP data centre using the network of NaaS CSP. The XaaS CSP offers the possibilities to store the content and to monitor usage parameters. XaaS CSP in cooperation with the NaaS CSP can duplicate the content in the network nodes, building a virtual CDN service. Basically XaaS CSP supports CDN functions, thus CDN is in some way "emulated" by the XaaS CSP, which cooperates with the NaaS CSP.
Roles	CSU, CSC, CSP
Figure (optional)	
Pre-conditions (optional)	– Content provider acting as CSC stores the content in XaaS CSP data centres. – Content provider acting as CSC monitors the use of content.
Post-conditions (optional)	– XaaS CSP offers the virtual CDN service using network resources of the NaaS CSP. – Content provider acting as CSC decides to move content from the data centre to the virtual CDN for a defined period of time.
Derived requirements	– Performance (refer to clause 7.1) – Operation and management (refer to clause 7.2) – Service chain (refer to clause 7.3)

II.3 NaaS platform related use cases

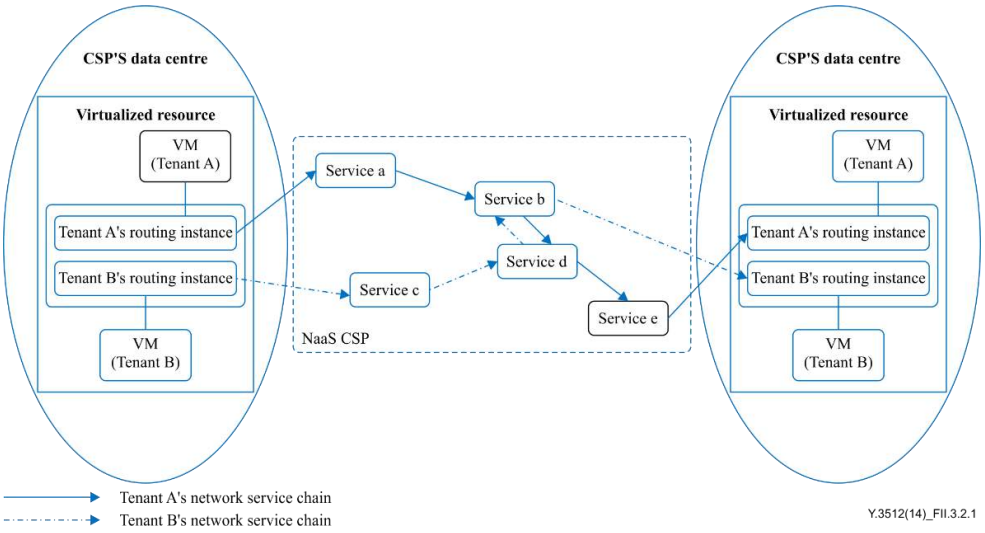
II.3.1 General use cases

None.

II.3.2 Detailed use cases

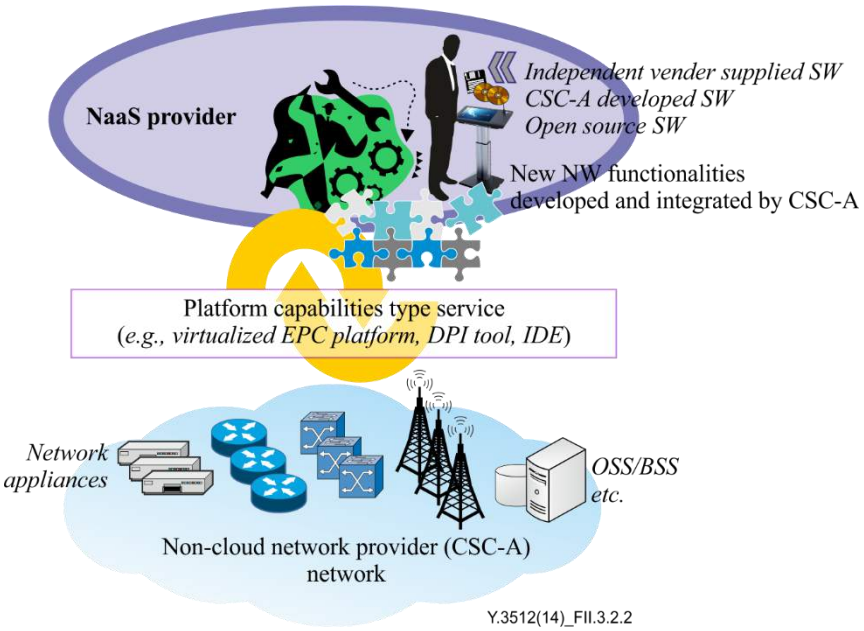
II.3.2.1 NaaS platform use case for service chain

Title	NaaS platform use case for service chain
Description	With CSC's tenants increasing requirements on the service diversity and complexity, CSP needs to deliver integrated network application services, such as deep packet inspection (DPI), intrusion detection, intrusion prevention, load balance, firewall, etc. Traditionally, the set of services are provided using dedicated physical network elements, which have limited network capacity and functionalities, complex configuration and update, and lengthy provision period. The situation, when the output of one service is used as input for the other service is called service chain. In traditional network the set-up of services chain,

	e.g., chain composed of intrusion protection system (IPS), load balancer and DPI, needs dedicated configuration and is not flexible in case of e.g., growth of traffic, adding/removing services to/from the chain. For the better service flexibility, it is recommended for NaaS CSP to provide programmable NaaS platform, on which NaaS applications such as vRouter, vCDN, vEPC, etc. can be deployed, in order to steer the CSC's traffic via customized NaaS applications sequence.
Roles	CSC (Tenant A, Tenant B), CSP
Figure (optional)	
Pre-conditions (optional)	– CSP can deliver dedicated physical network appliances solutions for services, such as DPI, intrusion detection, intrusion prevention, load balance, firewall, etc.
Post-conditions (optional)	– CSP can provide composed either virtual or physical network services or both, or services chains dynamically and flexibly according to the CSC's specific service logic in a shorter deployment, configuration, and update intervals, compared with dedicated physical network appliances solution.
Derived requirements	– Programmable NaaS platform (refer to clause 8.1) – Dynamic and flexible network services composition and steering (refer to clause 8.2) – Isolation of service chains for tenants (refer to clause 8.3)

II.3.2.2 NaaS platform use case for platform provision

Title	NaaS platform use case for platform provision
Description	CSC-A is a network operator. CSC-A wants to build advanced traffic analysis system and multi-dimensional reporting using dynamically scaling DPI functionalities, opportunistic services at low risk, and in short time of implementation, multi-tenant CDN, etc., in mobile networks. However, classical proprietary hardware-based network appliances inhibit the rapid roll out of new converged network functionalities and revenue earning services. They neither scale on-demand nor are flexible enough. CSC-A has the possibility to cope with its business innovation needs by developing necessary features and services using NaaS platform. Innovating using NaaS platform allows it to utilize CSP network services and combine them with the functionalities developed by CSC-A. All functionalities can be integrated by CSC-A on the basis of NaaS platform to build enhanced network services e.g., virtualized evolved packet core (EPC), software-based DPI platform, integrated development environments (IDEs). The capacity of NaaS platform needs to scale elastically according to the utilization of enhanced network services to secure the required performance. Solutions to support integration of the CSP network services with the CSC-A's developed software are also needed.
Roles	CSP, CSC

Figure (optional)	
Pre-conditions (optional)	CSC-A needs to build enhanced network services using dedicated hardware equipment for each functionality and manage the whole network.
Post-conditions (optional)	CSC-A used NaaS platform to combine CSP network services with self-developed functionalities and integrate them into enhanced network services.
Derived requirement	– Flexible scaling of NaaS platform (refer to clause 8.4) – Integration of software applications (refer to clause 8.5)

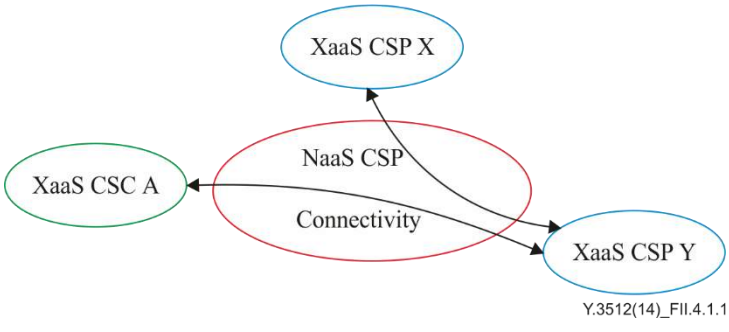
II.4 NaaS connectivity related use cases

This clause provides description of use cases where NaaS CSC can provision and use network connectivity.

II.4.1 General use cases

II.4.1.1 General NaaS connectivity use case

NOTE – The following use case is based on a use case provided in [ITU-T Y.3501].

Name	General NaaS connectivity use case
Description	A NaaS CSP sets up, maintains and releases the network connectivity between CSCs and between the CSP and the CSC as a cloud service. This can include on-demand and semi-permanent connectivity.
Roles	CSC, CSP
Figure	

Pre-conditions (optional)	– There is no connectivity between XaaS CSC A and XaaS CSP Y. – There is no connectivity between XaaS CSP X and XaaS CSP Y. – Either XaaS CSC A or XaaS CSP Y requests the connectivity between them with their end-point identifiers and associated characteristics (referring to QoS and security aspects) for the connectivity. – Either XaaS CSP X or XaaS CSP Y requests the connectivity between them with their end-point identifiers and associated characteristics (referring to QoS and security aspects) for the connectivity.
Post-conditions (optional)	– XaaS CSC A and XaaS CSP Y can communicate with each other. – XaaS CSP X and XaaS CSP Y can communicate with each other.
Requirements	– On-demand network configuration – Heterogeneous networks compatibility – QoS-guaranteed connectivity – Secured connectivity – Common control mechanism for NaaS connectivity (refer to clause 9.1) NOTE – The first 4 requirements belong to general requirements of NaaS which are provided in [ITU-T Y.3501].

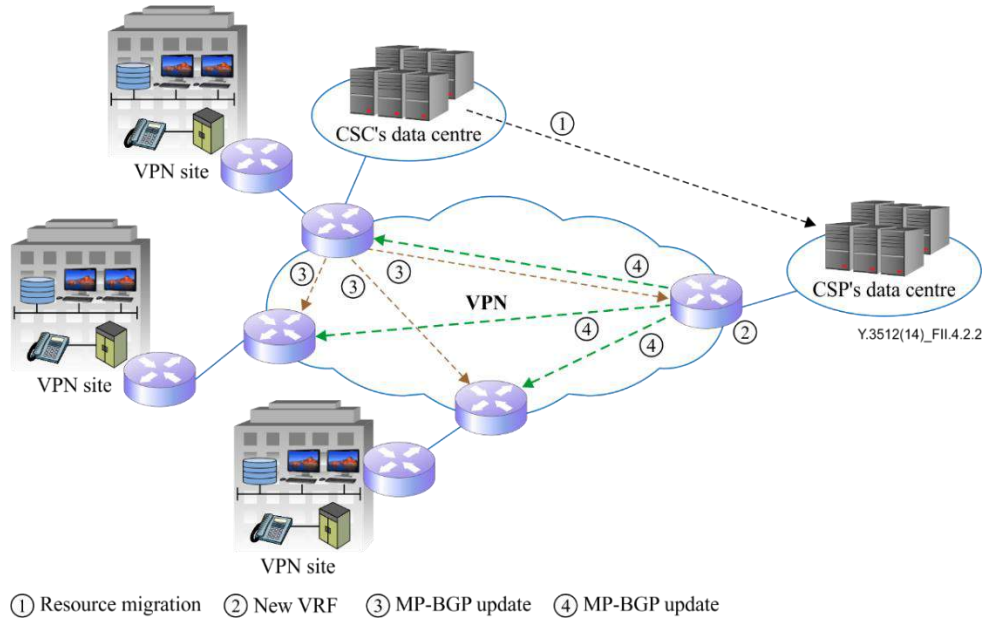
II.4.2 Detailed use cases

II.4.2.1 NaaS connectivity use case for dynamic transport network

Title	NaaS connectivity use case for dynamic transport network
Description	CSC demands a geographically distributed connectivity service and dynamic traffic capacity which can accommodate cloud bursting (e.g., VM migration or the transfer of large data files across data centres which sit in different places) which brings a surge of traffic passing through the backbone of the CSP. IP and transport networks of the CSP are separately managed and therefore cannot provide the common control mechanism for dynamic bandwidth adjustment. In order to guarantee the service continuity and consistent SLA to the CSC, such CSP would have to offer over-provisioning of links, most of which being not used effectively and thus causing resource waste. The CSP is recommended to cope with the surge of transit traffic which traverses its backbone without making use of traditional over-provisioning approaches of the networking resources.
Roles	CSC, CSP
Figure (optional)	
Pre-conditions (optional)	
Post-conditions (optional)	
Derived requirements	– Unified SLA for multiple optimized networks (refer to clause 9.2) – Leveraging transport networks dynamically (refer to clause 9.3) – Unified network control mechanism (refer to clause 9.4)

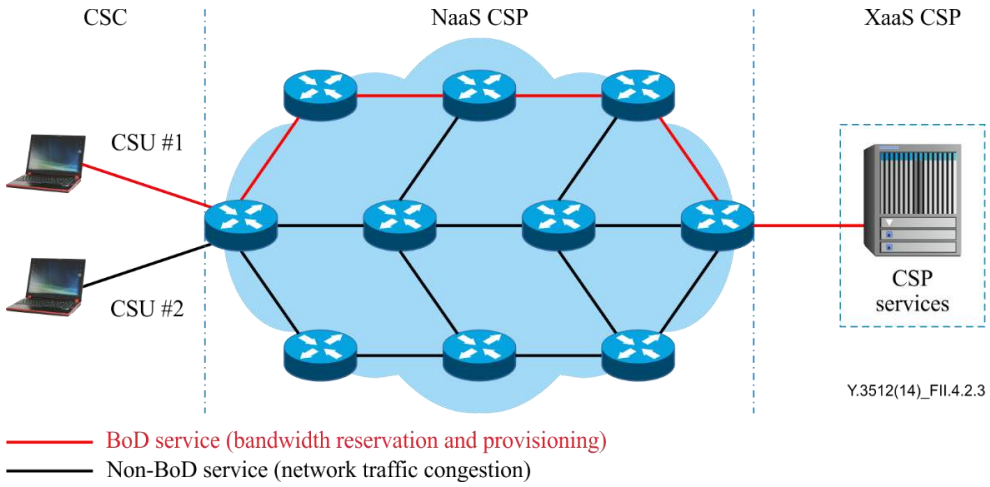
II.4.2.2 NaaS connectivity use case for flexible and extended VPN

Title	NaaS connectivity use case for flexible and extended VPN
Description	The different VPN sites are connected via BGP/MPLS IPVPN. The processing resources and the corresponding subnet are migrated from the CSC's data centre to the CSP's data centre, which is not yet involved in the VPN as a VPN site. In order to add this new site in the

	existing VPN, there is a need to provision a new subnet in the CSP's data centre and to set up a new virtual routing and forwarding (VRF) in its edge router. The migration of the corresponding subnet from the CSC's data centre to the CSP's data centre and the subnet removal from the CSC's data centre needs to be announced to the remaining edge routers. The concrete procedure is shown in the following figure. 1. Processing resources and the corresponding subnet migrate from the CSC's data centre to the CSP's data centre. 2. New VRF is configured in the edge router of the CSP's data centre. 3. The removal of the CSC's subnet is announced through MP-BGP update to all VPN sites. 4. CSP's new subnet is announced through MP-BGP update to all VPN sites. Service continuity needs to be ensured during the whole migration and reconfiguration procedure. However, the existing VPN is a black box from the CSC's perspective, and as such it can't be provisioned and reconfigured by the CSC. In addition, the current VPN technology cannot support the dynamic addition and reduction of the VPN sites and bandwidth capacity.
Roles	CSC, CSP
Figure (optional)	
Pre-conditions (optional)	
Post-conditions (optional)	
Derived requirements	– Elastic network reconfiguration (refer to clause 9.5)

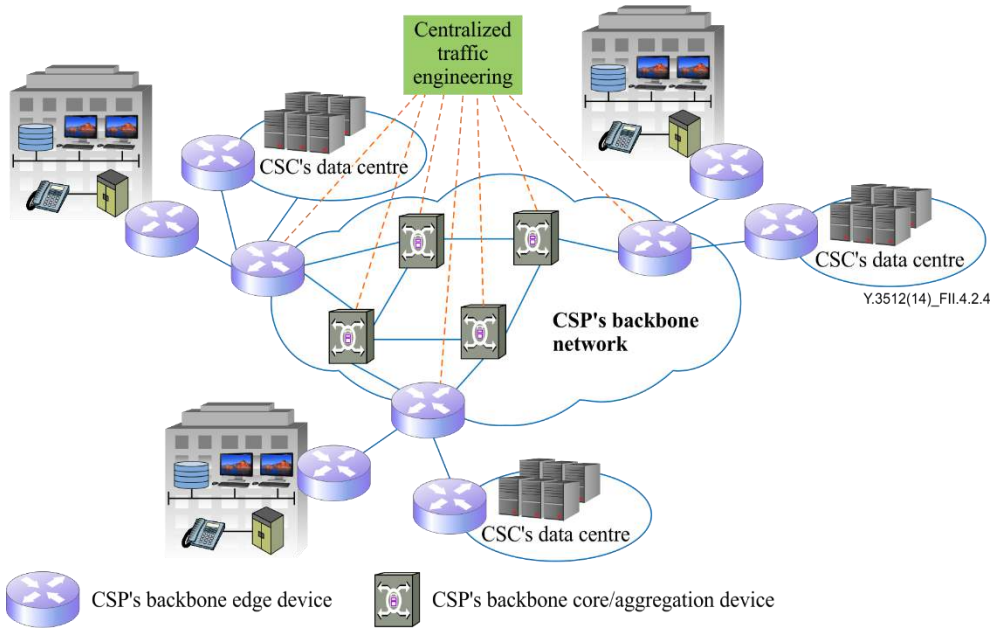
II.4.2.3 NaaS connectivity use case for BoD service

Title	NaaS connectivity use case for BoD service
Description	In this scenario CSU access to cloud computing service offered by XaaS CSP is considered (e.g., virtual desktop infrastructure (VDI), video streaming). CSU accesses the service from a fixed location e.g., using a company local area network (LAN) or from mobile location e.g., mobile terminal. The XaaS CSP serves the services on the basis of own data centres and has no impact on the performance of particular connectivity between end users and the data centre where the service is hosted. From the perspective of CSU, quality of experience (QoE) of the service is dependent on a combination of data centre and network performance. The XaaS CSP is able to guarantee certain service quality limited to its own data centre. This quality could be downgraded on network performance on the connection

	between CSC and particular data centre. The XaaS CSP acting alone is not able to impact network performance without interaction with NaaS CSP. As a solution to guarantee end-to-end service quality, bandwidth reservations can be applied in the network between the CSU and the data centre. This allows the guarantee of certain network performance and can be a basis for end-to-end SLA contract for the service between a CSU and the XaaS CSP. To fulfil these needs, XaaS CSP interacts with NaaS CSP. NaaS CSP can be any actor that has the ability to offer connectivity between XaaS CSP and the CSC, to which CSU belongs.
Roles	CSU, CSC, CSP
Figure (optional)	
Pre-conditions (optional)	– XaaS CSP has no impact on connectivity parameters between the service and the CSU.
Post-conditions (optional)	– XaaS CSP offers end-to-end service quality or SLA to the CSC, on the basis of cooperation with NaaS CSP.
Derived requirements	– Seamless and end-to-end solution of bandwidth allocation (refer to clause 9.6) – Symmetric or asymmetric capacity (refer to clause 9.7)

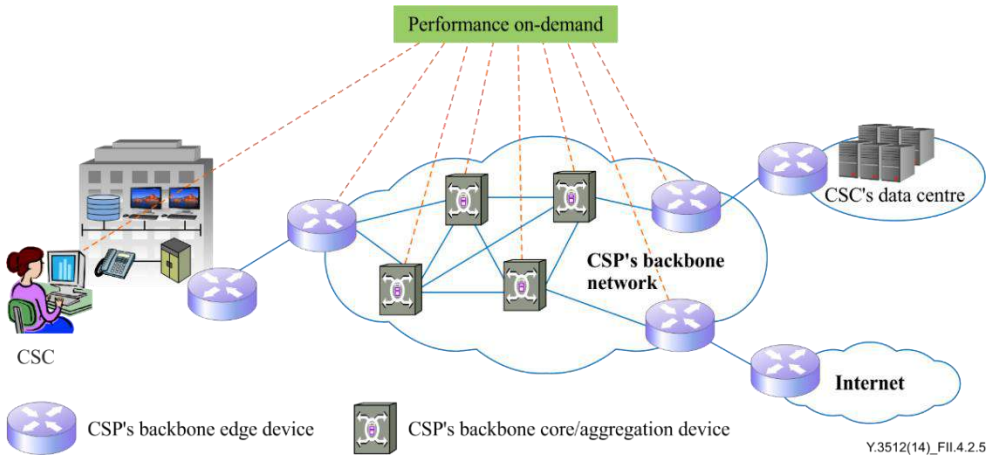
II.4.2.4 NaaS connectivity use case for optimized traffic engineering

Title	NaaS connectivity use case for optimized traffic engineering
Description	The CSP provides network connectivity services to a CSC in order for the CSC to inter-connect its own multiple geographically distributed data centres. With the increase of cloud services deployed over the CSC's data centres, more and more traffic, e.g., for data mirroring, redundancy, database synchronization, VM migration, active-active storage replication, is traversing the CSP's backbone network due to the CSC's increasing distributed services. Currently, CSP typically provides the CSC with static connectivity services resulting in either over-provisioned, under-utilized service capacity or under-provisioned, capacity-capped services. In order to make a more efficient use of its connectivity resources, a solution for the CSP is to support a central decision-making function for the backbone traffic engineering. At the minimum, such solution has to coexist with other legacy network solutions used by the CSP for the support of other services.
Roles	CSC, CSP

Figure (optional)	
Pre-conditions (optional)	
Post-conditions (optional)	
Derived requirements	– Optimized and fine-grained traffic engineering (refer to clause 9.8) – Coexistence with legacy network services and functions (refer to clause 9.9) – Centralized control view and abstraction view of resources (refer to clause 9.10)

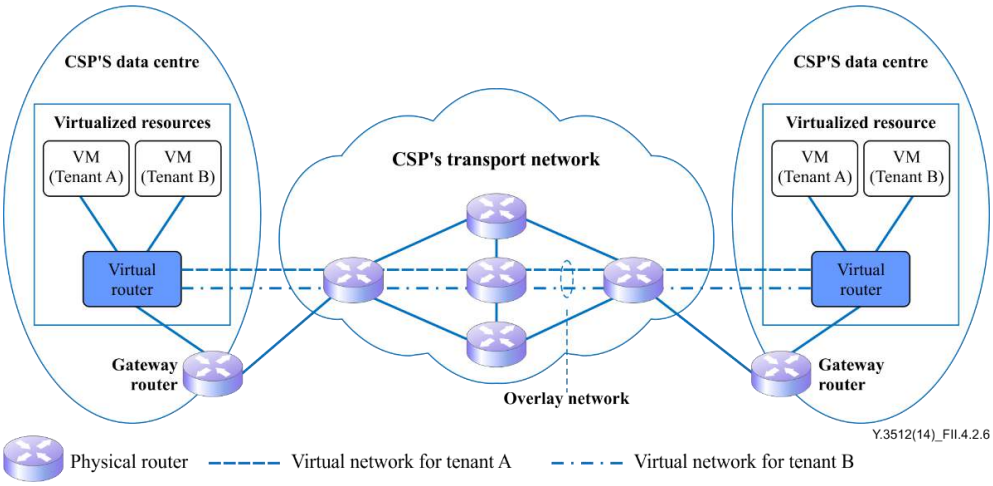
II.4.2.5 NaaS connectivity use case for performance on demand

Title	NaaS connectivity use case for performance on demand
Description	CSC requests CSP to provide on-demand network performance (such as bandwidth quantities, maximum latencies and other QoS parameters), which includes dynamic establishment, change and resized capacity of links. However, traditional solution based on human intervention lacks automation capabilities which make it difficult to deliver self-provisioned services and respond to time-sensitive changes in network performance requirements. Additionally, frequent changes sometimes result in congestion and instability because traffic, which comes from multiple sources, shares the same network link. CSP provides CSC the appropriate control in order to request services through a portal and to shield the underlying physical network to the CSC.
Roles	CSC, CSP

Figure (optional)	
Pre-conditions (optional)	
Post-conditions (optional)	
Derived requirements	– Centralized control view and abstraction view of resources (refer to clause 9.10) – CSC limited control of services (refer to clause 9.11)

II.4.2.6 NaaS connectivity use case for virtual router

Title	NaaS connectivity use case for virtual router
Description	According to [ITU-T Y.3500], multi-tenancy is a key characteristic of the cloud service, which requires the CSP to provide the CSC either shared physical or virtual resources or both, such that multiple tenants and their resources and data are isolated from and inaccessible to each other. These tenants share the same underlay physical resources, including physical servers, physical storage and physical networks and each tenant is assigned its own logical resources, including VMs, virtual storage and virtual networks. These logical resources need to be isolated from each other and the virtual compute, storage and network resources need to be integrated and matched in a fine granularity. However, the legacy underlay physical routers and switches of CSP's transport network don't contain each tenant's state, including tenant's medium access control (MAC) and IP addresses and the network policies attached to the VM that belongs to the tenant. In other words, the forwarding tables of the underlay physical routers and switches only contain the IP prefixes or MAC addresses of the physical servers. The virtual router is software implemented router and can be implemented within the virtualization infrastructure. The virtual router provides connectivity among virtual machines, virtual switches, etc., and contains per tenant state and a separate forwarding table for a virtual network. The forwarding table includes the IP prefixes (in the case of a layer 3 overlay network) or the MAC addresses (in the case of a layer 2 overlay network) of VMs. In addition, no single virtual router needs to contain all IP prefixes or all MAC addresses for all virtual machines in the CSP's data centre. A given virtual router only needs to contain those routing instances that are locally installed on the same server.
Roles	CSC, CSP

Figure (optional)	
Pre-conditions (optional)	– CSP's IP carrier network support overlay network mechnism.
Post-conditions (optional)	– CSC's VMs that run in different CSP's data centres can communicate with each other.
Derived requirements	– Logically isolated network partition (refer to clause 9.12) – Overlay network mechanism (refer to clause 9.13)

II.4.2.7 NaaS connectivity use case for private IP addresses and VPNs

Title	NaaS connectivity use case for private IP addresses and VPNs
Description	Case I: Public cloud site multi-tenant VPN gateway (GW) with overlapping private IP addresses Multi-tenant VPN GW in a public cloud site is shared by CSC-I-A and CSC-I-B. Both of them are interested to use the same private IP address pool for their end points. Both of CSCs are connected to the public cloud VPN GW through a given public IP address of it. The cloud VPN GW should be able to switch the traffic from each CSC to a proper subnet. Case II: Interworking support for different types of VPNs CSC-II has site-to-site proprietary MPLS-VPN connection between its headquarter (HQ) and private data centre. According to the company progress, CSC-II is interested to establish new site-to-site and site-to-client secure VPN connections (e.g., IP security (IPsec) VPN and secure socket layer (SSL) VPN). New VPN connections are planned between their globally distributed branch offices and mobile users, while keeping the CSC-II existing VPN investments. NaaS CSP should be able to provide interworking between the CSC owned existing VPN and different types of new VPNs. Case III: On-demand network support for the distributed end points CSC-III requires a solution of delivering reliable, predictable and on-demand network connections for all their locations. This service should be able to be changed dynamically according to the CSC-III's needs. The CSC-III is interested in elastic request parameters for connectivity to their location over the existing links. The connectivity should be established to one or more of the NaaS CSP's points of presence (PoPs) with minimum efforts for deploying additional equipment.
Roles	CSP, CSC

Figure (optional)

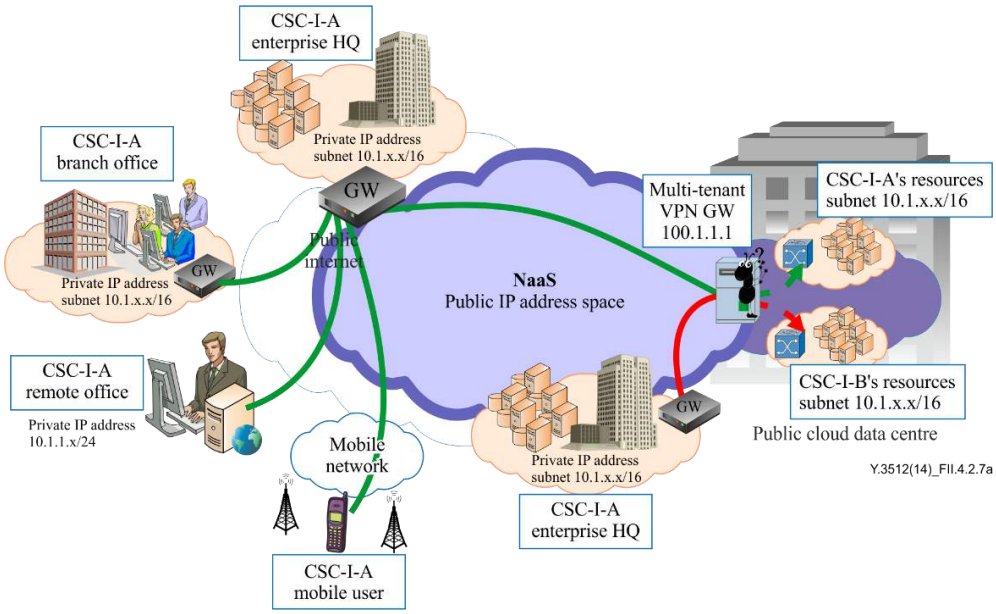


Figure 1 – Case I: Public Cloud site multi-tenant VPN GW with overlapping private IP addresses

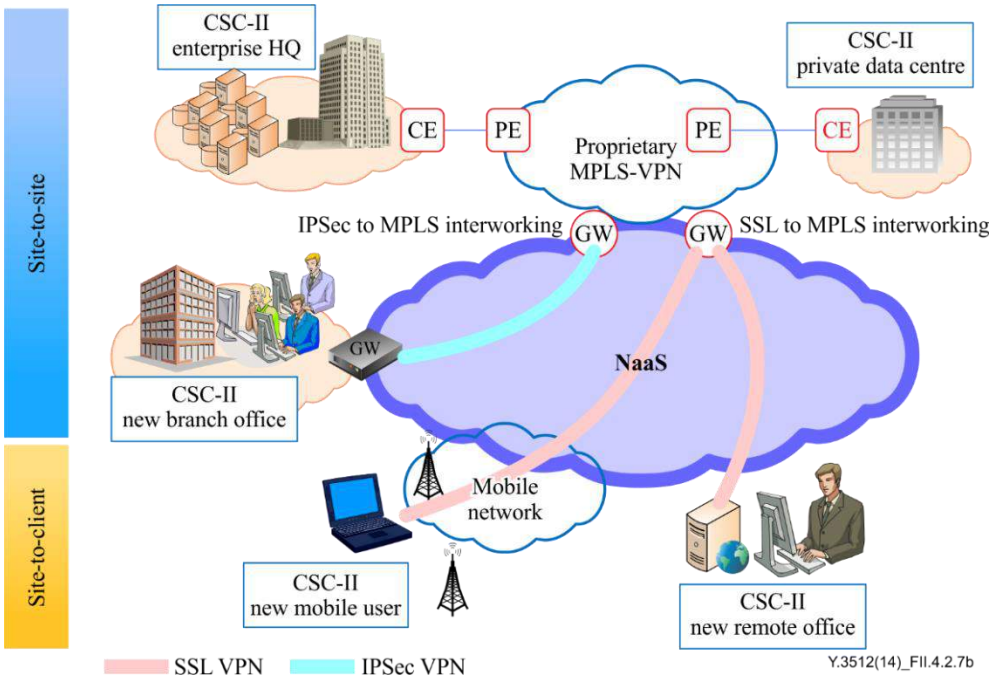
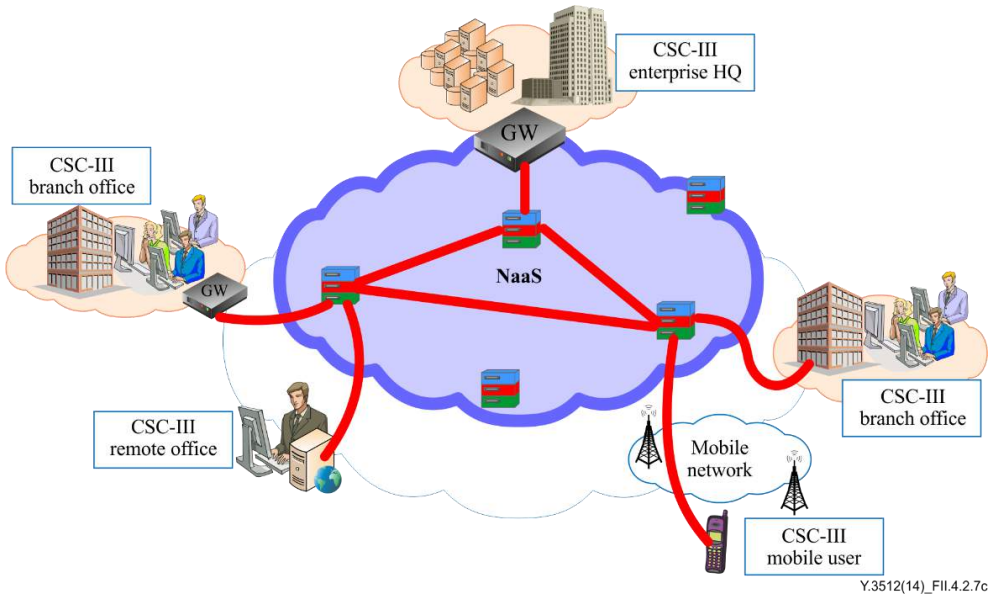


Figure 2 – Case II: Interworking support for different types of VPNs

	 **Figure 3 – Case III: On-demand network support for the distributed end points**
Pre-conditions (optional)	It is assumed that multi-tenant VPN GW in public cloud site is provided by the NaaS CSP.
Post-conditions (optional)	
Derived requirement	– Overlapped private IP addresses (refer to clause 9.14) – Interworking among different VPN solutions (refer to clause 9.15) – VPN connection in mobile environment (refer to clause 9.16) – Connection to NaaS CSP's network through public Internet (refer to clause 9.17)

Appendix III

Considerations on CSP's network related activities

(This appendix does not form an integral part of this Recommendation.)

This appendix provides considerations on CSP's network related activities.

Each individual service of the NaaS category can be specified by a set of terms including:

- Service interface – It is offered to the CSC and defines the functionality which is implemented by the CSP. Service interface can include functionality related to demarcation points for the interconnection of the CSP and the CSC, topology and route related functionality to share topologies, discovery related functionality to perform other services needed by inter-cloud related activities, and other functionalities related to monitoring, protection, verification, etc. Route related functionality requires information on ingress and egress end points and optionally intermediate points of a network segment. Attributes of a network segment can include edge point attributes, QoS parameters, performance attributes, time attributes, user attributes, service requester identifier, etc.
- Service demarcation point – This is a boundary point between NaaS CSP and NaaS CSC. It is used as a reference point to identify the responsibilities and obligations of all involved entities. For IP/MPLS networks, the demarcation point user-to-network interface (UNI) is a pair of customer edge and provider edge. For other transport networks, UNI and network-to-network interface (NNI) are defined as demarcation points. For example, UNI defined by Metro Ethernet Forum (MEF) is physically implemented over a bi-directional Ethernet link that provides the various data, control and management plane capabilities required by the metro Ethernet network (MEN) service provider to clearly demarcate the two different network domains involved in the operational, administrative, maintenance and provisioning aspects of the service. Often software abstraction layer (SAL) or network operating system (NOS) is used for the demarcation point for network platforms, and TCP/UDP sockets for network applications.
- Service capabilities – This is what NaaS delivers to the CSC via service interfaces as network connectivity and networking related service capabilities. While transport network connectivity capabilities include IP/MPLS network, transmission networks, IP multimedia subsystem (IMS), software defined networking (SDN) and CDN, virtual network connectivity capabilities include pseudo-wire, virtual private LAN service (VPLS), L3 VPN and VLAN. Networking related service capabilities can include WAN optimization, load balancing, domain name system (DNS), firewall, IPS/IDS, telecommunication services and network applications such as peer-to-peer (P2P) based file transfer, etc.

Although infrastructure capability type NaaS can provide such network as a whole, a CSC relies on CSP for the integration and customizing of software, reconfiguring and expanding functionalities of network elements, as well as management and administration of the network. When CSC leverages NaaS platforms to build its own network, the responsibility of CSP is up to the service demarcation point of the platform. CSC is responsible for managing, administering and operating the network as well as network functions and services implemented up on the demarcation point.

The composite services provisioned in cloud environments need SLA support in the following areas [b-EC SLA]:

- SLA specifications capturing the dependencies and interactions between the services. The dependencies should be parametric and express the overall service context (e.g., data movements, relationships between providers, orchestration rules).
- Convergence in SLA management to handle dependencies (e.g., joint management) while retaining the autonomy in resource management for each provider.

Enhanced SLA specification and management approaches should take into consideration that composition may be performed as either centralized (e.g., an entity managing the composition and the corresponding

service offerings) or distributed (e.g., achieved through consecutive SLA establishments) approaches. SLA specifications in cross-service scenarios should either include the common terms (limiting however end-to-end quality provision to these terms) or be implemented through links between SLAs (e.g., one SLA for each service with enriched specification to include links to the SLAs of other services), as a protocol to enable interaction between different layers and entities.

SLAs identify, in a clear and precise way, the responsibilities and obligations of all involved entities, as well as their boundaries and limits.

NaaS can be used to support other cloud service CSP's network related activities (e.g., provide network connectivity, deliver network services and provide network management services), where a logically isolated CSC cloud in the CSP's data centre allows a CSC to provision a private, isolated partition of the cloud where the CSC can use cloud capabilities in a virtual network, often using CSC-defined IP address ranges. A CSC cloud can have multiple subnets in a data centre. Network connectivity between the remote CSC and CSC cloud, for example, may include the following:

- IPsec VPN connection over public Internet (CSP edge VPN gateway – CSC premises VPN gateway);
- Dedicated network connection over private lines (CSP edge VPN gateway – customer premises equipment (CPE));
- IPsec VPN connection over private lines (CSP edge VPN gateway – CSC premises VPN gateway);
- VPN connection with a software appliance over public Internet (software VPN appliance – CSP edge Internet gateway - CSC premises VPN gateway, where Internet gateway only routes VPN connection over public Internet);
- Multi-protocol label switching (MPLS) VPN connections.

Cloud services needs interconnecting multiple CSC clouds into a contiguous virtual network as well as to meet this requirement NaaS may provide followings:

- Software VPN appliance based connections between CSC clouds for intra-cloud and inter-cloud (software VPN appliance at CSC cloud-1 – Internet gateway – Internet gateway – software VPN appliance at CSC cloud-2, where Internet gateway only routes VPN connection, over public Internet for inter-cloud case);
- Software VPN appliance to physical VPN connection between CSC clouds (VPN gateway at CSC cloud-1 – Internet gateway – software VPN appliance at CSC cloud-2, where Internet gateway only routes VPN connection);
- CSC managed CSC cloud-to-CSC cloud routing over physical IPsec VPN connections using CSC equipment and public Internet or private lines (VPN gateway at CSC cloud-1 – CSC equipment – VPN gateway at CSC cloud-2).

Bibliography

[b-IETF RFC 4364] IETF RFC 4364 (2006), *BGP/MPLS IP Virtual Private Networks (VPNs)*.

[b-EC SLA] European Commission Directorate General Communications Networks, Content and Technology Unit E2 – Software and Services, Cloud, (Brussels, June 2013), *Cloud Computing Service Level Agreements – Exploitation of Research Results*.


IaaS

Cloud computing – Functional requirements of Infrastructure as a Service

Recommendation ITU-T Y.3513

(08/2014)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Summary

Recommendation ITU-T Y.3513 introduces the concept of Infrastructure as a Service (IaaS) and describes its functional requirements. As one of the cloud computing service categories, Infrastructure as a Service provides cloud service customers with computing, storage and network services by cloud service providers. To derive those requirements, relevant use cases are also presented.

Keywords

Cloud computing, Infrastructure as a Service, IaaS, virtual machine.

Table of Contents

1 Scope

This Recommendation provides functional requirements and use cases of Infrastructure as a Service (IaaS), one of the representative cloud service categories. This Recommendation covers the following:

– General description of IaaS;

– Functional requirements of IaaS;

– Typical IaaS use cases.

NOTE – The general requirements of IaaS can be found in [ITU-T Y.3501].

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1601] Recommendation ITU-T X.1601 (2014), *Security framework for cloud computing*.

[ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014), Information technology – *Cloud computing – Overview and vocabulary*.

[ITU-T Y.3501] Recommendation ITU-T Y.3501 (2013), *Cloud computing framework and high-level requirements*.

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), Information technology – *Cloud computing – Reference architecture*.

[ITU-T Y.3510] Recommendation ITU-T Y.3510 (2013), *Cloud computing infrastructure requirements*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 cloud capabilities type [ITU-T Y.3500]: Classification of the functionality provided by a cloud service to the cloud service customer, based on resource used.

NOTE – The cloud capabilities types are application capabilities type, infrastructure capabilities type and platform capabilities type.

3.1.2 cloud computing [ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

3.1.3 cloud service [ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.4 cloud service category [ITU-T Y.3500]: Group of cloud services that possess some common set of qualities.

NOTE – A cloud service category can include capabilities from one or more cloud capabilities types.

3.1.5 cloud service customer [ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

3.1.6 cloud service customer data [ITU-T Y.3500]: Class of data objects under the control, by legal or other reasons, of the cloud service customer that were input to the cloud service, or resulted from exercising the capabilities of the cloud service by or on behalf of the cloud service customer via the published interface of the cloud service.

NOTE 1 – An example of legal controls is copyright.

NOTE 2 – It may be that the cloud service contains or operates on data that is not cloud service customer data; this might be data made available by the cloud service providers, or obtained from another source, or it might be publicly available data. However, any output data produced by the actions of the cloud service customer using the capabilities of the cloud service on this data is likely to be cloud service customer data, following the general principles of copyright, unless there are specific provisions in the cloud service agreement to the contrary.

3.1.7 cloud service provider [ITU-T Y.3500]: Party which makes cloud services available.

3.1.8 cloud service provider data [ITU-T Y.3500]: Class of data objects, specific to the operation of the cloud service, under the control of the cloud service provider.

NOTE – Cloud service provider data includes but is not limited to resource configuration and utilization information, cloud service specific virtual machine, storage and network resource allocations, overall data centre configuration and utilization, physical and virtual resource failure rates, operational costs and so on.

3.1.9 Infrastructure as a Service [ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer is an infrastructure capabilities type.

NOTE – The cloud service customer does not manage or control the underlying physical and virtual resources, but does have control over operating systems, storage, and deployed applications that use the physical and virtual resources. The cloud service customer may also have limited ability to control certain networking components (e.g., host firewalls).

3.1.10 infrastructure capabilities type [ITU-T Y.3500]: Cloud capabilities type in which the cloud service customer can provision and use processing, storage or networking resources.

3.1.11 open virtualization format [b-ISO/IEC OVF]: An open, secure, portable, efficient and extensible format for the packaging and distribution of software to be run in virtual machines.

3.1.12 party [ITU-T Y.3500]: Natural person or legal person, whether or not incorporated, or a group of either.

3.1.13 tenant [ITU-T Y.3500]: Group of cloud service users sharing access to a set of physical and virtual resources.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CPU	Central Processing Unit
CSC	Cloud Service Customer
CSP	Cloud Service Provider
LUN	Logical Unit Number
IaaS	Infrastructure as a Service
IP	Internet Protocol
I/O	Input/Output
NaaS	Network as a Service
NAT	Network Address Translation
NIC	Network Interface Card

OVF	Open Virtualization Format
QoS	Quality of Service
SLA	Service Level Agreement
UML	Unified Modelling Language
VLAN	Virtual Local Area Network
VM	Virtual Machine

5 Conventions

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

In the body of this Recommendation and its annexes, the words shall, shall not, should, and may sometimes appear, in which case they are to be interpreted, respectively, as is required to, is prohibited from, is recommended, and can optionally. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative are to be interpreted as having no normative intent.

6 General description

Infrastructure as a Service (IaaS) is one of the representative categories of cloud services, in which the cloud capabilities type provided to the cloud service customer (CSC) is an infrastructure capabilities type. IaaS allows the CSC to use cloud infrastructure resources (processing, storage or networking). Use of cloud infrastructure resources is supported by service functions, which can include the relevant operations.

IaaS provides to the CSC the following service functions:

– **computing service functions** allow the CSC to provision and use processing resources. CSC can perform operations relevant to processing resources including machine (physical or virtual machine) lifecycle operations and functions such as virtual machine (VM) migration, backup, snapshot, clone and reservation;

– **storage service functions** allow the CSC to use storage resources. The CSC can perform operations relevant to storage resources including lifecycle operations and functions such as snapshot, backup, input/output (I/O) performance, load balance and reservation;

– **network service functions** allow the CSC to use networking resources. The CSC can integrate infrastructure resources using network relevant functions such as IP address, network isolation (e.g., virtual local area network (VLAN)), virtual networking (e.g., virtual switch), load balance and firewall.

The high level concept of IaaS using the layering framework defined in [ITU-T Y.3502] is illustrated in Figure 6-1.

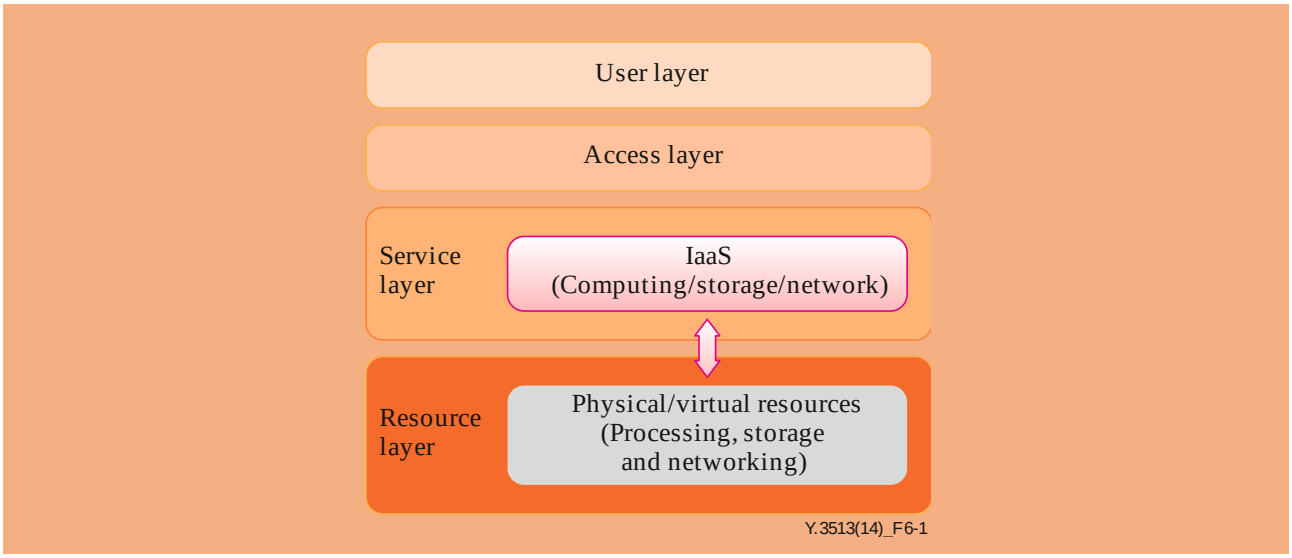


Figure 6-1 – High level concept of IaaS

An IaaS instance can be configured by the CSC using a template to define the set of parameters stating, how infrastructure resources are organized. Such IaaS instance consists of configured processing, storage or networking resources, as well as information located in the resources, which may include cloud service provider data, cloud service customer data or both.

IaaS cloud service provider (CSP) also provides business and administration capabilities to CSC, which are common capabilities for cloud services. The functional requirements of business and administration capabilities are for further study.

NOTE – Regarding the network connectivity, one important difference between IaaS and Network as a Service (NaaS) is that IaaS is a cloud service category that is offered in only one flavour of cloud capability type, and that is infrastructure capabilities type [ITU-T Y.3500]. However, NaaS is a cloud service category that can be offered in all three cloud capabilities types.

7 Functional requirements

– It is recommended that IaaS CSP provides to the CSC IaaS functions, such as a composition of processing, storage, and networking resources with service logic, specific service level agreements (SLAs) and charging model.

– It is required that IaaS CSP provides the CSC with operations handling mechanisms related to provisioned infrastructure resources, such as assign, modify, query and release.

– It is recommended that IaaS CSP provides status information about the infrastructure in response to queries from the CSC.

NOTE – The status information includes, but not limited to, available, reserved and in-use.

– It is recommended that IaaS CSP provides template to the CSC, related to instantiation of infrastructure, which allows to provision processing, storage and networking resources that could be implemented based on the configuration.

– It is recommended that IaaS CSP provides the CSC with operations handling mechanisms related to infrastructure templates to allow modification of infrastructure, such as upload, update, disable, enable, query or release.

7.1 Computing service functional requirements

– It is required that IaaS CSP provides computing functions with specific SLAs and charging model to the CSC.

7.1.1 Physical machine

– It is recommended that IaaS CSP provides specific hardware specifications of physical machine to the CSC according to SLA.

NOTE – SLA includes, but not limited to, central processing unit (CPU) type, CPU speed, number of CPU cores, memory size, disk size and network interface card (NIC) number.

– It is recommended that IaaS CSP provides the CSC with operation handling mechanisms related to physical machine such as start, shutdown, hibernate and wakeup.

– It is recommended that IaaS CSP provides physical machine related information in response to queries from the CSC.

NOTE – The information includes, but not limited to, physical machine specifications, status and network interfaces.

7.1.2 Virtual machine

– It is recommended that IaaS CSP provides virtual machine based on the VM template.

NOTE – By using the VM template, CSC can select the required number of CPU cores, memory size, disk size, NIC within the resources available according to SLA.

– IaaS CSP can optionally provide virtual machine based on the configurations specified by the CSC.

– It is required that IaaS CSP provides the CSC with operations handling mechanisms related to VM, including, but not limited to, create, delete, start, shutdown, suspend, restore, hibernate and wakeup.

– It is recommended that IaaS CSP provides VM related information in response to queries from the CSC.

NOTE – The VM related information includes, but not limited to, VM specifications, volume information, VM status, IP address and network interfaces.

7.1.3 VM migration

– It is recommended that IaaS CSP provides virtual machine with migration functions. Based on migration policies, the virtual machine can be migrated from one host to another.

7.1.4 VM scaling

– It is recommended that IaaS CSP provides virtual machine with scaling functions based on the scaling policies and monitored events of the virtual machine.

NOTE – The types of VM scaling includes, but not limited to, configuration changes (e.g., CPU, memory, bandwidth increased or bandwidth decreased) or components changes (new virtual machine added or removed).

7.1.5 VM snapshot

– It is recommended that IaaS CSP provides virtual machine with snapshot functions. Schedule of snapshots taken from the virtual machine can be performed automatically or manually.

7.1.6 VM clone

– It is recommended that IaaS CSP provides virtual machine with clone functions. The cloned VM has identical configuration and CSP/CSC data as the original one.

7.1.7 VM backup

– It is recommended that IaaS CSP provides virtual machine with backup functions. When VM becomes faulty or its data is lost, the VM can be restored using its backup stored according to the CSC policy.

7.1.8 VM time synchronization

– It is recommended that IaaS CSP provides time synchronization functions, which allow the CSC to control the VM time.

7.1.9 VM reservation

– It is recommended that IaaS CSP provides processing resources reservation (such as CPU, memory) functions. Resources reservation is used to reserve available resources from IaaS infrastructure before VM is initiated.

7.1.10 VM image

– It is recommended that IaaS CSP offers the ability for the CSC to provide and use virtual machine images. VM image consists of infrastructure configuration and CSP data, CSC data or both.

NOTE – VM image allows to start a new instance of VM.

– It is recommended that IaaS CSP supports different machine image format.

– It is required that IaaS CSP provides operation handling mechanisms related to image，including, but not limited to, add, import, store, register, deregister, query, update, delete and export.

7.1.11 VM template

– It is recommended that IaaS CSP supports open virtualization format (OVF) template, which is a packaging standard designed to address the portability and deployment of virtual appliances.

– It is recommended that IaaS CSP provides operations handling mechanisms related to machine templates, such as upload, update, disable, enable, query and delete to the CSC.

7.2 Storage service functional requirements

– It is recommended that IaaS CSP provides storage functions, such as block level storage, file level storage and object-based storage, with specific SLAs and charging model to the CSC. The storage functions can be provided to the CSC directly or used by the virtual machine as attached storage.

– It is recommended that IaaS CSP provides the CSC with operations handling mechanisms related to storage, such as create, attach, detach, query and delete a volume of storage at either block level or file-system level, write, read and delete data for a given storage.

– It is recommended that IaaS CSP provides storage utilisation information in response to queries from the CSC.

7.2.1 Storage migration

– It is recommended that IaaS CSP provides storage migration functions. Based on migration policies, data can be migrated between different logical unit numbers (LUNs), different storage devices, local storage to shared storage and vice versa.

7.2.2 Storage snapshot

– It is recommended that IaaS CSP provides storage with snapshot functions. Snapshot can be realized at either block or file-system levels. The data can be restored using the snapshot.

7.2.3 Storage backup

– It is recommended that IaaS CSP provides storage with backup functions. Backup can be realized at block level, file level or object-based storage.

7.2.4 I/O performance

– It is recommended that IaaS CSP provides input/output (I/O) limitation for each VM.

7.2.5 Storage resource reservation

– It is recommended that IaaS CSP provides storage resource (e.g., storage space and LUN) reservation functions.

7.3 Network service functional requirements

– It is recommended that IaaS CSP provides network functions, such as IP address, VLAN, virtual switch, load balance, firewall, with specific SLAs or charging model. Network functions are applied to access and interconnect of processing and storage resources.

– It is recommended that IaaS CSP provides network information in response to queries from the CSC.

NOTE – The information includes, but not limited to, network device(s) specification, network traffic performance (in terms of throughput, jitter, loss, delay) and network topology.

7.3.1 Network policy migration

– It is recommended that IaaS CSP provides network policy migration along with virtual machine migration. In that case, the network policy of the migrated virtual machine is the same as before the migration.

7.3.2 Network QoS

– It is recommended that IaaS CSP provides operation handling mechanisms related to the network quality of service (QoS), such as bandwidth limit, bandwidth reservation, traffic shaping, traffic classification, congestion avoidance, at port level, device level and network level.

7.3.3 IP address

– It is recommended that IaaS CSP provides IP address reservation.

NOTE – CSP reserves a pool of public IP addresses or a segment of private IP addresses for the CSC.

– It is required that IaaS CSP allows the CSC to apply, bind, unbind, query, release an IP address to processing resources or storage resources.

– It is recommended that IaaS CSP allows the CSC to allocate IP addresses to provisioned processing resources or storage resources with dynamic or static method.

– IaaS CSP can optionally provide network address translation (NAT).

7.3.4 Network isolation

– It is required that IaaS CSP provides the CSC with isolated tenants' networks.

– It is recommended that IaaS CSP provides the CSC with operations handling mechanisms related to isolated tenants' networks, such as create, query and release.

7.3.5 Virtual networking

– It is recommended that IaaS CSP manages virtual networking to provide network connectivity amongst various processing and storage resources.

7.3.6 Load balance

– It is recommended that IaaS CSP optimizes infrastructure resources utilization by providing load balance related functions, such as throughput, response time, to avoid overload of any one of the infrastructure resources.

– IaaS CSP can optionally provide multipath routing to achieve an optimized traffic management (e.g., to improve network utilization, to guarantee QoS at network congestion or fault).

7.3.7 Firewall

– It is recommended that IaaS CSP delivers physical or virtual firewall to the CSC.

7.3.8 Gateway

– It is recommended that IaaS CSP provides necessary network interworking functions so that the CSC uses provisioned infrastructure resources as if they are at the CSC's premises.

7.3.9 Network configuration

– It is recommended that IaaS CSP provides the CSC with operations handling mechanisms related to the network configurations according to the objectives of the SLA.

8 Security considerations

Security aspects for consideration within the cloud computing environment, including IaaS, are addressed by security challenges for the CSPs, as described in [ITU-T X.1601]. In particular, [ITU-T X.1601] analyses security threats and challenges, and describes security capabilities that could mitigate these threats and meet the security challenges.

Appendix I

Use case of Infrastructure as a Service

(This appendix does not form an integral part of this Recommendation.)

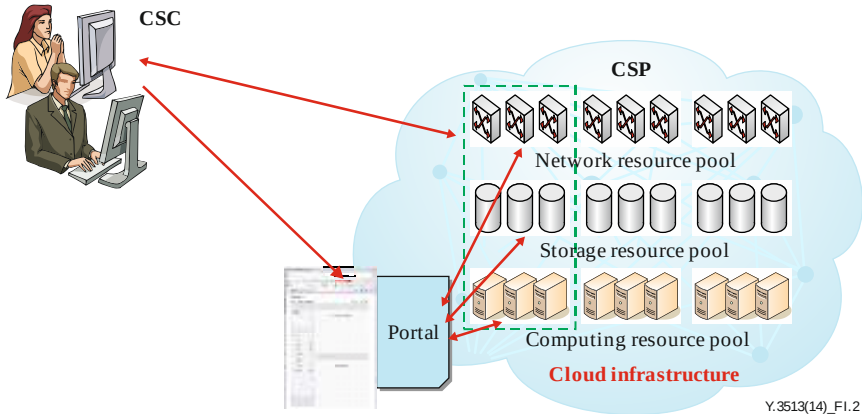
This appendix includes IaaS related use cases including an infrastructure level use case, and computing , storage and network service use cases.

I.1 Use case template

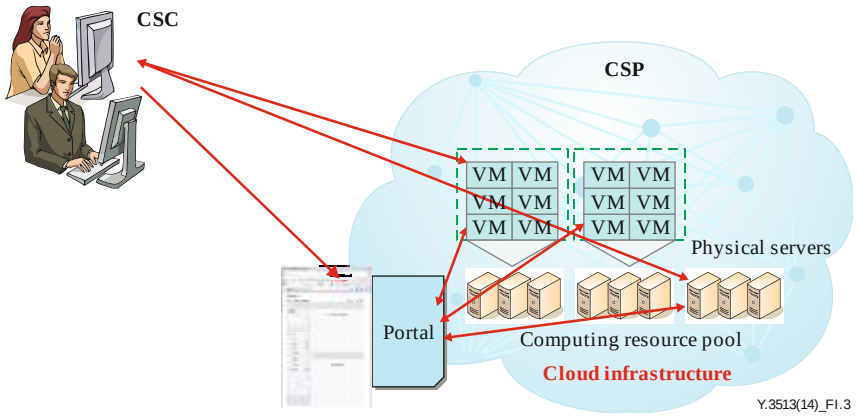
The use cases developed in this appendix should adopt the following unified format for better readability and convenient material organization.

Use case	
Name	Title of the use case
Abstract	Description for overview and feature of the use case
Roles	Roles relating to or appearing in the use case
Figure	Figure to present the use case (UML-like diagram is suggested for clarifying relations between roles but it is not mandatory)
Pre-conditions (optional)	The pre-conditions represent the necessary conditions or use cases that should be achieved before starting to describe the use case. As dependency may exist among different use cases, such a description can help others to understand relation among the use cases.
Post-conditions (optional)	Similar to that for pre-conditions, the post-conditions describe conditions or use cases that will be carried out after the termination of currently describing use case. Such an inter-use case dependency clarification improves the collaboration of use cases.
Description	Description introduces the detail information of the use case, such as the processes or major steps. It is helpful for the reader to better understand it.
Requirements	Requirements (titles) derived from the use case. For example; – **Large-scale migration**: A CSP in the inter-cloud federation is required to be able to guarantee continuity of all the services in this CSP by large-scale service migration with minimum impact during a desired period. It is recommended to consider priority of services when migrating.

I.2 IaaS use case on infrastructure level

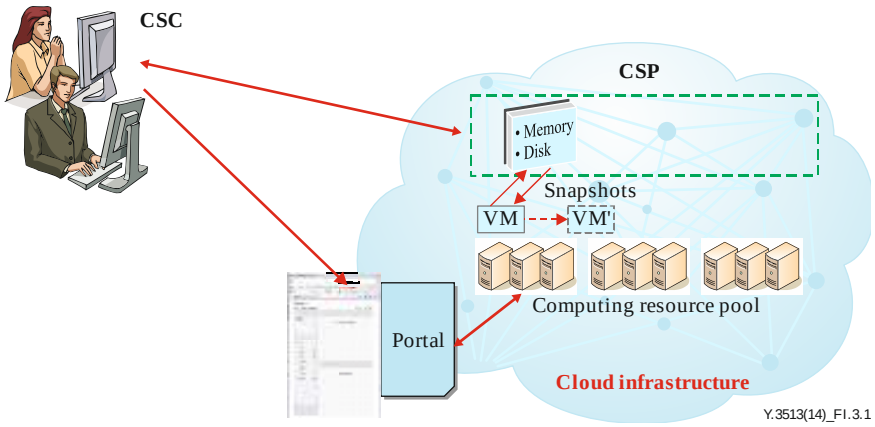
Use case	
Name	IaaS use case on infrastructure level
Abstract	CSC uses a composition of processing, storage and networking resources with service logic, specific SLAs and charging model, provided by the CSP
Roles	CSC, CSP
Figure	
Pre-conditions (optional)	– CSC accesses the IaaS through portal with appropriate security mechanism and retrieves computing, storage and network functions.
Post-conditions (optional)	
Description	– CSC accesses and queries the CSP portal to retrieve the list of supported functions (e.g., infrastructure templates) related to the infrastructure. – CSC selects the appropriate infrastructure template from the query results and requests the CSP to create an infrastructure based on the selection. – CSC manages and monitors the created infrastructure during its lifecycle. It includes, but not limited to: • **assign**: start IaaS by allocating to the service the **available resources** as identified by **configuration** (e.g., create, initiate, start, enable, power-on) • **modify**: change the amount of **resource** being **in-use** according to the demand (e.g., update, add, enable, disable) • **release**: close the IaaS service by making **available** the **resource** being **in-use** by the service (e.g., delete, shutdown, disable, power-off) • **query**
Requirements	– IaaS operations (refer to clause 7) – Infrastructure resources status (refer to clause 7) – Infrastructure template (refer to clause 7)

I.3 IaaS computing service use case

Use case	
Name	IaaS use case on computing
Abstract	CSC uses physical machine or virtual machine provided by the CSP.
Roles	CSC, CSP
Figure	
Pre-conditions (optional)	– CSC accesses the IaaS through portal with appropriate security mechanism and retrieves the functions exposed that are related to computing.
Post-conditions (optional)	
Description	– CSC accesses and queries the CSP portal to retrieve the list of supported functions necessary for computing functions. – CSC selects the appropriate template and image from the query results and requests CSP to create a virtual machine or physical machine based on the selection. – CSP creates a virtual machine or physical machine from the computing resource pool based on the information provided by the CSC. – CSC requests CSP to start up the virtual machine or physical machine. – CSC manages and monitors the created virtual machine or physical machine during its lifecycle. It includes, but not limited to: • start, shutdown, suspend, restore, hibernate, wakeup and delete the virtual machine; • start, shutdown, hibernate and wakeup physical machine; • query the virtual machine or physical machine information and its status; • set migration or scaling policies for the virtual machine; • scaling the virtual machine; • execute performance metrics; • snapshot, backup, clone the virtual machine; • configure VM time synchronization; • reservation computing resource; • make image based on the virtual machine; • generate template based on the virtual machine.
Requirements	– Physical machine (refer to clause 7.1.1) – Virtual machine (refer to clause 7.1.2) – VM migration (refer to clause 7.1.3) – VM scaling (refer to clause 7.1.4) – VM snapshot (refer to clause 7.1.5) – VM clone (refer to clause 7.1.6) – VM backup (refer to clause 7.1.7) – VM time synchronization (refer to clause 7.1.8)

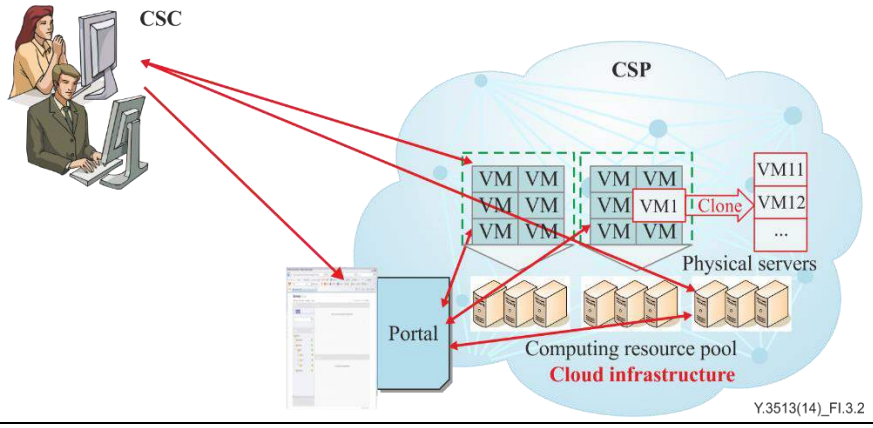
Use case	
	– VM reservation (refer to clause 7.1.9) – VM image (refer to clause 7.1.10) – VM template (refer to clause 7.1.11)

I.3.1 VM snapshot use case

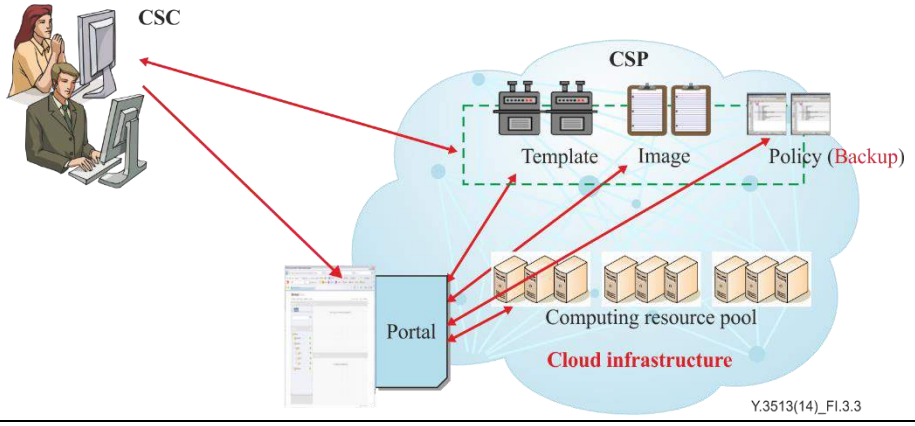
Use case	
Name	IaaS use case on VM snapshot
Abstract	CSC uses the snapshot functions during the lifecycle of a VM.
Roles	CSC, CSP
Figure	
Pre-conditions (optional)	– CSC accesses the IaaS through portal with appropriate security mechanism. – CSC has created a VM which is in normal running state, stopped state or suspending state.
Post-conditions (optional)	
Description	– CSC has found that the VM is working properly; and an operation that may cause faults, for example, conducting a software upgrade, is to be performed. – CSC snapshots the VM, a name for the snapshot is required while the description is optional. It also contains the runtime information, including the VM CPU and memory states, if the VM is not powered-off. – CSC performs the software upgrade operation, VM is in VM' (as the figure shows) state and there is something wrong, for example, the user data of the software has been lost and VM cannot work properly. – CSC recovers the VM using the snapshot it created above and all the software running on the VM is recovered to state "VM" too.
Requirements	– VM snapshot (refer to clause 7.1.5)

I.3.2 VM clone use case

Use case	
Name	IaaS use case on VM clone
Abstract	CSC uses the clone functions to create a new VM.
Roles	CSC, CSP

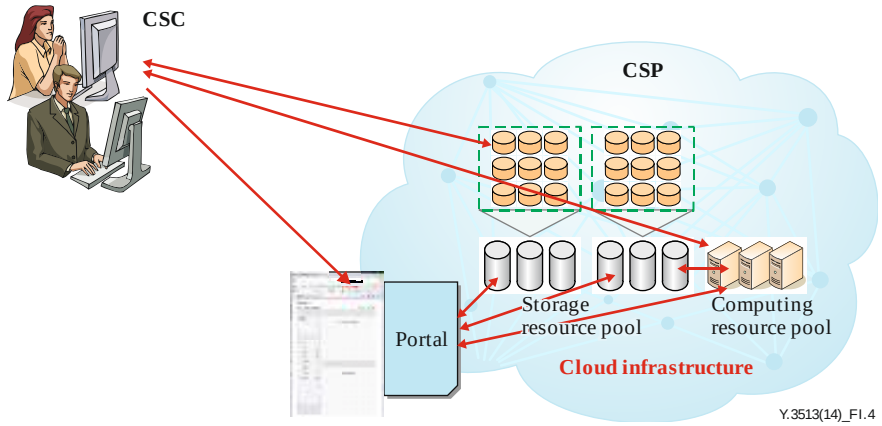
Use case	
Figure	
Pre-conditions (optional)	– CSC accesses the IaaS through portal with appropriate security mechanism. – CSC has created a VM (e.g., VM1). – CSC needs more VMs identical or similar to VM1.
Post-conditions (optional)	
Description	– CSC selects VM1 which it wants to clone. – CSC selects clone operation, and changes some regular parameters, for example, VM name, the number of CPUs and memory. In this case, CSC clones two VMs, i.e., VM11 and VM12. – CSC starts the cloned VMs, and the cloned VMs are similar to the original one, with slight difference in the changed parameters.
Requirements	– VM clone (refer to clause 7.1.6)

I.3.3 VM backup use case

Use case	
Name	IaaS use case on VM backup
Abstract	CSP recovers the VM according to the backup policies CSC configured.
Roles	CSC, CSP
Figure	
Pre-conditions (optional)	– CSC accesses the IaaS through portal with appropriate security mechanism. – CSC has created a VM which is in a normal running state and deployed CSC's application on the VM. – CSC needs backup functions to support its application.
Post-conditions (optional)	

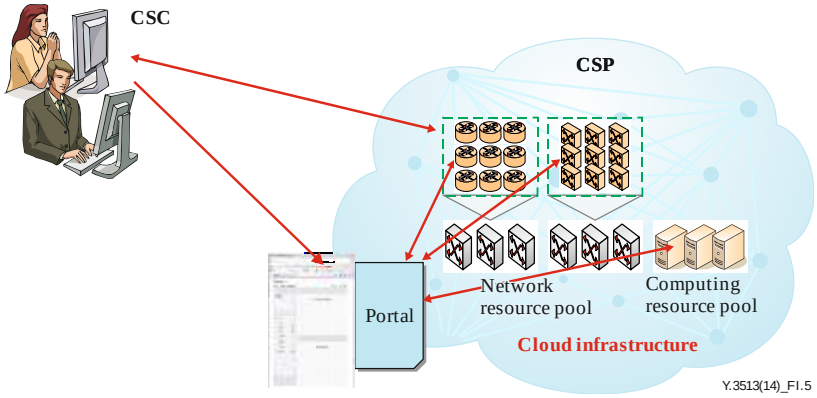
Use case	
Description	– CSC configures the backup policy for the VM, and the policy could be weekly backup. – CSP performs the backup operation according to the policy the CSC configured. – CSP detects that the VM becomes faulty or its data is lost, CSP recovers the VM using backup automatically without CSC's awareness.
Requirements	– VM backup (refer to clause 7.1.7)

I.4 IaaS storage service use case

Use case	
Name	IaaS use case on storage
Abstract	CSC uses block, file or object storage directly or attach to the virtual machine provided by the CSP
Roles	CSC, CSP
Figure	
Pre-conditions (optional)	– CSC accesses the IaaS through the portal with appropriate security mechanism and retrieves the functions exposed that are related to storage and attached computing, if needed.
Post-conditions (optional)	
Description	– CSC accesses and queries the CSP portal to retrieve the list of supported functions related to storage functions. – CSC selects the appropriate storage from the query results and requests the CSP to create block, file or object storage based on the selection. – CSP creates block, file or object storage from the storage resource pool based on the information provided by the CSC. – CSC attaches the created storage to specified virtual machine if needed. – CSC manages and monitors the created storage during its lifecycle. It includes, but not limited to: • create, attach, detach, query and delete a volume of storage at either block level or file-system level; • write, read and delete data; • query the storage information and its status; • set migration or I/O limitation policies; • execute performance metrics; • snapshot or backup the storage; • reservation storage resource.

Use case	
Requirements	– Storage migration (refer to clause 7.2.1) – Storage snapshot (refer to clause 7.2.2) – Storage backup (refer to clause 7.2.3) – I/O performance (refer to clause 7.2.4) – Storage resource reservation (refer to clause 7.2.5)

I.5 IaaS network service use case

Use case	
Name	IaaS use case on network
Abstract	CSC uses network functions, such as IP address, VLAN, virtual switch, load balance and firewall provided by the CSP
Roles	CSC, CSP
Figure	
Pre-conditions (optional)	– CSC accesses the IaaS through portal with appropriate security mechanism and retrieves the functions exposed that are related to network and computing, if needed.
Post-conditions (optional)	
Description	– CSC accesses and queries the CSP portal to retrieve the list of supported network functions (e.g., IP address, VLAN, virtual switch, load balance, firewall). – CSC selects the appropriate network service from the query results and requests CSP to create a network based on the selection. – CSC requests the CSP to attach the created network with the related virtual machine. – CSC manages and monitors the created network during its lifecycle. It includes, but not limited to: • bind the network connectivity service to the related virtual machine; • query the network and its status; • update, upgrade or scaling the network; • execute performance metrics; • manage the IP address pool; • manage network services, such as VLAN, virtual switch, load balance, firewall, gateway; • manage tenants' network according to the SLA objectives.

Use case	
Requirements	– Network policy migration (refer to clause 7.3.1) – Network QoS (refer to clause 7.3.2) – IP address (refer to clause 7.3.3) – Network isolation (refer to clause 7.3.4) – Virtual networking (refer to clause 7.3.5) – Load balance (refer to clause 7.3.6) – Firewall (refer to clause 7.3.7) – Gateway (refer to clause 7.3.8) – Network configuration (refer to clause 7.3.9)

Appendix II

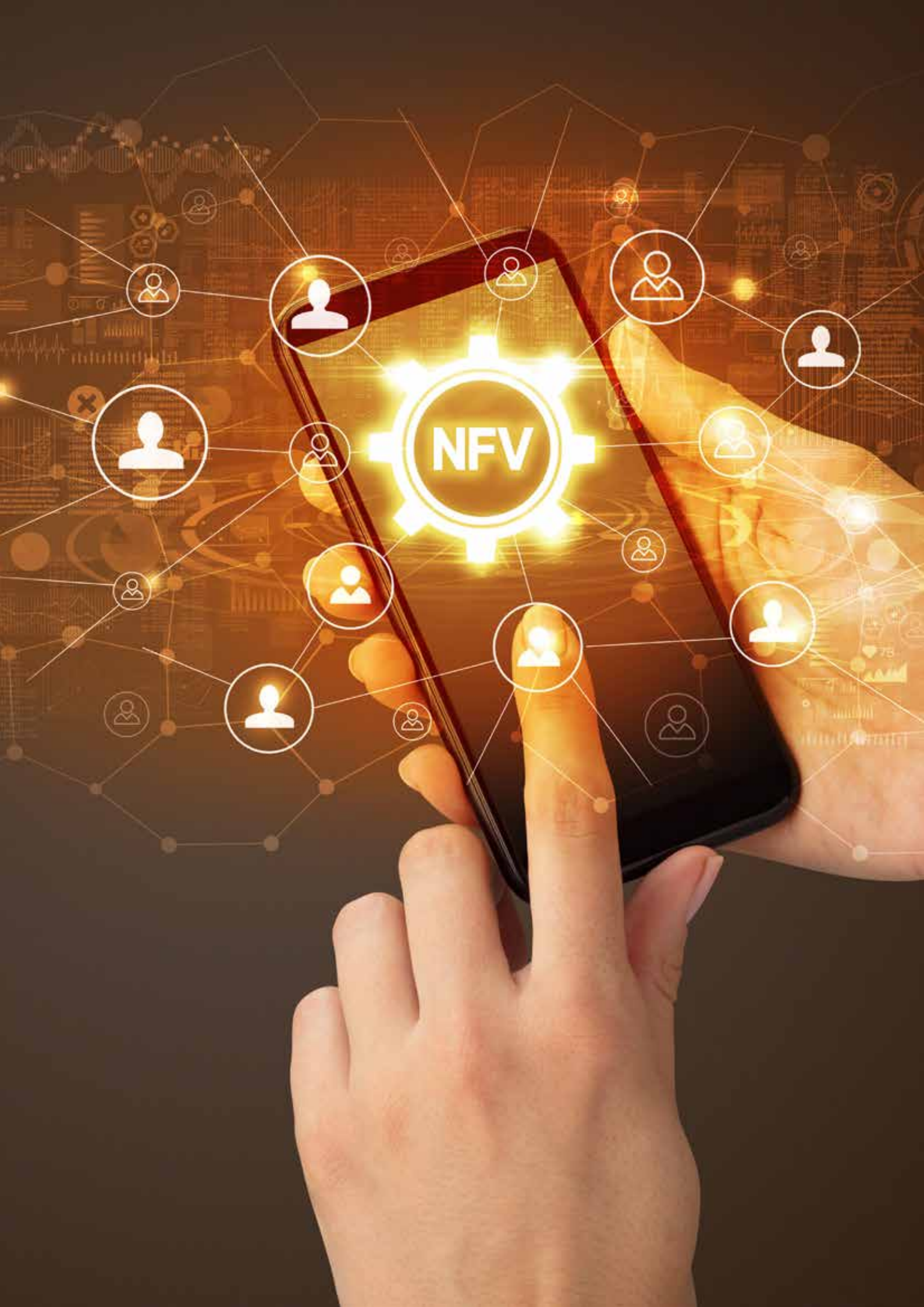
Methodology of mapping use cases and requirements

(This appendix does not form an integral part of this Recommendation.)

In order to improve the effectiveness of this Recommendation and the harmonization with the related ITU-T Recommendations, the same use case driven approach is applied in this Recommendation as described in [ITU-T Y.3501]. A set of use cases had been selected and elaborated, based on these use cases, different categories of requirements may be introduced.

Bibliography

[b-ISO/IEC OVF] ISO/IEC Standard 17203:2011, Information technology -- *Open Virtualization Format (OVF) specification*.


NFV

Cloud computing – Functional architecture of Network as a Service

Recommendation ITU-T Y.3515

(07/2017)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Summary

Recommendation ITU-T Y.3515 provides Network as a Service (NaaS) functional architecture by specifying functionalities and functional components as well as reference points for the operation support system (OSS). This Recommendation also describes the mapping between functionalities and functional requirements of NaaS, relationship between the NaaS functional architecture and software-defined networking (SDN), and illustrated usage of SDN and network functions virtualization (NFV) in support of the NaaS functional architecture.

Keywords

NaaS, NaaS functionality, NaaS functional architecture, NaaS functional component, NaaS product, network as a service.

Table of Contents

1 Scope

This Recommendation provides the Network as a Service (NaaS) functional architecture by specifying functionalities and functional components as well as reference points for the operation support system (OSS).

The scope of this Recommendation consists of:

– Overview of the NaaS functional architecture;

– NaaS functionalities;

– NaaS functional components;

– OSS reference points in the NaaS functional architecture.

This Recommendation also provides appendixes describing:

– The mapping between NaaS functionalities described in this Recommendation and NaaS functional requirements specified in [ITU-T Y.3512];

– The relationship between the NaaS functional architecture and software-defined networking (SDN);

– An illustrated usage of SDN and network functions virtualization (NFV) in support of the NaaS functional architecture.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing*.

[ITU-T Y.2320] Recommendation ITU-T Y.2320 (2015), *Requirements for virtualization of control network entities in next generation network evolution*.

[ITU-T Y.3300] Recommendation ITU-T Y.3300 (2014), *Framework of software-defined networking*.

[ITU-T Y.3302] Recommendation ITU-T Y.3302 (2017), *Functional architecture of software-defined networking (SDN)*.

[ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary*.

[ITU-T Y.3501] Recommendation ITU-T Y.3501 (2016) | ISO/IEC 17789:2014, *Cloud computing – Framework and high-level requirements*.

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), *Information technology – Cloud computing – Reference architecture*.

[ITU-T Y.3512] Recommendation ITU-T Y.3512 (2014), *Cloud computing – Functional requirements of Network as a Service*.

[ITU-T Y.3521] Recommendation ITU-T Y.3521/M.3070 (2016), *Overview of end-to-end cloud computing management*.

[ITU-T Y.3522] Recommendation ITU-T Y.3522 (2016), *End-to-end cloud service lifecycle management requirements*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 activity [ITU-T Y.3502]: A specified pursuit or set of tasks.

3.1.2 cloud computing [ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

3.1.3 cloud service [ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.4 cloud service customer [ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

NOTE – A business relationship does not necessarily imply financial agreements.

3.1.5 cloud service product [ITU-T Y.3502]: A cloud service, allied to the set of business terms under which the cloud service is offered.

NOTE – Business terms can include pricing, rating and service levels.

3.1.6 cloud service provider [ITU-T Y.3500]: Party which makes cloud services available.

3.1.7 Network as a Service (NaaS) [ITU-T Y.3500]: Cloud service category in which the capability provided to the cloud service customer is transport connectivity and related network capabilities.

3.1.8 product catalogue [ITU-T Y.3502]: A listing of all the cloud service products which cloud service providers make available to cloud service customers.

3.1.9 role [ITU-T Y.3502]: A set of activities that serves a common purpose.

3.1.10 service catalogue [ITU-T Y.3502]: A listing of all the cloud services of a particular cloud service provider.

3.1.11 service chain [ITU-T Y.3512]: An ordered set of functions that is used to enforce differentiated traffic handling policies for a traffic flow.

3.1.12 service level agreement [ITU-T Y.3500]: Documented agreement between the service provider and customer that identifies services and service targets.

NOTE 1 – A service level agreement can also be established between the service provider and a supplier, an internal group or a customer acting as a supplier.

NOTE 2 – A service level agreement can be included in a contract or another type of documented agreement.

3.1.13 software-defined networking [ITU-T Y.3300]: A set of techniques that enables to directly program, orchestrate, control and manage network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner.

3.1.14 sub-role [ITU-T Y.3502]: A subset of the activities of a given role.

3.1.15 tenant [ITU-T Y.3500]: One or more cloud service users sharing access to a set of physical and virtual resources.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 NaaS product: A cloud service product for which the cloud service related to that product is of the NaaS cloud service category.

3.2.2 network function: A function of a network infrastructure whose external interfaces and functional behaviour are well specified.

NOTE – Examples of network functions include network switches and network routers.

3.2.3 network service: A collection of network functions with a well specified behaviour.

NOTE – Examples of network services include content delivery networks (CDNs) and IP multimedia subsystem (IMS).

3.2.4 physical network function: A network function implemented via a tightly coupled software and hardware system.

NOTE – Examples of physical network functions include physical network switches and physical routers.

3.2.5 virtualized network function: A network function that can be deployed as a software on a NaaS cloud service provider infrastructure.

NOTE – Examples of virtualized network functions include virtual switches and virtual routers.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
BSS	Business Support System
CCRA	Cloud Computing Reference Architecture
CCS	Cloud Compute and Storage
CDN	Content Delivery Network
CSC	Cloud Service Customer
CSN	Cloud Service Partner
CSP	Cloud Service Provider
DevOps	Development and Operation
DNS	Domain Name System
EMS	Element Management System
ID	Identifier
IMS	IP Multimedia SubsystemIP Internet Protocol
IT	Information Technology
KPI	Key Performance Indicator
L2	Layer 2
L3	Layer 3
MPLS	Multiprotocol Label Switching
NaaS	Network as a Service
NC	Network Connectivity
NF	Network Function
NFV	Network Functions Virtualization
NFVI	Network Functions Virtualization Infrastructure
NMS	Network Management System
NS	Network Service
OSS	Operation Support System
OTN	Optical Transport Network
PNF	Physical Network Function
PoP	Points of Presence
QoE	Quality of Experience

QoS	Quality of Service
SDN	Software-Defined Networking
SLA	Service Level Agreement
vCDN	Virtual Content Delivery Network
vEPC	Virtual Evolved Packet Core
vIMS	Virtual IP Multimedia Subsystem
VM	Virtual Machine
VNF	Virtualized Network Function
VPC	Virtual Private Cloud
VPN	Virtual Private Network
VPNaaS	VPN as a Service
vRouter	Virtual Router
vSwitch	Virtual Switch
VXLAN	Virtual Extensible Local Area Network
WAN	Wide Area Network

5 Conventions

None.

6 Overview of NaaS functional architecture

6.1 Key NaaS characteristics

The NaaS functional architecture aims for a scalable and programmable on-demand network allowing the cloud service customer (CSC) to provision network services (NSs) and resources, as needed, automatically or with minimal interaction with the NaaS cloud service provider (CSP). Key NaaS characteristics to be achieved include:

– **Self-service**: the ability to manage network services automatically or with minimal human interaction. Examples include self-provisioning, self-care and self-design;

– **On-demand**: the ability to deploy and adjust (increase or decrease) network services rapidly and as needed. Examples include fast time-to-market, try before you buy, accelerate innovation, easy migration, update and upgrade;

– **Scalability**: the ability to scale network services and resources (scale out, in, up or down) in response to a large usage demand. Example includes scale-up resources based on traffic growth;

– **Programmability**: the ability to access services features through application programming interfaces (APIs). Examples include programmable quality of service (QoS) and network policy rules;

– **Measured service**: metered delivery of services such that usage can be monitored, controlled, reported, and charged. Example includes case of NaaS CSCs charged only for the services or resources that they use.

6.2 NaaS CSC activities

Activities of the NaaS CSC role are described in clause 8.2 of [ITU-T Y.3502]. These activities are applicable to the case of a NaaS CSC involved in a relationship with a NaaS CSP. Taking the use cloud service activity in CSC-CSP relationship (see Annex A of [ITU-T Y.3502]), Figure 6-1 illustrates the relationships between functional components involved in the use cloud service activity of the CSC:cloud service user sub-role.

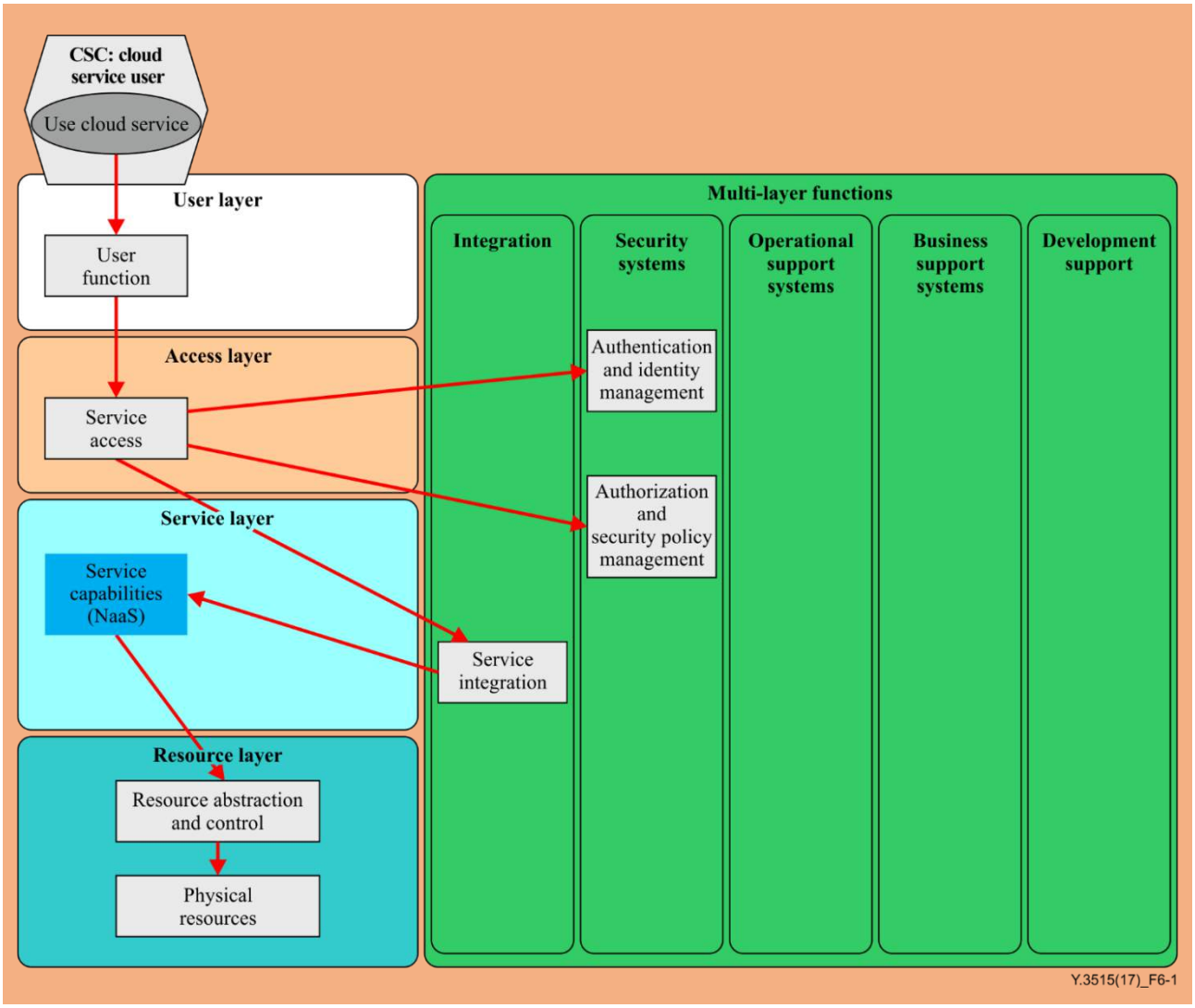


Figure 6-1 – Use of a NaaS service

As for any cloud service, NaaS service capabilities (together with NaaS administration and business capabilities) are positioned in the service layer of the cloud computing layering framework (see clause 9.2 in [ITU-T Y.3502]).

NaaS services are made available to the CSC:cloud service users via an endpoint and interface enabled by the service access functional component. The CSC:cloud service user performs the use cloud service activity through the user function functional component, which then invokes NaaS through the service access functional component. The service access functional component performs any authentication of the CSC:cloud service user and establishes authorization to use particular NaaS service capabilities of NaaS. If authorized, the service access functional component invokes the NaaS service's software implementation which then handles the request.

NaaS services provide self-service capabilities allowing the NaaS CSC to control, manage, monitor and optimize the resources offered as a service by the NaaS CSP in a programmable manner.

Resources offered by the NaaS CSP to the NaaS CSC depend on the type of NaaS service (e.g., NaaS connectivity, NaaS applications as described in [ITU-T Y.3512]) being provided by the NaaS CSP. These resources can be negotiated by the NaaS CSC with the NaaS CSP through the use of the service interface provided by the NaaS CSP. For example, subject of such negotiation can cover connectivity parameters for a NaaS connectivity service provided by the NaaS CSP.

Service requests made by the NaaS CSC via the service interface will trigger interactions with other NaaS CSP's functionalities such as evolved real-time OSS functionalities (see clause 7.7) and NaaS CSP's resource functionalities (e.g., network elements), for example for instantiating network services, network functions, for allocating cloud computing resources and network connectivity resources in NaaS CSP's infrastructure. The service interface can also allow the NaaS CSC to instantiate and operate flexible, scalable and functionally expandable virtualized networks as well as provide unified control and management functionalities to the NaaS CSC for changing, moving, or removing resources associated to such virtualized networks being offered by the NaaS CSP.

6.3 Virtualization of network functions

As described in [ITU-T Y.3512], NaaS services include:

– NaaS application and NaaS platform services such as virtual IP multimedia subsystem (vIMS), virtual evolved packet core (vEPC) and virtual content delivery network (vCDN);

– NaaS connectivity services such as virtual private network (VPN) services and bandwidth on demand.

These NaaS services rely on network services (see clause 3.2.3) and network functions (see clause 3.2.2) provided on-demand by the NaaS CSP to the NaaS CSC. When deployable as software by the NaaS CSP, network functions are known as virtualized network functions (VNFs) (see clause 3.2.5). Examples of such VNFs are virtualized control network entities (see [ITU-T Y.2320]). When implemented via a tightly coupled software and hardware system, network functions are considered as physical network functions (PNFs) (see clause 3.2.4).

Figure 6-2 provides a representation of aspects that need to be controlled and managed by NaaS CSP.

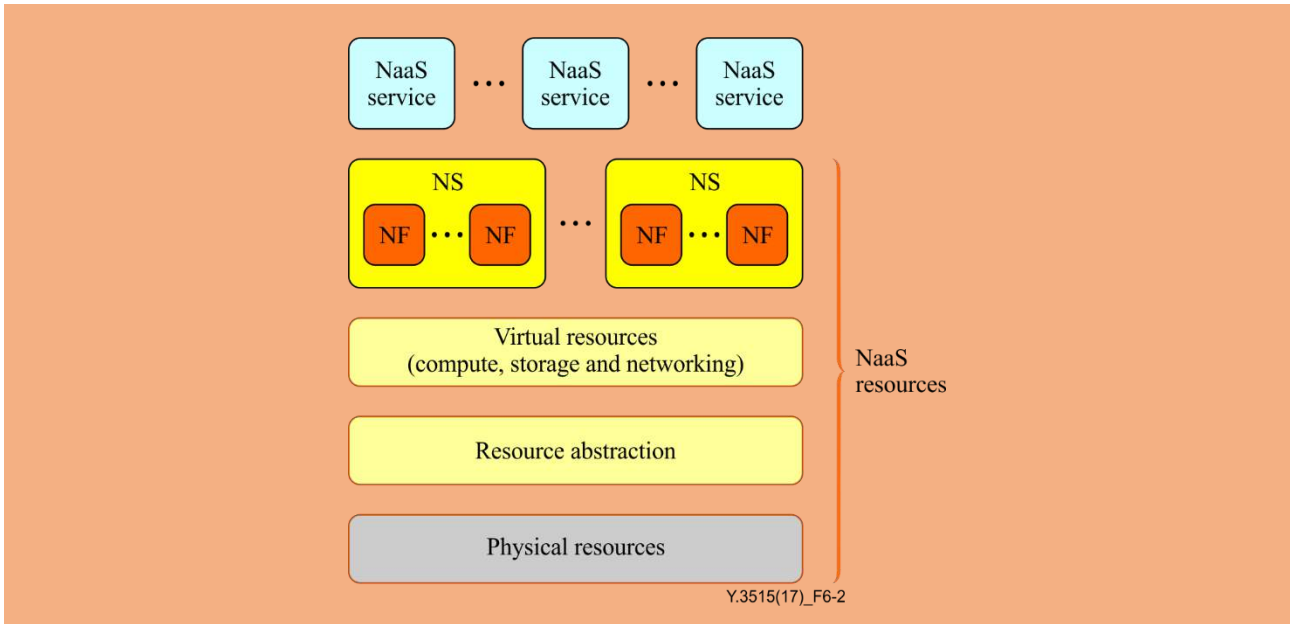


Figure 6-2 – Aspects managed by NaaS CSP

NaaS services offered to NaaS CSCs are based on NSs and network functions (NFs) that need to be managed by the NaaS CSP. Although not illustrated in Figure 6-2, connectivity between NFs needs also to be managed by the NaaS CSP, including connectivity between NFs in a given NS and connectivity between different NSs.

Other aspects to be managed by the NaaS CSP include physical (hardware) resources (compute, storage and networking resources), resource abstraction and virtual resources. The main functions of resource abstraction are:

– abstraction of physical resources allowing decoupling of NFs from underlying physical resources;
– allocation of virtual resources from physical resources;
– provision of virtual resources (virtual compute, virtual storage) for execution of NFs as well as virtualized network connectivity resources for interconnecting NFs of a given NS or for interconnecting multiple NSs.

7 Functionalities for NaaS

This clause aims to provide the functionalities which are derived from the functional requirements specified in [ITU-T Y.3512]. The mapping between NaaS service functional requirements and the functionalities described in this clause is presented in Appendix I.

7.1 NaaS business related functionalities

Business related functionalities in the NaaS architecture are mainly related to the interaction between the NaaS CSC and NaaS CSP regarding NaaS products offered by the NaaS CSP. This includes NaaS CSP functionalities related to the selection and purchasing of specific NaaS products from a product catalogue by the NaaS CSC and all other business related aspects, such as billing. An instance of a NaaS product represents the subscription to a NaaS product by a given NaaS CSC.

NaaS business related functionalities cover cloud customer management and cloud product management functionalities supported by the NaaS CSP as per [ITU-T Y.3521] where the cloud customer is a NaaS CSC and the cloud product is a NaaS product. These functionalities include NaaS CSP's functionalities concerned with the lifecycle of NaaS products offered to and purchased by NaaS CSCs, i.e., functionalities related to NaaS products' order management, performance management, usage statistics, as well as the management of NaaS product instances delivered to NaaS CSCs. More details about lifecycle management of cloud products and services can be found in [ITU-T Y.3522].

7.2 Functionalities for NaaS service instantiation

7.2.1 Description of NaaS service instantiation

These functionalities are responsible for the instantiation of a NaaS service following the receipt of a valid NaaS product (and associated NaaS services) order request from a NaaS CSC (e.g., a request for a vCDN service or VPNaaS service). NaaS service instantiation functionalities maps the validated NaaS CSC request to specific NaaS service deployment policies. For the requested NaaS service instance, the NaaS service functionalities requests to the NaaS service orchestration functionalities (see clause 7.3) to realise the corresponding automatic configuration of required NaaS resources (including network services, network functions and resources) in the different infrastructure domains of the NaaS CSP (e.g., in access transport domain, core transport domain and virtualization infrastructure domain) in a programmable manner.

NaaS service instantiation results in the instantiation of NaaS functional components (i.e., NaaS service capabilities and NaaS administration capabilities components) in the service layer [ITU-T Y.3502] of the NaaS CSP. For example, in the case of a VPNaaS service being instantiated, dedicated VPNaaS capabilities functional components will be instantiated in the service layer. These VPNaaS service and administration capabilities provided by the service layer will allow the NaaS CSC to request for management and configuration changes of a VPN instance to the NaaS CSP and also enable the NaaS CSC to request dynamic VPN network reconfiguration.

7.2.2 Modelling for NaaS service instantiation

As part of NaaS service instantiation functionality, a global, coherent and abstract view and representation of NaaS resources (including network resources, network services, network functions and network operational policies) used during the lifetime of the NaaS service instance will be provided and presented to

the NaaS CSC. This representation avoids the direct communication and interaction between the NaaS CSC and these NaaS resources (e.g., network elements of the NaaS CSP infrastructure) and masks implementation specific aspects of NaaS resources used in the context of the NaaS service instance. This abstract view presented to the NaaS CSC also allows real-time configuration change demands from the NaaS CSC to be reflected by the NaaS CSP on its own resources. Therefore, a hierarchical and extensible framework, which can be realised by a set of information models, needs to be designed to hide the protocol specific and/or vendor specific details of the resources being used by the NaaS CSP. The modelled objects being part of these NaaS information models can be grouped as NaaS resource model, NaaS service model, and NaaS service operational policy model.

NaaS resource models reflect in an abstract manner NaaS CSP's resources including their associated topological view across different layers (e.g., layer 2 (L2) and layer 3 (L3)). NaaS resource models designed by the NaaS CSP or cloud service partners (CSNs) (e.g., service developer) are used by the NaaS CSP to represent NaaS CSP's resources at a conceptual level, including physical and/or virtualized network functions as well as connectivity links. NaaS resource models are not exposed to the NaaS CSC.

A NaaS service model is service specific, i.e., specific to the NaaS service being offered to the NaaS CSC by the NaaS CSP but rely on underlying NaaS resource models. Once a NaaS service is instantiated for a NaaS CSC, the corresponding NaaS service model designed by the NaaS CSP is exposed to the NaaS CSC.

A NaaS service operational policy model is service specific, i.e., are specific to the NaaS service being offered to the NaaS CSC. This model defines NaaS CSP-wide policies applicable for the corresponding NaaS service and is designed by the NaaS CSP or CSN (e.g., service developer). During the instantiation of a NaaS service, the NaaS service operational policy model is combined with the NaaS service model and mapped into a target configuration of NaaS CSP's resources (e.g., network elements), according to NaaS resource models.

NOTE – The usage example of modelling is provided in Appendix II.

7.3 Functionalities for NaaS service orchestration

The NaaS service orchestration functionalities are responsible for cross-domain service orchestration within the NaaS CSP, e.g., for a NaaS connectivity service, the functionality will be capable to orchestrate NaaS resources (including network services, network functions and resources) in multiple NaaS CSP domains (including legacy domains and virtualized network domains).

Upon receipt of a NaaS service request from the NaaS CSC, these functionalities are responsible for decomposing, as necessary, the request into several independent requests and for distributing each of the resulting requests to the relevant control functions of the NaaS CSP. An example of a composite NaaS service is a service chain path, i.e., an ordered list of connection points forming a chain of network functions (PNFs and/or VNFs), along with policies associated to the list.

The NaaS service orchestration functionalities interact with the NaaS service instantiation functionalities to address NaaS service decomposition and configuration of requests received from NaaS service instantiation functionalities (see clause 7.2.1).

In case of a non-composite NaaS service request received from the NaaS CSC, the NaaS service orchestration functionalities can transfer this request to the relevant domain control function.

The NaaS orchestration functionalities are also responsible for ensuring that NaaS resources (e.g., NSs, NFs, connectivity) are appropriately instantiated throughout the different NaaS CSP domains (e.g., across one or network domains that can be using different networking connectivity technologies).

7.4 Functionalities for network analytics

Functionalities for network analytics are responsible for data collection from the NaaS CSP's network environment (such as network jitter, delay, packet loss rate, round-trip time, domain name system (DNS) resolution time) and events listening to continuously monitor NaaS services during their lifecycle. These functionalities help to provide customized analytical network applications and provide the analysed results to the related functional components (such as resource abstraction and control) for further action, including healing the service, appropriately scale up or scale down the service, dynamically adjust routing, etc.

The analytical network applications are used to match specific conditions based on the analytical results. Once a condition is matched, the application can activate the pre-defined event and the further actions will depend on the specific policies associated with this condition.

These functionalities can be achieved along with other related functionalities, such as NaaS service instantiation, NaaS service orchestration, resource abstraction and control, and evolved real-time OSS, and can help to complete the whole NaaS service lifecycle management in an iterative way. More details on the lifecycle management of cloud services can be found in [ITU-T Y.3522].

7.5 Autonomic functionalities

Autonomic functionalities in the NaaS architecture are responsible for making decisions on their own, using high-level policies. They constantly check and optimize their status automatically and adapt themselves to changing conditions.

From an operational point of view, closed control loops driven through autonomic functionalities can be included at resource level (PNFs, VNFs) as well as in the different OSS functionalities described in clause 7.8. Typically, a closed loop control is comprised of functionalities for collecting and monitoring data from the system being managed, analysing (through filtering, correlation and other mechanisms), planning (different actions based on inferring trends, finding causes of the problem) and executing the decided plan(s). Autonomic functionalities can therefore involve and rely on the use of network analytics functionalities (see clause 7.4). Policies can be used with control loops to guide their operation (see clause 7.6 regarding policy related functionalities).

7.6 Policy related functionalities

Policy related functionalities in the NaaS architecture play an important role in realizing lifecycle management (refer to different OSS functionalities, see clause 7.8), network operational policy modelling (refer to NaaS service instantiation functionalities, see clause 7.2) as well as closed loop automation (refer to autonomic functionalities, see clause 7.5) and network analytics functionalities (see clause 7.4). The main goal of policy functionalities is to control in a simple manner the behaviour of the NaaS CSP system using configurable policies and rules.

Policy related functionalities include:

– Policy creation: used to design and validate policies rules, identify and resolve overlaps and conflicts between policies. A policy can be of a high-level nature to create a condition, requirement or constraint that must be provided, maintained, and enforced. A policy may also be defined at a lower level, such as a machine-readable rule or software condition. Policies can be created in conjunction with NaaS services (refer to development functionalities in clause 7.9 or independently from NaaS services (e.g., policies unrelated to NaaS services such as NaaS CSP internal security policies).

– Policy distribution: after being created, policies available in repositories are distributed to the right policy-enabled components in the NaaS architecture;

– Policy decision and enforcement: at runtime, policies that were previously distributed to policy-enabled NaaS components will be used by those components to control or influence their functionality and behaviour, including any decisions and actions that have to be taken.

7.7 NaaS resource functionalities

The NaaS resource functionalities include the functionalities necessary for the support of NaaS services. This include functionalities such as network services, network functions, as well as the resources used in underlying cloud computing infrastructures and network infrastructures (see clause 6.3 for further description of NaaS resources). For example, these NaaS resource functionalities can be used to provide virtualized networks exposed by the service layer to the NaaS CSC.

NaaS resource functionalities include network connectivity functionalities used in the different NaaS CSP domains. Network connectivity functionalities include interworking functionalities between the different

networking layers used by the NaaS CSP, covering interworking of the relevant control functionalities, forwarding functionalities as well as management functionalities for each of these networking layers.

7.7.1 Functionalities for mapping between physical resources and virtualized networks

As part of NaaS resource functionalities, these functionalities are responsible to support the mapping between underlying physical resources and virtualized networks exposed to the NaaS CSC as part of NaaS services, via which, the near real-time utilization of underlying physical resources (physical nodes, physical links, etc) can be obtained.

7.8 Functionalities for an evolved real-time OSS

The OSS functionalities for NaaS consist of a set of capabilities for accessing the relevant OSS functions related to NaaS. They are related to functional components of the operations support systems defined in the multi-layer functions. These functions span the layered framework of the cloud computing reference architecture (CCRA).

As presented in clause 6.3, aspects to be controlled and managed in real-time by the OSS include the following:

- NaaS services;
- network services (see definition in clause 3.2.3);
- network functions (see definition in clause 3.2.2);
- virtual cloud compute and storage (CCS) resources;
- virtualized network connectivity;
- physical resources (compute, storage, networking).

Figure 7-1 describes the organization of the OSS functionalities to fulfil the management of the above aspects.

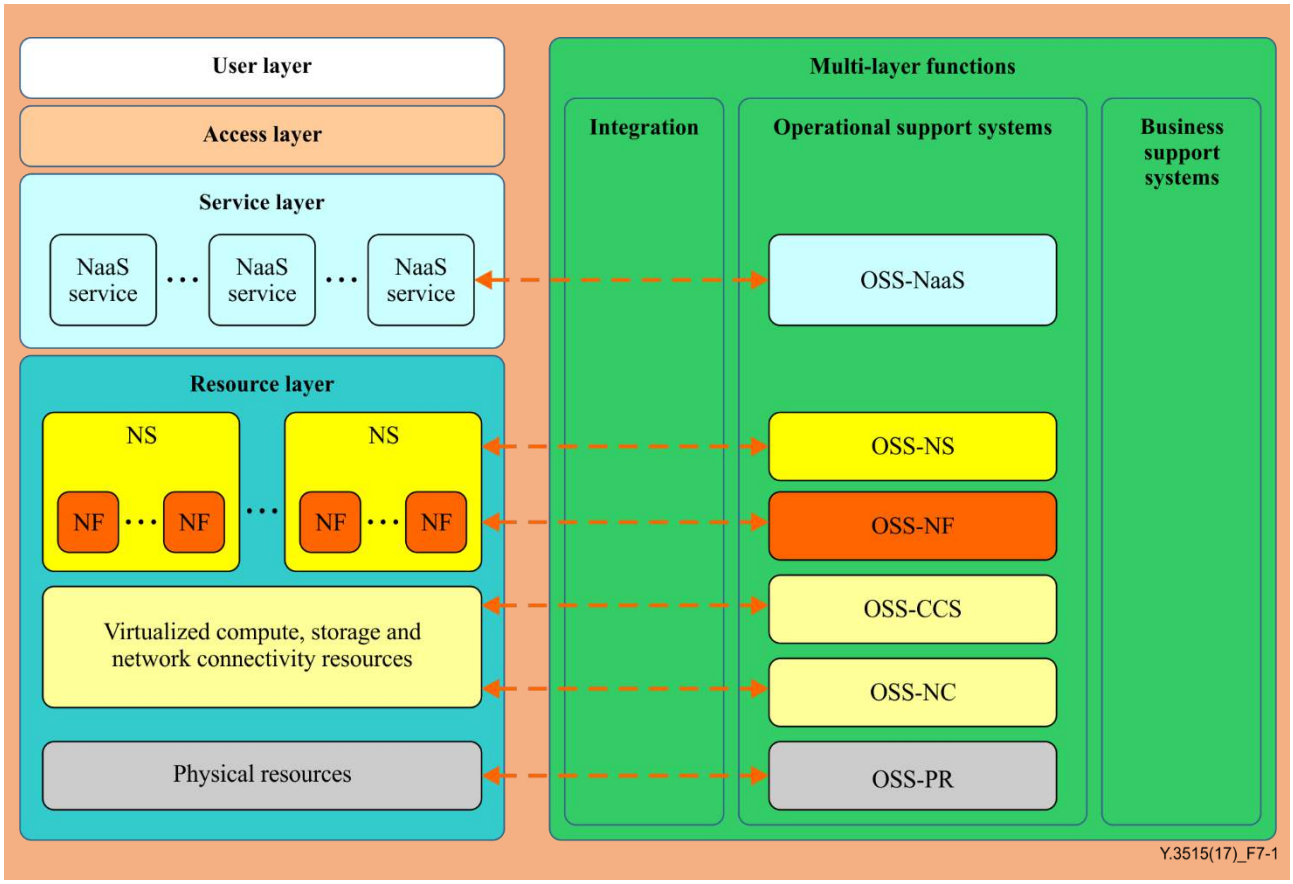


Figure 7-1 – OSS functionalities for NaaS

From the perspective of the management layers described in [ITU-T Y.3521], the OSS functionalities described in this clause cover the service management layer and resource management layer aspects (see Figure 8-3 of [ITU-T Y.3521]). The service management layer takes care of the management of NaaS services offered to NaaS CSCs, i.e., OSS-NaaS services functionalities described in clause 7.8.1. Regarding resource management layer aspects, they cover the management of the different NaaS resources (see clause 6.3) that are involved in the support of NaaS services, i.e., network services, network functions, cloud compute and storage resources, network connectivity resources and physical resources. These management functionalities are described in more detail in clause 7.8.2.

7.8.1 Service management layer functionalities

The OSS-NaaS services (OSS-NaaS) functionalities are responsible for the management of NaaS services (covering their deployment and operation), i.e., including service fulfilment, service assurance and service repositories [ITU-T Y.3521].

In accordance with clause 10.3 of [ITU-T Y.3521], these functionalities include:

– Catalogue management of NaaS services (e.g., connectivity as a service, network function as a service, network service as a service), with their relevant descriptions in terms of required network functions and their interconnectivity;

– NaaS service order management functionalities including NaaS service order orchestration and distribution decomposing the NaaS service order into resource order requests towards the relevant OSS functionalities described in clause 7.8.2;

– NaaS service assurance functionalities such as performance management, problem management and quality management of NaaS services instances;

– Inventory management of NaaS services instances;

– Usage management of NaaS services instances.

7.8.2 Resource management layer functionalities

This clause describes the resource management layer functionalities (see clause 10.4 of [ITU-T Y.3521]) for the support of NaaS services. These functionalities cover the management functionalities related to NaaS resources, i.e., network services, network functions, cloud compute and storage resources, network connectivity resources and physical resources.

7.8.2.1 OSS-network services

The OSS-network services (OSS-NS) functionalities are responsible for the management (including the deployment and operation) of network services.

In accordance with clause 10.4 of [ITU-T Y.3521], these functionalities include:

– Catalogue management of network services with their relevant descriptions in terms of required network functions and their interconnectivity;

– Network services' order management functionalities including the automated creation, modification and termination of network services instances (following NaaS service order requests received from OSS-NaaS);

– Network services' assurance functions such as performance monitoring, fault management of network services' instances; These functions include monitoring of network services' instances, calculating and performing restoration activities when monitoring detects one or more faulty network service instances as well as reporting status of network services' instances to clients of OSS-NS, e.g., OSS-NaaS functionalities;

– Inventory management of network services' instances (including availability and performance of network services' instances and the resources used to support the network services' instances);

– Usage collection and distribution of network services' instances.

The OSS-NS will handle the management of network service chains including the automated deployment, policy management and profile management of network service chains. By routing traffic flows according to a 'service graph', service chains address the requirement for optimization of the network through the provisioning of network services that are tailored to the customer context.

7.8.2.2 OSS-network functions

The OSS-network functions (OSS-NF) functionalities are responsible for the management of network functions such as instantiation, update, query, scaling, and termination of network functions. The services provided by the OSS-NF can be consumed by other functionalities such as the OSS-NS (see clause 7.8.2.1).

In accordance with clause 10.4 of [ITU-T Y.3521], the OSS-NF include functionalities such as:

– Catalogue management of network functions with their relevant descriptions and software;
– Network functions' order management functionalities including the automated creation, modification and termination of network functions' instances (including instances of network functions' components and their inter-connectivity);
– Network functions' assurance functions such as performance management and, fault management of network functions instances; These functions include monitoring of network functions' instances, calculating and performing restoration activities when monitoring detects one or more faulty network functions' instances as well as reporting status of network functions' instances to clients of OSS-NF, e.g., OSS-NS functionalities;
– Inventory management of network functions instances;
– Usage collection and distribution of network functions instances.

7.8.2.3 OSS-cloud compute and storage

The OSS-cloud compute and storage (OSS-CCS) functionalities are responsible for the management of virtual compute and storage resources. The functionalities provided by the OSS-CCS can be used by other OSS functionalities such as the OSS-NS (see clause 7.8.2.1) or the OSS-NF (see clause 7.8.2.2).

In accordance with clause 10.4 of [ITU-T Y.3521], the OSS-CCS includes functionalities such as:

– Catalogue management of cloud compute and storage resources;
– Resource order management functionalities such as the allocation, modification and termination of virtual compute and storage resources;
– Resource assurance functions such as performance management and fault management of allocated virtual compute and storage resources;
– Inventory management of allocated virtual compute and storage resources;
– Usage collection and distribution of virtual compute and storage resources.

7.8.2.4 OSS-network connectivity

The OSS-network connectivity (OSS-NC) functionalities are responsible for the management of network connectivity resources. The OSS-NC functionalities can be used by other OSS functionalities such as the OSS-NS (see clause 7.8.2.1) the OSS-NF (see clause 7.8.2.2) or the OSS-CCS (see clause 7.8.2.3).

In accordance with clause 10.4 of [ITU-T Y.3521], the OSS-NC includes functionalities such as:

– Resource order management functionalities such as allocation, modification and termination of virtualized network connectivity resources such as virtualized networks, links, sub-networks;
– Resource assurance functionalities such as performance management and fault management of allocated virtualized network connectivity resources;
– Inventory management of allocated virtualized network connectivity resources;
– Usage management of virtualized network connectivity resources.

The OSS-NC functionalities can be consumed by other NaaS functionalities such as OSS-NS (see clause 7.8.2.1) or OSS-NaaS functionalities (see clause 7.8.1). Control plane functions are topology and device detection,

virtual partitioning, traffic isolation, reachability, traffic engineering and path computation, flow management, failure detection, path convergence, QoS control and management, as well as policy control and management. The configuration of virtualized networks requires interfaces to all relevant components, including network elements (physical switches and physical routers) in the infrastructure network domains, virtual switches (vSwitchs) as well as virtual routers (vRouters) in hypervisors, and embedded switches as well as routers in computing platforms.

The OSS-NC functionalities are basically responsible to manage network connectivity in a given infrastructure network domain (e.g., access, core). This functionality provides on-demand network service through northbound interfaces to the higher layer functions, abstracts the various southbound interfaces, and invokes the underlying infrastructure network interfaces. Several OSS-NC functionalities may exist in a given NaaS CSP each responsible for a particular network domain with overall end-to-end network connectivity through multiple network domains being handled by e.g., the functionalities for NaaS service orchestration (see clause 7.3) and/or OSS-NaaS functionalities (see clause 7.8.1).

7.8.2.5 OSS-physical resources

The OSS-physical resources (OSS-PR) are functionalities responsible for the management of physical resources such as compute, storage and networking physical resources. The functionalities provided by the OSS-PR can be used by other OSS functionalities such as the OSS-CCS (see clause 7.8.2.3) or the OSS-NC (see clause 7.8.2.4).

Functionalities provided by the OSS-PR include:

– Catalogue management of physical resources (compute, storage, networking);

– Resource order management of physical resources;

– Resource assurance functionalities such as performance management and fault management of physical resources;

– Inventory management of available physical resources.

7.9 Functionalities for the development of NaaS products and NaaS services

Development functionalities for NaaS enable the design, building and testing of NaaS products, NaaS services (offered by NaaS products) as well as the design, building and testing of resources including NSs and NFs that are used for the support of the designed NaaS services. The design of NaaS products, NaaS services and NaaS resources is realized using model-driven engineering techniques providing the ability to create and manage NaaS products, NaaS services and NaaS resources in terms of models (refer to NaaS service models, NaaS resource models, NaaS service operational policy models as described in clause 7.2.2).

Once designed, built and tested, the resulting models for NaaS products, respectively for NaaS services, will be made available in the product catalogue, respectively service catalogue, by the NaaS CSP. Similarly network service models and network function models will also made available in NaaS resource catalogues for further instantiation as needed by the relevant OSS functionalities.

Development functionalities for NFs allow for the design and build of NFs according to the following cases:

- Features and capability required by the NFs are provided by elementary NFs;
- Composite NF provided by mixing NFs.

Development functionalities for NSs allow for the design and build of NSs taking into account the following cases:

- NS that includes NFs and/or composite NFs;
- Composite NS provided by mixing NSs.

According to [ITU-T Y.3502], the design includes the creation of configuration metadata relating to NaaS services, NFs and NSs being developed and also supports the creation of scripts and related artefacts that are then used by the provider's operational support systems to provision and configure the NaaS services, NFs or NSs.

In addition, the development functionalities include the building of generated and ready-to-deploy software packages for NaaS services, NFs and NSs which can be then passed on-boarded for deployment in a cloud infrastructure. The software package consists of both the implementation software and also the configuration metadata and scripts.

8 Functional components

This clause presents NaaS functional components definition and description based on NaaS functionalities identified in clause 7. NaaS functional components include instantiated functional components defined in [ITU-T Y.3502] and functional components defined in this Recommendation.

The functional components in a functional architecture represent sets of functions that are required to perform the cloud computing activities for various roles and sub-roles involved in cloud computing. The functional architecture of NaaS complies with CCRA [ITU-T Y.3502], where dependencies between functions are defined in the functional architecture.

8.1 Business support system functional components for NaaS products

The functional components for NaaS products (BSS-NaaS products) are shown in Figure 8-1.

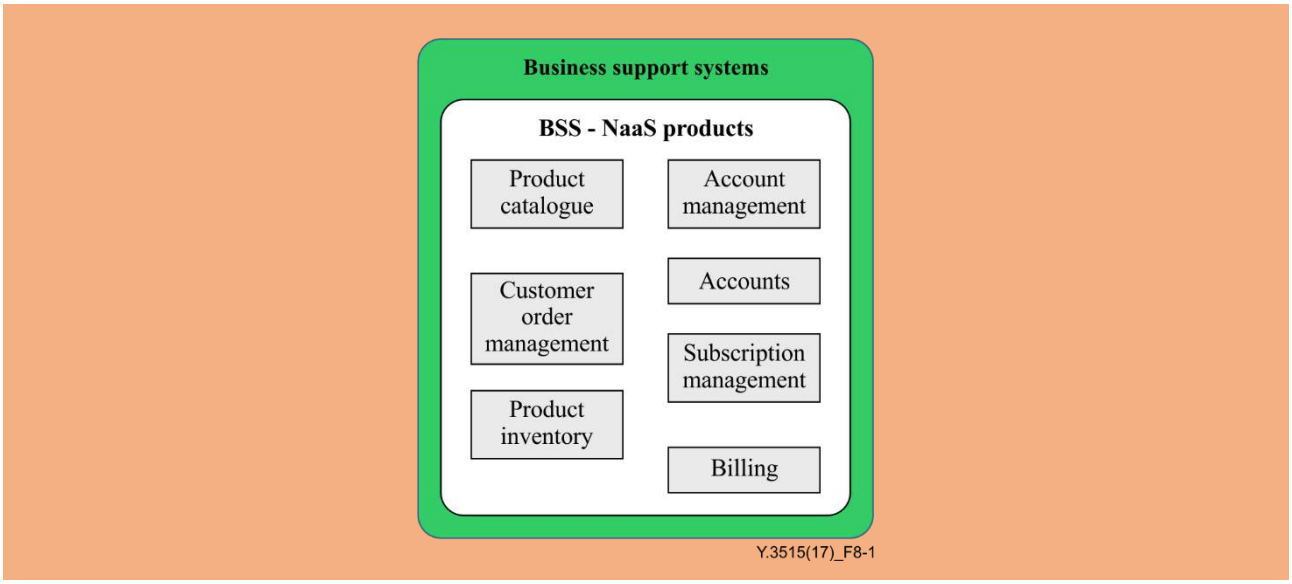


Figure 8-1 – Functional components for BSS-NaaS products

Functional components for BSS-NaaS products include the business support system (BSS) functional components described in clause 9.2.5.4 of [ITU-T Y.3502], i.e., product catalogue functional component, account management functional component, subscription functional component, billing functional component and accounts functional component.

These components are used to support NaaS business related functionalities of the NaaS CSP as described in clause 7.1. In particular:

– The product catalogue functional component provides capabilities for NaaS CSCs to browse the list of available NaaS service offerings which they can purchase, plus a set of capabilities for the management of the content of the catalogue which are available to the staff of the NaaS CSP. Product catalogue entries consist of technical information about each of the NaaS service offerings (capabilities provided by the NaaS service, interface definitions for the NaaS service), plus related business information such as pricing or rating;

– The subscription management functional component handles subscriptions from NaaS CSCs to particular NaaS services, aiming to record new or changed subscription information from the NaaS CSC and ensure the delivery of the subscribed NaaS service(s) to the NaaS CSC;

– Billing functional component. The billing functional component has capabilities for the metering and rating of the use of NaaS services by NaaS CSCs and the generation of invoices based on the charges for the use of NaaS services created by the metering and rating function, and the transmission of the invoices to the NaaS CSCs.

In addition to BSS components defined in [ITU-T Y.3502], the following functional components are added (see Figure 8-1):

– The customer order management functional component is responsible of the lifecycle management of a NaaS CSCs' requests for NaaS products (and NaaS services offered by these NaaS products). This includes customer order establishment (step guiding, data collection and validation), customer order orchestration and overall customer order lifecycle management (see [ITU-T Y.3521] and [ITU-T Y.3522]). Orders from NaaS CSCs may be for new NaaS products and NaaS services, or may be for updating or terminating of an existing NaaS service;

– The product inventory functional component holds information of NaaS products' instances ordered by NaaS CSCs. This information is updated during the lifecycle of the NaaS products instances, reflecting changes resulting from execution of management operations on these NaaS product instances.

8.2 Service layer functional components for NaaS

Figure 8-2 shows the service layer functional components used for NaaS services instantiation and also when a NaaS service is instantiated by the NaaS CSP.

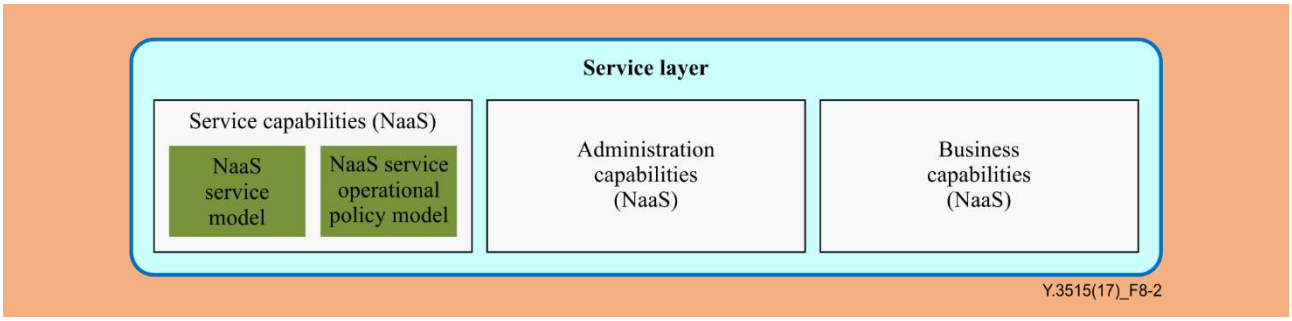


Figure 8-2 – Service layer functional components for NaaS

8.2.1 Business capabilities (NaaS)

The business capabilities (NaaS) functional component provides a set of capabilities for accessing the NaaS business related functionalities (see clause 7.1) related to the provision of NaaS services. The business functionalities are contained within the business support systems (BSS) functional components (see clause 8.1).

In particular, the business capabilities (NaaS) functional component provide access means for the NaaS CSC to select and purchase a NaaS product (and associated NaaS services with associated NaaS service models and NaaS service operational policy models) available in the product catalogue functional component (see clause 8.1). Once validated by the NaaS CSP, the requested NaaS service is instantiated by the NaaS CSP, i.e., a corresponding service capabilities (NaaS) functional component is made available in the service layer allowing for further NaaS service interactions between the NaaS CSC and the NaaS CSP. If not already instantiated an administration capabilities (NaaS) functional component is also made available in the service layer allowing for NaaS service-related management interactions between the NaaS CSC and the NaaS CSP.

Interactions through the business capabilities (NaaS) functional component also allow for the NaaS CSC to access the billing information related to the usage of instantiated NaaS services. Using BSS and OSS functional components, the NaaS CSP collects relevant usage measurements and usage events in order to generate and provide a bill to the NaaS CSC.

8.2.2 Administration capabilities (NaaS)

The administration capabilities (NaaS) functional component provides a set of capabilities for accessing the OSS-NaaS functionalities (see clause 7.8.1) related to the management of instantiated NaaS services. This includes functionalities contained within the OSS-NaaS functional components. For example, the administration capabilities (NaaS) functional component allows the NaaS CSC to view performance and fault information related to instantiated NaaS services. The NaaS CSP will collect information requested by the NaaS CSC and make it available through reporting to the NaaS CSC via the administration capabilities (NaaS) functional component.

8.2.3 Service capabilities (NaaS)

The service capabilities (NaaS) functional component consists of the necessary software required to implement the NaaS service offered to the NaaS CSC and implements the functionality defined by the NaaS service interface, i.e., the interface offered to the NaaS CSC, independent of the service implementation.

As shown in Figure 8-2, the service capabilities (NaaS) functional component provides capabilities exposed to the NaaS CSC according to the NaaS service model and NaaS service operational policy model selected by the NaaS CSC through business level interactions with the NaaS CSP. Refer to clause 8.3.1 for the description of these two NaaS-related service models.

Using the NaaS service exposed API provided by the service capabilities (NaaS) functional component, the NaaS CSC can trigger NaaS service specific on-demand behaviours (made possible by the NaaS CSP according to the selected NaaS service model). These on-demand requests are validated by the NaaS CSP according to the NaaS service specific policies that govern such on-demand behaviour. The on-demand behaviours (and associated constraints) are defined in the NaaS service operational policy model selected by the NaaS CSC at NaaS instantiation time. For example, a NaaS service operational policy model may describe the range of bandwidth in which the NaaS CSC is permitted to send traffic to the NaaS CSP or the range of computing resources that a specific NF instance is allowed to be allocated in the NaaS CSP infrastructure.

8.3 OSS functional components

The OSSs functional components encompass the set of operational-related management capabilities of the NaaS functional architecture in order to manage and control aspects from NaaS services down to the NaaS CSP infrastructure resources including cloud compute and storage, network connectivity and physical resources.

The OSS components described in this clause are intended to support the functionalities for an evolved real-time OSS described in clause 7.8. The description of OSS components follows the structure of the OSS as shown in Figure 7-1.

Annex A describes reference points related to OSS functional components.

8.3.1 OSS-NaaS functional components

The OSS-NaaS functional components encompass the set of operational-related management functionalities that are required in order to manage and control NaaS services offered to customers (refer to clause 7.8.1).

NOTE – These functional components are not meant to be specific to NaaS and are applicable to other cloud service categories provided by NaaS CSPs.

Figure 8-3 shows the OSS-NaaS functional components.

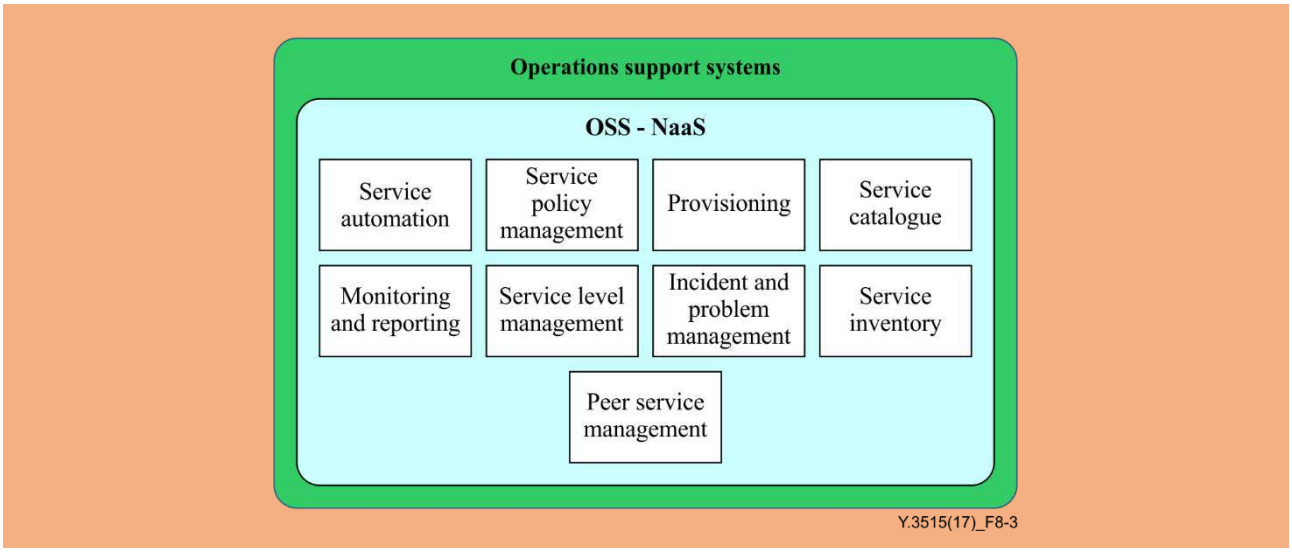


Figure 8-3 – OSS-NaaS functional components

The OSS-NaaS functional components include the following OSS functional components:

1) Service catalogue functional component (see clause 9.2.5.3 of [ITU-T Y.3502]). This component includes a listing of all cloud services of NaaS CSPs including the relevant NaaS services;

   Modelling is needed for ensuring an efficient control and management of the NaaS services, policies, and resources by the NaaS CSP. The following models used for NaaS service instantiation (see clause 7.2.2) are needed in the service catalogue:

   – NaaS service models

     A NaaS service model provides the information model of a given NaaS service (e.g., VPN as a service (VPNaaS)) being offered by the NaaS CSP. NaaS service models are used for creating and deploying NaaS service solutions by the NaaS CSP. In a NaaS service model, a NaaS service specification is needed which includes the various interfaces related to the operations offered by a NaaS service. The NaaS service model is used when instantiating the corresponding NaaS service. For example, in case of a VPN service instance the different service attributes used to model a VPN service, such as tenant ID, VPN site IDs, VPN type and access bandwidth are part of the NaaS service model and will be subsequently used by the NaaS CSC when triggering VPN-related service requests.

   – NaaS service operational policy models

     A NaaS service operational policy model provides the information model related to network operational policies for a given NaaS service. The operational policies can be created at different levels of abstraction and can represent different types of policy rules for controlling NaaS resources managed by the NaaS CSP. The operational policies are used to control the configuration changes of NaaS resources (e.g., network elements).

     For a given NaaS service, the corresponding NaaS service model and NaaS service operational policy model always work together although loosely bound to each other. The creation, deletion, and any major state changes of a specific NaaS service instance (instantiated based on the corresponding NaaS service model selected by the NaaS CSC) usually trigger the execution of one specific NaaS service operational policy model, which is used together with the NaaS service model during the whole lifecycle of the NaaS service.

   – NaaS resource models

     A NaaS resource model reflects, in an abstract manner, NaaS CSP's resources including their associated topological view across different layers. A NaaS resource model reflects the attributes and operational parameters of given NaaS resources (e.g., NS, NF, virtualized

resources, physical resources) described by the model. A NaaS resource model provides the information model of NaaS resources, e.g., the topology attributes of a physical and virtualized network such as bandwidth or latency of corresponding links, and the operational parameters needed to support the deployment of these NaaS resources.

2) Provisioning functional component (see clause 9.2.5.3 of [ITU-T Y.3502]). This component provides the capabilities for provisioning NaaS services;

3) Monitoring and reporting functional component (see clause 9.2.5.3 of [ITU-T Y.3502]). This component provides the capabilities for monitoring services including NaaS services provided by the NaaS CSP;

4) Service policy management functional component (see clause 9.2.5.3 of [ITU-T Y.3502]). The service policy management functional component provides capabilities to define, store and retrieve policies that apply to cloud services including NaaS services;

5) Service automation functional component (see clause 9.2.5.3 of [ITU-T Y.3502]). The service automation functional component provides capabilities for service delivery including the management and execution of service templates and the orchestration of services, which include NaaS services. The service automation functional component realizes the NaaS service orchestration functionalities described in clause 7.3.

   In order to realize the functionalities for NaaS service orchestration, a unified abstract modelling of NaaS services provided to the NaaS CSC by the service layer is a must. With such modelling being defined, the NaaS service automation functional component when receiving a composite NaaS service request from the NaaS CSC will be able to decompose the request into several independent NaaS resources order requests and distribute each of these independent requests to the appropriate control or OSS functionalities of the NaaS CSP specific domains, automatically. The OSS-NaaS service automation functional component provides coordination, aggregation and composition of multiple services in order to deliver NaaS services.

   The OSS-NaaS service automation functional component provides service orchestration according to the NaaS service model and NaaS service operational policy model. The service automation functional component handles NaaS service requests received from the NaaS CSC and decomposes these NaaS service requests according to the NaaS service models and policy models, respectively.

6) Service level management functional component (see clause 9.2.5.3 of [ITU-T Y.3502]). The service level management functional component provides capabilities for managing the service levels of a particular cloud service, aiming to ensure that the cloud service meets the requirements of the service level agreement (SLA) which applies to the service. This includes service level management of NaaS services;

7) Incident and problem management functional component (see clause 9.2.5.3 of [ITU-T Y.3502]). The incident and problem management functional component provides capabilities for the capture of incident or problem reports and managing those reports through to resolution. Incidents and problems can be detected and reported by the NaaS CSP's systems, or they can be detected and reported by NaaS CSCs;

8) Peer service management functional component (see clause 9.2.5.3 of [ITU-T Y.3502]). The peer service management functional component provides capabilities for connecting the NaaS CSP's operational support systems and business support systems to the administration capabilities and business capabilities of peer NaaS CSPs, in respect of peer cloud services that are used by the NaaS CSP;

9) Service inventory functional component. The service inventory functional component provides contains and maintains information about the instances of NaaS services deployed by the NaaS CSP.

NOTE – This component may also apply to cloud service categories different from NaaS.

8.3.2 OSS-NS functional components

NOTE – The following description is based on an adaptation of the OSS functional components as described in clause 9.2.5.3 of [ITU-T Y.3502].

The OSS-NS functional components encompass the set of operational-related management capabilities that are required in order to manage and control network services offered to customers as part of NaaS services. See clause 7.8.2.1 for a description of OSS-NS functionalities.

Figure 8-4 shows the OSS-NS functional components.

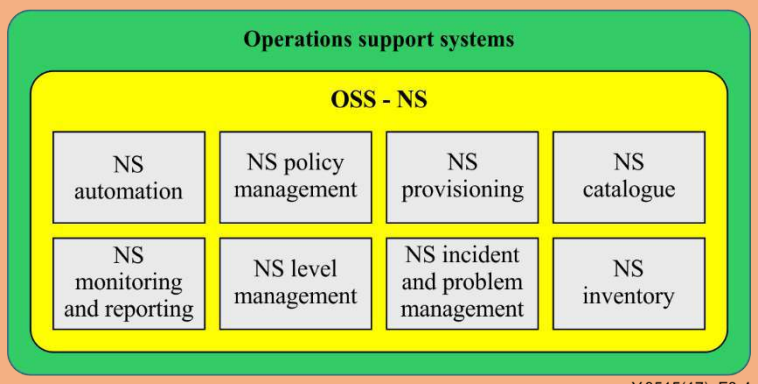


Figure 8-4 – OSS-NS functional components

The OSS-NS functional components include:

– NS catalogue;
– NS provisioning;
– NS monitoring and reporting;
– NS policy management;
– NS automation;
– NS level management;
– NS incident and problem management;
– NS inventory.

8.3.2.1 NS catalogue

The NS catalogue functional component provides a listing of all network services of the NaaS CSP. The NS catalogue contains and /or references all relevant technical information required to deploy, provision and run a network service.

8.3.2.2 NS provisioning

The NS provisioning functional component provides the capabilities for provisioning network services, both in terms of the provisioning of network service implementations and of network service access endpoints and the workflow required to ensure that elements are provisioned in the correct sequence.

8.3.2.3 NS monitoring and reporting

The NS monitoring and reporting functional component provides capabilities for:

– Monitoring the activities of other functional components throughout the NaaS CSP's system. This includes functional components involved in the support of network services, such as functional components in the OSS-NS itself like the NS automation functional component (e.g., the provisioning of a network service instance for a particular customer).
– Providing reports on the behaviour of the NaaS CSP's system, which can take the form of alerts for behaviour which has a time-sensitive aspect (e.g., the occurrence of a fault, the completion of a task), or it can take the form of aggregated forms of historical data (e.g., service usage data).
– Storage and retrieval of network service monitoring and event data as logging records.

There is a need to guarantee the availability, confidentiality and integrity of the logging records held by the NS monitoring and reporting functional component. For multi-tenant cloud services, there is also a need to design access to the records so that particular tenants can only gain access to information about their own tenancy and about no other tenancy.

8.3.2.4 NS policy management

The NS policy management functional component provides capabilities to define, store and retrieve policies that apply to network services. Policies can include business, technical, security, privacy and certification policies that apply to network services and their usage by NaaS CSCs.

Some policies can be general and apply to a network service irrespective of the customer concerned. Other policies can be specific to a particular customer.

8.3.2.5 NS automation

The NS automation functional component provides capabilities for network service delivery including the management and execution of network service templates and the orchestration of network services. The NS automation functional component holds the network service templates which define the cloud computing activities and workflows required to provision and deliver a specific entry in the NS catalogue.

Network service provisioning can be automated in order to support scalable resource operations, including configuration and charging.

Network service administration activities of NaaS CSC can be capable of being automated and need not require any intervention by NaaS CSP.

The NS automation functional component works with the NS provisioning functional component and the service integration functional component to achieve its goals.

8.3.2.6 NS level management

The NS level management functional component provides capabilities for managing the service levels of a particular network service, aiming to ensure that the network service meets the requirements of the SLA which applies to the network service.

The NS level management functional component manages the capacity and performance relating to a network service. This can involve the application of network service policies (e.g., a placement rule which aims to avoid single points of failure).

The NS level management functional component obtains monitoring information from the NS monitoring and reporting functional component in order to measure and record key performance indicators (KPIs) for the network service. Capacity of network service is allocated or de-allocated based on the basis of these KPIs.

The NS level management functional component also keeps track of the overall state of allocated and available resources. The comparison of allocated capacity against network service performance KPIs can assist in the identification of current or potential bottlenecks, in support of capacity planning.

8.3.2.7 NS incident and problem management

The NS incident and problem management functional component provides capabilities for the capture of network service incident or problem reports and managing those reports through to resolution.

Network service incidents and problems can be detected and reported by the NaaS CSP's systems, or they can be detected and reported by NaaS CSCs.

8.3.2.8 NS inventory

The NS inventory functional component holds information of all network service instances. This information is updated during the lifecycle of the network service instances, reflecting changes resulting from execution of management operations on these network service instances.

8.3.3 OSS-NF functional components

NOTE – The following description is based on an adaptation of the OSS functional components as described in clause 9.2.5.3 of [ITU-T Y.3502].

The OSS-NF functional components encompass the set of operational related management capabilities that are required in order to manage and control the network functions offered to customers as part of network services. Refer to clause 7.8.2.2 for a description of OSS-NF functionalities.

Figure 8-5 shows the OSS-NF functional components.

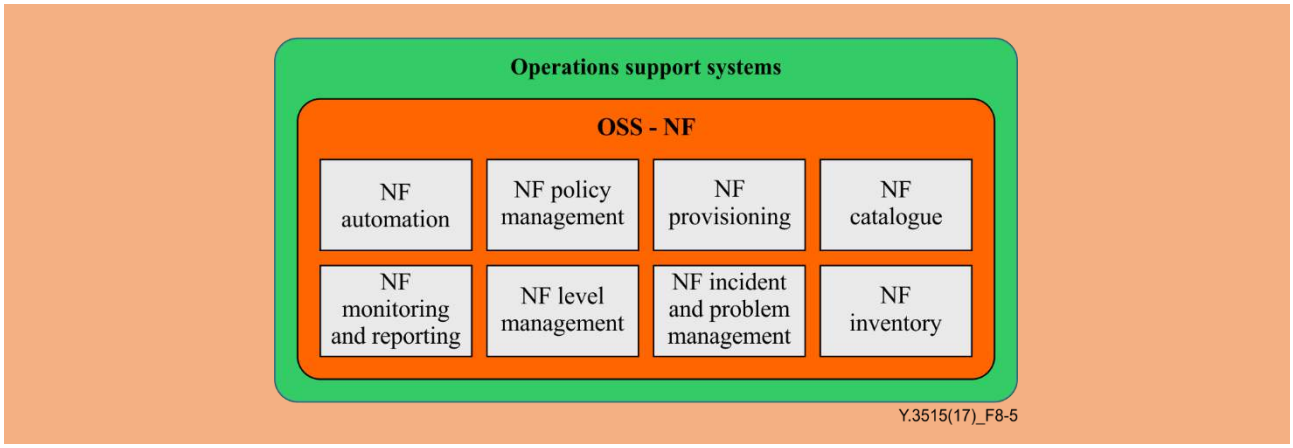


Figure 8-5 – OSS-NF functional components

The OSS-NF functional components include:

– NF catalogue;
– NF provisioning;
– NF monitoring and reporting;
– NF policy management;
– NF automation;
– NF level management;
– NF incident and problem management;
– NF inventory.

8.3.3.1 NF catalogue

The NF catalogue functional component provides a listing of all network functions of the NaaS CSP. The NF catalogue functional component contains and/or references all relevant technical information required to deploy, provision and run a network function.

8.3.3.2 NF provisioning

The NF provisioning functional component provides the capabilities for provisioning network functions, both in terms of the provisioning of network functions implementations and of network functions access endpoints and the workflow required to ensure that necessary NF elements are provisioned in the correct sequence.

8.3.3.3 NF monitoring and reporting

The NF monitoring and reporting functional component provides capabilities for:

– Monitoring the activities of other functional components throughout the NaaS CSP's system. This also includes functional components involved in the support of network functions, such as other OSS-NF functional components like the NF automation functional component (e.g., the provisioning of a network functions instance for a particular customer);

– Providing reports on the behaviour of the NaaS CSP's system, which can take the form of alerts for behaviour which has a time-sensitive aspect (e.g., the occurrence of a fault, the completion of a task), or it can take the form of aggregated forms of historical data (e.g., network function usage data);
– Storage and retrieval of network functions monitoring and event data as logging records.

There is a need to guarantee the availability, confidentiality and integrity of the logging records held by the NF monitoring and reporting functional component.

8.3.3.4 NF policy management

The NF policy management functional component provides capabilities to define, store and retrieve policies that apply to network functions. Policies can include business, technical, security, privacy and certification policies that apply to network functions and their usage by NaaS CSCs.

Some policies can be general and apply to a network function irrespective of the customer concerned. Other policies can be specific to a particular customer.

8.3.3.5 NF automation

The NF automation functional component provides capabilities for network functions' delivery including the management and execution of network functions' templates and the orchestration of network functions. The NF automation functional component holds the network functions templates which define the cloud computing activities and workflows required to provision and deliver a specific entry in the NF catalogue.

Network function provisioning can be automated in order to support scalable resource operations, including configuration and charging.

Network function administration activities of the NaaS CSC can be capable of being automated and need not require any intervention by the NaaS CSP.

The NF automation functional component works with the NF provisioning functional component to achieve its goals.

8.3.3.6 NF level management

The NF level management functional component provides capabilities for managing the service levels of a particular network function, aiming to ensure that the network function meets the requirements of the SLA which applies to the related network service.

The NF level management functional component manages the capacity and performance relating to a network function. This can involve the application of network function policies (e.g., a placement rule which aims to avoid single points of failure).

The NF level management functional component obtains monitoring information from the NF monitoring and reporting functional component in order to measure and record KPIs for the network function. Capacity of a network function can be allocated or de-allocated based on the basis of these KPIs.

The NF level management functional component also keeps track of the overall state of allocated and available resources. The comparison of allocated capacity against network function performance KPIs can assist in the identification of current or potential bottlenecks, in support of capacity planning.

8.3.3.7 NF incident and problem management

The NF incident and problem management functional component provides capabilities for the capture of network function incident or problem reports and managing those reports through to resolution.

Network function incidents and problems can be detected and reported by the NaaS CSP's systems, or they can be detected and reported by NaaS CSCs.

8.3.3.8 NF inventory

The NF inventory functional component holds information of all network function instances. This information is updated during the lifecycle of the network function instances, reflecting changes resulting from execution of management operations on these network function instances.

8.3.4 OSS-CCS functional components

NOTE – The following description is based on an adaptation of the OSS functional components as described in clause 9.2.5.3 of [ITU-T Y.3502].

The OSS-CCS functional components encompass the set of operational-related management capabilities that are required in order to manage and control the virtual resources for CCS necessary for the support of network functions instances. These virtual resources are provided in NaaS CSP's infrastructure points of presence (PoPs) (e.g., data centres) in which network functions instances are deployed. Typical virtual resources for compute include virtual machines (VMs) or containers. See clause 7.8.3 for a description of OSS-CCS functionalities.

Figure 8-6 shows the OSS-CCS functional components.

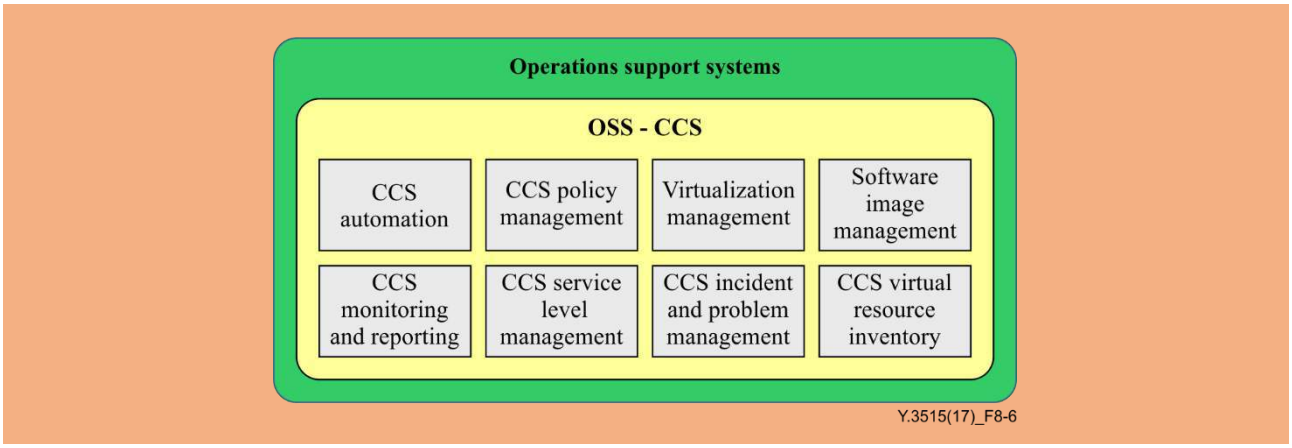


Figure 8-6 – OSS-CCS functional components

8.3.4.1 CCS automation

The CCS automation functional component provides capabilities for delivering and orchestrating virtual resources for cloud compute and storage. This includes orchestration of allocation, release, upgrade of relevant infrastructure resources including optimizing of such resources usage, as well as managing the association of the virtual resources to the physical resources. Provisioning of these virtual resources can be automated in order to support scalable resource operations, including configuration.

8.3.4.2 CCS monitoring and reporting

The CCS monitoring and reporting functional component provides capabilities for:

– Reporting on the behaviour of the NaaS CSP's system, which can take the form of alerts for behaviour which has a time-sensitive aspect (e.g., the occurrence of a fault, the completion of a task), or it can take the form of aggregated forms of historical data (e.g., service usage data);

– Storing and retrieving monitoring and event data as logging records.

There is a need to guarantee the availability, confidentiality and integrity of the logging records held by the CCS monitoring and reporting functional component. For multi-tenant cloud services, there is also a need to design access to the records so that particular tenants can only gain access to information about their own tenancy and about no other tenancy.

8.3.4.3 CCS policy management

The CCS policy management functional component provides capabilities for defining, storing and retrieving policies (e.g., quotas) that apply to virtual resources for cloud compute and storage. Policies can include technical and security policies that apply to these virtual resources and their usage by their users.

8.3.4.4 CCS service level management

The CCS service level management functional component provides capabilities for managing the service levels of virtual resources for cloud compute and storage, aiming to ensure that each virtual resource meets the negotiated service level requirements.

The CCS service level management functional component manages the capacity and performance relating to virtual resources for cloud compute and storage. This can involve the application of policies (e.g., a placement deployment rule which aims to avoid single points of failure).

The CCS service level management functional component obtains monitoring information from the CCS monitoring and reporting functional component in order to measure and record KPIs for the virtual resources. Capacity of virtual resources is allocated or de-allocated based on the basis of these KPIs.

The CCS service level management functional component also keeps track of the overall state of allocated and available resources for cloud compute and storage. The comparison of allocated capacity against performance KPIs can assist in the identification of current or potential bottlenecks, in support of capacity planning. This includes the management of the virtual resources capacity (e.g., density of virtual resources to physical resources), and the forwarding of information related to infrastructure resources capacity and usage reporting.

8.3.4.5 CCS incident and problem management

The CCS incident and problem management functional component provides capabilities for capturing incident or problem reports related to virtual resources for CCS and managing those reports through to resolution.

8.3.4.6 Virtualization management

The virtualization management functional component provides the capabilities for managing the virtualization of the resources for CCS (e.g., realized by means of hypervisors).

8.3.4.7 CCS virtual resource inventory

The CCS virtual resource inventory functional component keeps track of the allocation of virtual resources for CCS to physical resources (e.g., server pool).

8.3.4.8 Software image management

The software image management functional component manages software images (e.g., network functions) as requested by other OSS functional components (e.g., OSS for network functions). These requests include operations on images such as add, delete, update, query and perform rollback. Once validated by the software image management functional component, software images are stored in a software image repository.

8.3.5 OSS-NC functional components

NOTE – The following description is based on an adaptation of the OSS functional components as described in clause 9.2.5.3 of [ITU-T Y.3502].

The OSS-NC functional components encompass the set of operational related management capabilities that are required in order to manage and control the network connectivity in NaaS CSP domains, also called NaaS CSP connectivity domains. See clause 7.8.4 for a description of the OSS-NC functionalities.

The OSS-NC functional components may be able to manage network connectivity across one or multiple NaaS CSP's domains (e.g., access, backhaul or core NaaS CSP domains) and can also manage network connectivity at one or multiple technology layers (e.g., overlay, IP, multiprotocol label switching (MPLS), optical transport network (OTN)).

Figure 8-7 shows the OSS-NC functional components.

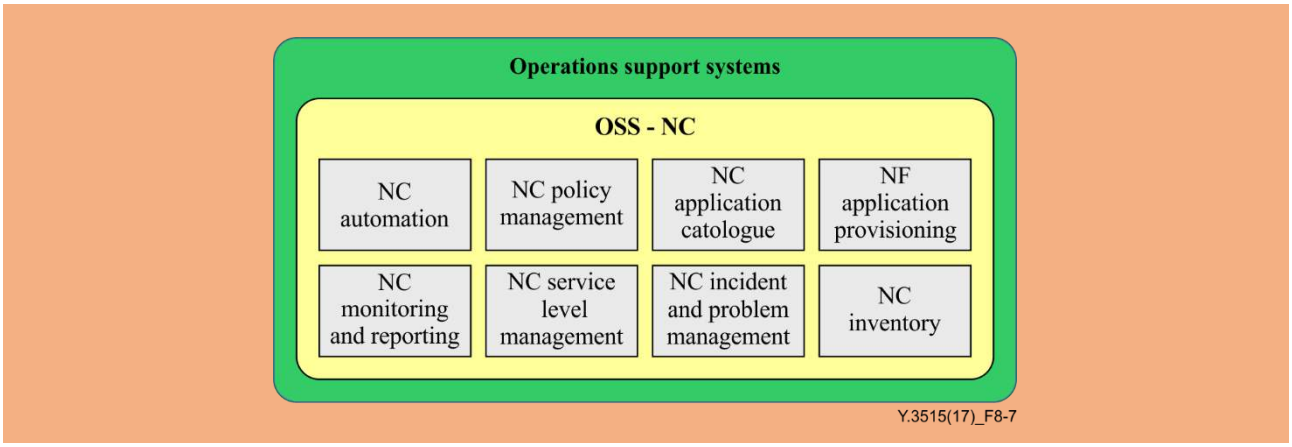


Figure 8-7 – OSS-NC functional components

8.3.5.1 NC application catalogue

The NC catalogue functional component provides a listing of all NC applications supported by the OSS-NC. A NC catalogue can contain and/or reference all relevant technical information required to deploy, provision and run a NC application.

8.3.5.2 NC application provisioning

The NC provisioning functional component provides the capabilities for provisioning NC applications, both in terms of the provisioning of NC application implementations and of access endpoints and the workflow required to ensure that elements are provisioned in the correct sequence.

8.3.5.3 NC automation

The NC automation functional component provides capabilities for the delivery of network connectivity applications and the orchestration of network connectivity across one or multiple NaaS CSP connectivity domains. This includes orchestrating the allocation, release, upgrade of network connectivity through the relevant NaaS CSP connectivity domains.

8.3.5.4 NC monitoring and reporting

The NC monitoring and reporting functional component provides capabilities for:

– Providing reports on the behaviour of the NaaS CSP's NC applications, which can take the form of alerts for behaviour which has a time-sensitive aspect (e.g., the occurrence of a fault on a given established NC, the completion of a task), or it can take the form of aggregated forms of historical data (e.g., NC usage data).

– Storage and retrieval of NC related monitoring and event data as logging records.

There is a need to guarantee the availability, confidentiality and integrity of the logging records held by the NC monitoring and reporting functional component.

8.3.5.5 NC policy management

The NC management functional component provides capabilities to define, store and retrieve policies that apply to NC applications. Policies can include technical and security policies that apply to NC applications and their usage by users of these NC applications.

8.3.5.6 NC service level management

The NC service level management functional component provides capabilities for managing the service levels of NC, aiming to ensure that the negotiated NC service level requirements are met.

The NC service level management functional component manages the capacity and performance relating to NC. This can involve the application of policies (e.g., a placement rule which aims to avoid single points of failure).

The NC service level management functional component obtains monitoring information from the NC monitoring and reporting functional component in order to measure and record KPIs for the NC. NC capacity can be allocated or de-allocated based on the basis of these KPIs.

The NC service level management functional component also keeps track of the overall state of an allocated NC capacity and available network capacity. The comparison of allocated capacity against performance KPIs can assist in the identification of current or potential bottlenecks, in support of capacity planning. This includes the management of connectivity capacity and the forwarding of information related to NC capacity and usage reporting.

8.3.5.7 NC incident and problem management

The NC incident and problem management functional component provides capabilities for the capture of incident or problem reports related to NC and managing those reports through to resolution.

8.3.5.8 NC inventory

The NC inventory functional component keeps track of the allocated NC including the associated characteristics.

8.3.6 OSS functional components for physical resources

NOTE – This clause is out of the scope of this Recommendation.

8.4 Functional components for NaaS development support

Refer to clause 7.9 for a description of development functionalities for NaaS products and services.

The functional components for NaaS development support include the development support functional components described in clause 9.2.5.5 of [ITU-T Y.3502]:

– Developer environment functional component. Provides the capabilities to support the development of the NaaS service software implementation including the development of the following software components:
  - Network function software. A network function software can be developed in such a way that features and capability of the network function is provided by elementary network functions; It can also be provided by composition of other developed network functions;
  - Network services;
  - Network connectivity applications software (such as for SDN applications).
– The development environment functional component includes capabilities for the creation of the configuration metadata for the above software components as well as scripts and related artefacts that are then used by the provider's operational support systems to provision and configure the network function, network service or network connectivity application.
– Build management functional component. Supports the building of a ready-to-deploy NaaS software package for network functions, network services and network connectivity applications which can be passed to the NaaS CSP for deployment into the NaaS cloud service environment. The software package consists of both the service implementation software and also the configuration metadata and scripts.
– Test management functional component. Supports the execution of test cases against any build of the NaaS service implementation. The test management functional component produces reports of the executed tests and these can be communicated to the NaaS CSP along with a build of the NaaS service implementation.

The functional components for NaaS development support (Dev-NaaS products and services) are shown in Figure 8-8.

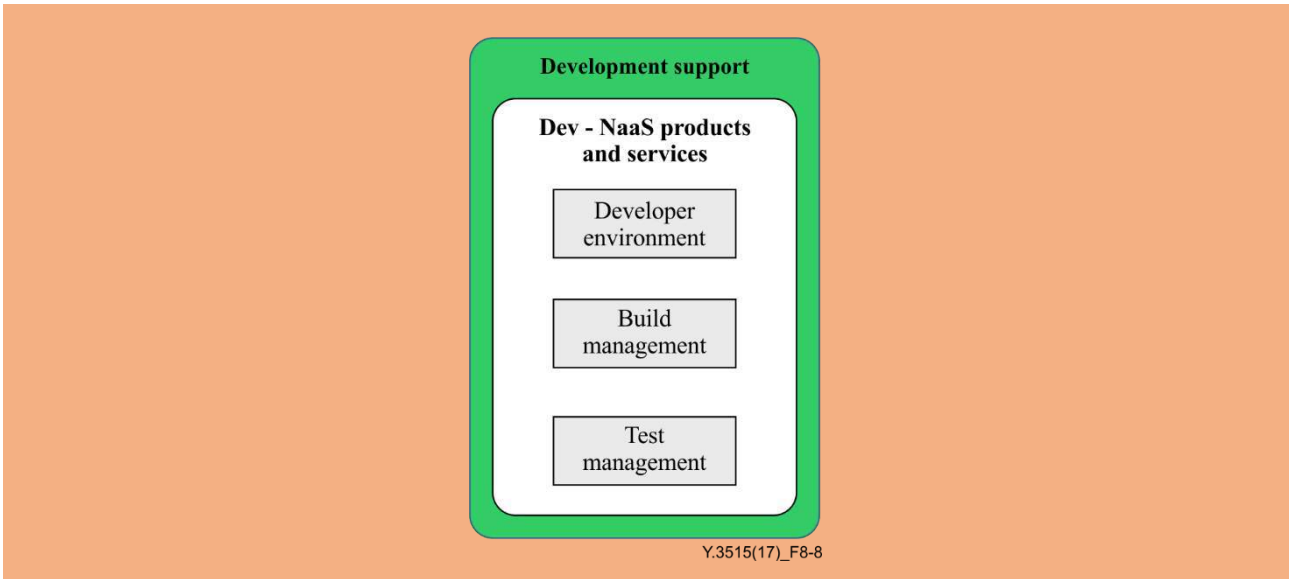


Figure 8-8 – Functional components for Dev-NaaS products and services

9 Security considerations

Security aspects for consideration within the cloud computing environment, including NaaS, are addressed by security challenges for NaaS CSPs, as described in [ITU-T X.1601]. In particular, [ITU-T X.1601] analyses security threats and challenges, and describes security capabilities that could mitigate these threats and meet the security challenges.

The functional components for security systems defined in clause 9.2.5.2 of [ITU-T Y.3502] are applicable in the context of the NaaS functional architecture. These components are responsible for applying security related controls to mitigate the security threats in cloud computing environments and encompass all the security facilities required to support cloud services of the NaaS cloud service category.

Annex A

OSS reference points

(This annex forms an integral part of this Recommendation.)

This annex describes reference points related to OSS whose functional components are described in clause 8.3 of the NaaS functional architecture.

Figure A.1 identifies the reference points internal to the OSS (reference points labelled as ''oss'') as well as reference points between the OSS and external entities.

For a NaaS service that involves either a ''legacy'' (i.e., non-virtualized) network functions (i.e., PNFs), the ''OSS for NaaS services'' will interact with the OSS (called ''legacy OSS'' in Figure A.1) responsible for the management of these ''legacy'' network functions. The ''OSS legacy'' system typically includes management systems such as network management systems (NMSs) or element management systems (EMSs).

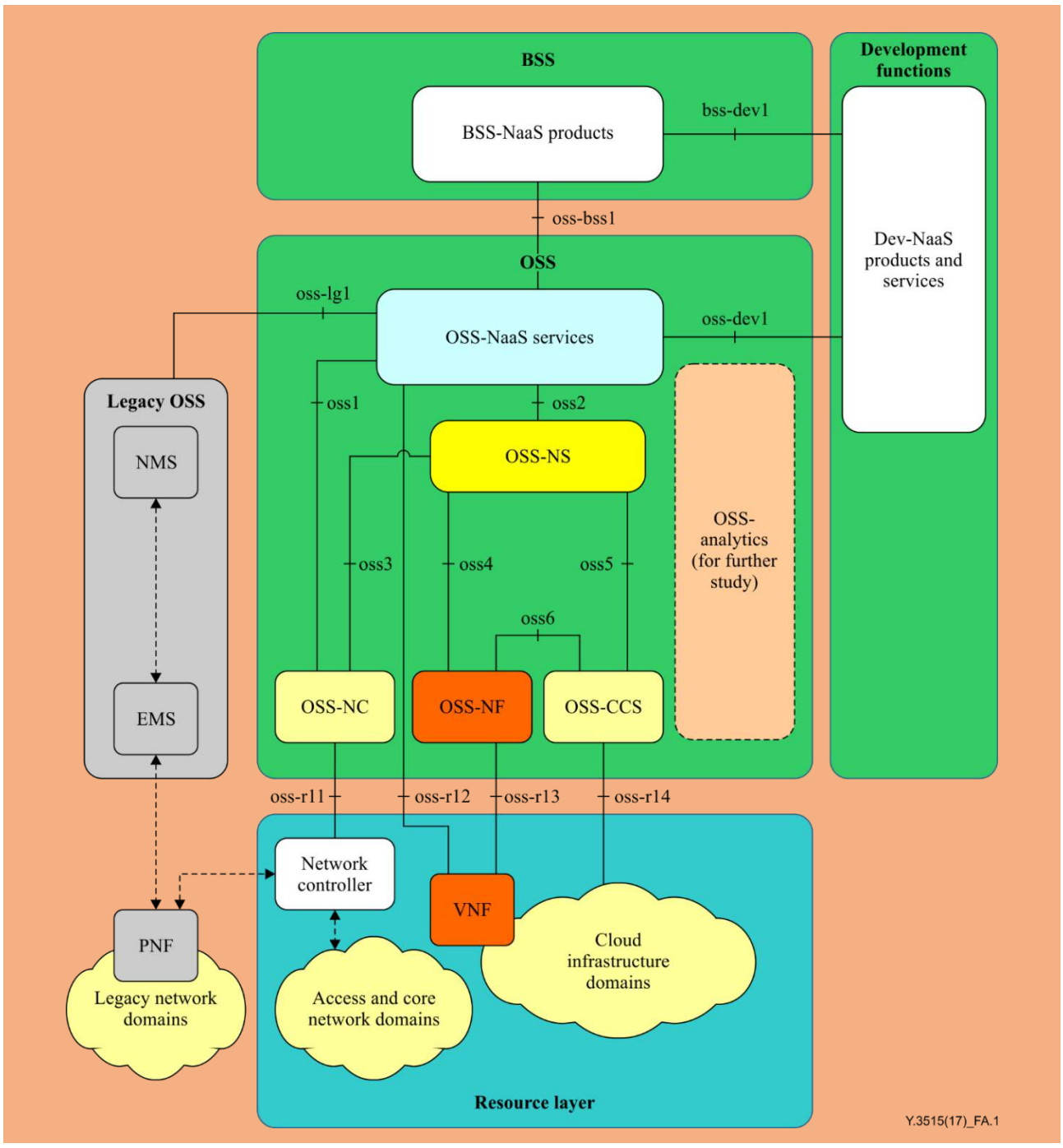


Figure A.1 – OSS-related reference points

The internal reference points illustrated in Figure A.1 are listed as follows:

– **oss1**: This reference point covers interactions between the OSS-NaaS and OSS-NC, e.g., for wide area network (WAN) connectivity management.

– **oss2**: This reference point covers interactions between the OSS-NaaS and the OSS-NS. This includes interactions related to network service lifecycle management, network service fault and performance management, network service usage management and network service inventory management.

– **oss3**: This reference point covers interactions between the OSS-NS and OSS-NC, e.g., for WAN connectivity management, as required by a given network service orchestrated by the OSS-NS.

– **oss4**: This reference point covers interactions between the OSS-NS and OSS-NF. This includes interactions related to network functions lifecycle management, network functions fault and performance management, network functions usage management and network functions inventory management.

– **oss5**: This reference point covers interactions between the OSS-NS and OSS-CCS. This includes interactions related to virtual resources life cycle management, virtual resources fault and performance management, virtual resources usage management and virtual resources inventory management.

– **oss6**: This reference point covers interactions between the OSS-NF and OSS-CCS. This includes interactions related to virtual resources life cycle management, virtual resources fault and performance management, virtual resources usage management and virtual resources inventory management.

The external reference points illustrated in Figure A.1 are listed as follows:

– **oss-bss1**: This reference point covers interactions between BSS functional components for NaaS products (BSS-NaaS products) and OSS components for NaaS services (OSS-NaaS). This includes for example NaaS service order interactions between the BSS account management functional component and the OSS-NaaS following a NaaS CSC order for a NaaS product.

– **oss-rl1**: This reference point covers interactions between the OSS-NC and a network controller (e.g., a SDN controller). This includes interactions related to virtualized network connectivity life cycle management, fault and performance management, usage management and inventory management. In this case the OSS-NC can be viewed as a set of SDN applications as per [ITU-T Y.3300], [ITU-T Y.3302] and the interactions being carried over the SDN Application Control Interface (ACI) reference point.

– **oss-rl2**: This reference point covers interactions between the OSS-NaaS and a VNF. This includes interactions related to the network functions' configuration management and network functions' fault and performance management from a NaaS service perspective.

– **oss-rl3**: This reference point covers interactions between the OSS-NF and a VNF. This includes interactions related to the network functions' configuration management and network functions' fault and performance management.

– **oss-rl4**: This reference point covers interactions between the OSS-CCS with the NaaS cloud infrastructure domain. This includes interactions related to the specific assignment of virtual resources in response to resource allocation requests and the exchange of virtual resources state information.

– **oss-lg1**: This reference point covers interactions between the OSS-NaaS with a legacy OSS system that manages legacy networks including PNFs.

– **oss-dev1**: This reference point covers interactions between the OSS-NaaS with Development Functions for NaaS products and Services. This include interactions related the distribution of developed NaaS services in order to make them available in the service catalogue functional component within the OSS-NaaS.

– **bss-dev1**: This reference point covers interactions between the BSS-NaaS products with development functions for NaaS products and services. This includes interactions related to the distribution of developed NaaS products in order to make them available in the product catalogue functional component within the BSS-NaaS products.

NOTE 1 – In some cases, interaction of the OSS-NaaS with a PNF may be realized through the OSS-NC using either oss1 reference point or oss2 plus oss3 reference points. In such case the OSS-NC will typically interact with a Network Controller (e.g., a SDN controller or the NMS/EMS that controls and manages the PNF).

NOTE 2 – The OSS-Analytics box shown in Figure A.1 is for further study. Main objective of the OSS-Analytics is to support network analytics functionalities as described in clause 7.3. Interactions of the OSS-analytics with other OSS components needs further study.

Annex B

Functional components on mapping between physical and virtualized networks

(This annex forms an integral part of this Recommendation.)

This annex describes the functional components on mapping between physical and virtualized networks.

NOTE – A virtualized network can be seen as a specific realization of a NS whose resources are provided on top of physical resources that constitute a physical network.

In order to realize the functionality for mapping between physical and virtualized networks (refer to clauses 7.7.1 and I.4), specialized mapping functional components are necessary.

The resource abstraction and control functional component [ITU-T Y.3502] is used by NaaS CSPs to:

– Provide access to the physical computing resources through software abstraction;

– Ensure efficient, secure, and reliable usage of the underlying infrastructure;

– Enable a NaaS CSP to offer qualities such as rapid elasticity, resource pooling and on-demand self-service.

The resource abstraction and control functional component can include software elements such as hypervisors, virtual machines, virtual data storage, and time-sharing.

The physical resources functional component [ITU-T Y.3502] includes hardware resources, such as computer, networks (routers, firewall, switches, network links and network connectors), storage components and other physical computing infrastructure elements.

The resource abstraction and control functional component and the physical resources functional component can be instantiated to realise the functionality described in clause 7.7.1, as shown in Figure B.1.

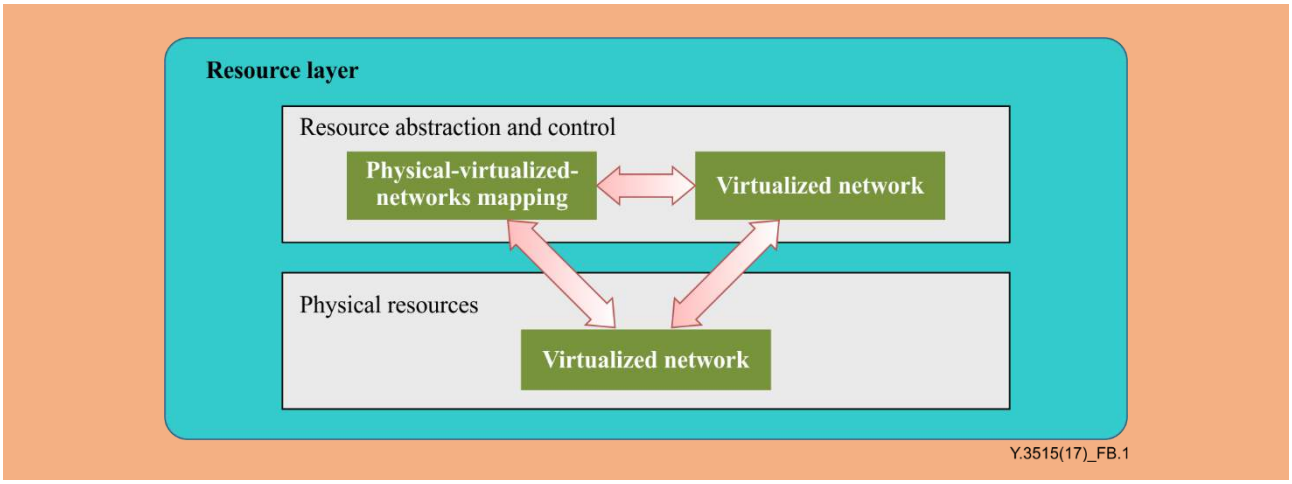


Figure B.1 – Functional components on mapping between physical and virtualized networks

B.1 Physical network

Physical network functional component provides physical agents of physical network elements, such as physical nodes, ports, switches and links.

NOTE – Physical agents are the representations of actual physical network nodes, ports, switches, links, etc.

B.2 Virtualized network

Virtualized network functional component provides virtualized network elements, such as virtual nodes, ports, switches and links. Each tenant is represented by one virtualized network and different tenants can only discover their own virtualized network. All virtualized network elements are mapped to at least one physical element and can be enabled, disabled, modified or reorganised at runtime.

NOTE – A virtualized network element is a broader concept than VNF. It can be a VNF but also can correspond to a network port or network link.

B.3 Physical-virtualized-networks mapping

Physical-virtualized-networks mapping functional component enforces the mapping between virtualized (overlay) networks and physical (underlay) networks. The mapping contents are stored in a database, which can be accessed by both physical and virtualized networks.

Appendix I

Mapping among NaaS functional requirements and functionalities

(This appendix does not form an integral part of this Recommendation.)

This appendix aims to describe the mapping among NaaS functional requirements (specified in [ITU-T Y.3512]) and functionalities. The mapping between functionalities and functional requirements of three kinds of NaaS services had been taken into account.

I.1 Mapping and derivation of functionality for NaaS service instantiation

Taking the functional requirements ''elastic network reconfiguration'', ''dynamic and flexible network services composition and steering'', and ''unified network control mechanism'' as the analysis example, NaaS architecture needs to satisfy dynamic configuration change requirements based on real-time network status and policy, and network resource abstraction across different layers including application layer (L7), IP layer (L3), and lower layers (L0-L2).

The traditional development and operation procedures are always separated and hardly address real-time configuration changes due to slow deployment of network functions/devices and unsatisfactory quality of experience (QoE). Therefore, it is also needed for the NaaS CSP to offer programmable ways to configure networks (so called development and operations (DevOps)), which is also mentioned in the functional requirement ''programmable NaaS platform''.

NOTE – DevOps is a software development method that stresses communication, collaboration (information sharing and web service usage), integration, automation and measurement of cooperation between software developers and other IT professionals. DevOps acknowledges the interdependence of software development and IT operations.

To implement network resource abstraction across different layers, it is needed to model different network resources in a unified manner, including physical and/or virtualized network nodes and links. Apart from this, network services and the corresponding deployment policies also need respective unified models. These three kinds of models should be able to share information with one another in order that the real-time configuration change demands can be transferred from the NaaS CSC to the NaaS CSP's network elements.

Moreover, regarding the requirement ''optimized and fine-grained traffic engineering'', its detailed description includes ''collects near real-time utilization metrics and topology data from its own network equipment'' and ''controls the network resource allocation by reconfiguring network profiles as well as properties in response to dynamically changing traffic demands'', which also require dynamic configuration changes response. Therefore, this can be grouped to derive the common functionality with the above mentioned functional requirements.

I.2 Mapping and derivation of functionality for service orchestration

Regarding ''coexistence with legacy network services and functions'', its detailed description includes ''avoid or mitigate possible performance and flexibility impacts when introducing new network connectivity services'' and ''support coexistence of new network connectivity services with legacy systems'', which requires NaaS architecture to provide the evolution and incremental deployment mechanism for the new paradigm of networking.

Taking the introduction of SDN as an example, during its transition, SDN-based networks should/could coexist with legacy IP networks, any SDN-based deployment should/could be able to exchange reachability information, forwarding traffic, and express routing policies with exiting IP networks.

Moreover, ''interworking among different VPN solutions'' is an example of networking connectivity interworking implementation requirement and can also be grouped in this functionality.

Regarding the ''unified network control mechanism'', ''centralized control view and abstraction view of resources'', ''unified SLA for multiple optimized networks'', and ''leveraging transport networks dynamically'' functional requirements, their detailed description includes ''provide a unified control mechanism for the

end-to-end NaaS connectivity given to a CSC'', ''support logically centralized management and control view of networking resources'', ''provide network connectivity services using unified SLA for CSC's management of multiple optimized networks in order to simplify and unify the control and management of networks'', and ''leverage transport networks dynamically form multiple choices of physical and virtualized networks for the purpose of providing network connectivity services'', which requires NaaS architecture to provide the dedicated mechanism to present a panorama portal to the NaaS CSC, allowing a unified abstract service modelling repository to receive, parse, and transfer NaaS CSC's requirement to the control function of specific domain, which is implemented separately with other parallel control function of dedicated domains. Using this manner, it is feasible to realize the composite NaaS service, which can be decomposed automatically and dispatched to the appropriated control function.

Take the use case for dynamic transport network, specified in [ITU-T Y.3512], as an example, it is a typical composite NaaS service, which requires the service management related function to separate the requirement composition into independent service model and distribute them to the independent network control functions.

I.3 Mapping and derivation of functionalities for network analytics, policy, and autonomy

Regarding the requirement ''optimized and fine-grained traffic engineering'' in [ITU-T Y.3512], whose detailed description includes ''collect near real-time utilization metrics and topology data from its own network equipment'', ''provide the CSC with fine-grained view on usage of network resources'', ''control the network resource allocation by reconfiguring network profiles as well as properties (e.g., topology, bandwidth) in response to dynamically changing traffic demands'', which requires NaaS architecture provide analytical mechanism to collect near real-time data from NaaS CSP's network environment, maintain monitoring NaaS service during its lifecycle, trigger the corresponding pre-defined action based on the matched specific condition.

In order to perform the closed analysis and control loop in NaaS service lifecycle management mentioned above, it is also needed for NaaS architecture to provide configurable policy mechanism, covering policy creation, policy distribution, and policy decision and enforcement.

Based on the analytical and policy mechanisms, autonomy at resource level of NaaS architecture can be achieved accordingly.

I.4 Mapping and derivation of functionality for mapping between physical and virtualized networks

On the one hand, the ''overlay network mechanism'', ''logically isolated network partition'', and ''overlapped private IP addresses'' functional requirements, whose detailed description includes ''support virtualized overlay networks on top of the physical underlay network'', ''implement LINP'', and ''allows different CSCs to use their own private IP addresses even when the subnet addresses are overlapped'' can be satisfied by virtualized overlay network mechanism, e.g., virtual extensible local area network (VXLAN), VPN. On the other hand, the ''optimized and fine-grained traffic engineering'' functional requirement asks for ''NaaS CSP provides the CSC with fine-grained view on usage of network resource''. If the network resource mentioned here consists of not only physical network, but also virtualized network, which are always implemented by tunnelling overlay mechanism, the NaaS CSC cannot obtain the near real-time utilization on physical networks. Because the virtualized network is overlaid over the physical networks, and shields the underlying information to the NaaS CSC, this results in possible underutilization/overutilization of resource.

Hence, NaaS architecture needs to provide the mapping between physical underlay network and virtual overlay network in order to present fine-grained view on usage of physical network resource.

I.5 Mapping and derivation of functionalities for an evolved real-time OSS

The ''operation and management'', ''performance'' and ''service chain'' requirements for NaaS applications described in clause 7 of [ITU-T Y.3512] imply that functionalities for performance management as well as for flexible provisioning and configuration of NaaS applications and their chaining have to be supported by the OSS.

Concerning NaaS platform related requirements described in clause 8 of [ITU-T Y.3512], ''programmable NaaS platform'', ''isolation of service chain for tenants'' and ''flexible scaling of NaaS platform'' requires that the OSS functionalities be flexible and efficient enough to allow for the instantiation of network services, network functions and corresponding cloud computing resources in an automated manner.

Regarding NaaS connectivity related requirements identified in clause 9 of [ITU-T Y.3512], ''unified network control mechanism, ''elastic network reconfiguration'', ''leveraging transport networks dynamically'' and ''seamless and end-to-end solution of bandwidth'', this requires that the NaaS architecture provides OSS functionalities that support the real-time control, management and orchestration of end-to-end connectivity across the NaaS cloud computing infrastructure as well as access and core network domains.

I.6 Mapping and derivation of functionalities for NaaS products and NaaS services development

''Integration of software applications'' requirements as described in clause 8.5 of [ITU-T Y.3512] implies that integration of these applications on the NaaS platform allows the building and design of combined solutions which will be tested prior to their deployment by the NaaS CSP. Functionalities for the development of NaaS services are therefore required to be supported in the NaaS architecture.

I.7 Mapping and derivation of functionalities related to NaaS business

[ITU-T Y.3512] does not explicitly address requirements related to NaaS business capabilities since the requirements in [ITU-T Y.3512] are related to the three types of NaaS services, i.e., NaaS application, NaaS platform and NaaS connectivity. However, these business capabilities have to be addressed in the NaaS architecture to support the management of NaaS service offerings by the NaaS CSP including NaaS CSC requests for selection and purchase of NaaS products and services available in the NaaS CSP product catalogue.

Appendix II

Modelling usage example of NaaS service, NaaS service operational policy and NaaS resource model

(This appendix does not form an integral part of this Recommendation.)

II.1 Introduction

In practice, a NaaS CSP can virtualize cloud resources into multiple isolated virtual private clouds (VPCs) and provide them to NaaS CSCs. A NaaS CSC can establish and manage the network easily in a typical VPC, for example: deploying or removing virtualized network devices (e.g., vRouter and vSwitch), adjusting the topology of VPC networks, specifying packet forwarding policies, and deploying or removing virtualized network services (e.g., load balancer, firewalls, databases, DNS). The NaaS functionalities that the NaaS CSC can obtain are virtualized and actually performed by VMs located on compute servers, which may be located in different geographically distributed data centres, connected through physical or overlay networks.

The manipulation of the virtualized VPC network may also affect the configuration of physical networks. For example, when two new VMs associated to a given VPC are deployed in two different data centres, the VPC control mechanism needs to generate a VPN between these two data centres for the internal VPC communications. Therefore, the control mechanism for a VPC should be able to adjust the underlying network at runtime when the NaaS CSC requests changes to the VPC network or service deployment.

When the NaaS CSC moves from one location to another, which is near to another NaaS CSP's data centre, and in the case the network load between these two data centres is low, NaaS CSC's VM(s) should be migrated to the new data centre in order to allow for a better user experience.

As illustrated by Figure II.1, a VPC corresponds to a combination of cloud computing resources with a VPN infrastructure to give NaaS CSCs the abstraction of a private set of cloud resources that are transparently and securely connected to their own infrastructure. VPCs are created by taking dynamically configurable pools of cloud resources and connecting them to enterprise sites with VPNs.

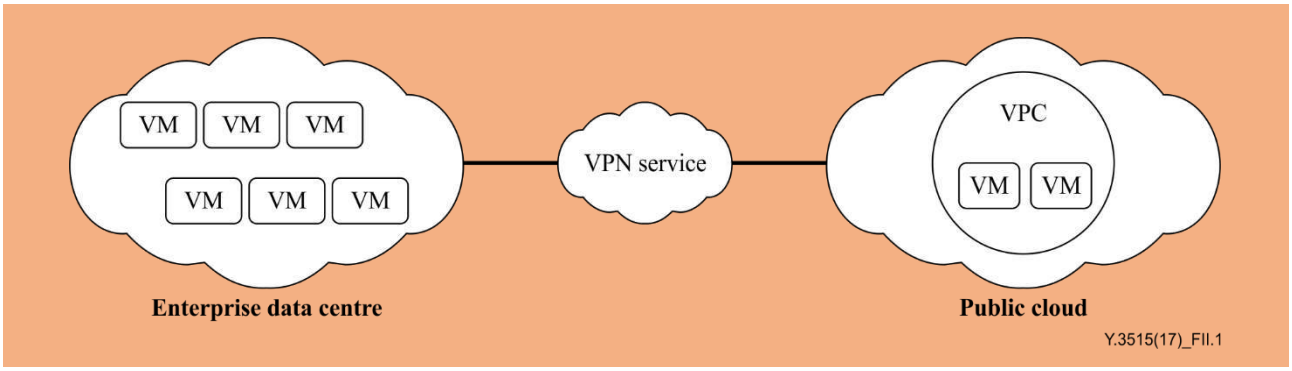


Figure II.1 – Example of VPC and VPN relationship

II.2 Modelling usage

Based on the description given in clause II.1, the VPC service can be modelled as a VPC NaaS service model based on its concrete service attributes, including service ID, tenant ID, access bandwidth, access virtualized network device, attached virtual service, etc.

The initial provisioning configuration can be generated based on the VPC NaaS service model, together with the corresponding NaaS service operational policy model, which includes the following aspects:

– The required services on data centres according to NaaS CSC's profile are allocated;

– Services located in multiple distributed data centres are interconnected via e.g., VPNs;

– The VPN associated to the services provided for NaaS CSC matches NaaS CSC's profile in terms of latency, speed, and bandwidth.

The runtime VM migration configuration can be generated based on the VPC NaaS service model, together with the corresponding NaaS service operational policy model, which includes the aspects below:

– The action is triggered by the event that an NaaS CSC's location is changed (location near to another NaaS CSP's data centre) and the network load between these two data centres is low;

– The VM is migrated to the new data centre;

– The VPN connecting an NaaS CSC's services is updated.

The above used network resources are managed by a resource abstraction and control functional component in the form of NaaS resource model, containing the network topology (physical and virtual interconnection of network elements, etc.), inventory (database of network elements, ports, device type, capabilities, etc.), protocol specific information, etc.

Appendix III

Relationship between NaaS functional architecture and SDN

(This appendix does not form an integral part of this Recommendation.)

As categorized by [ITU-T Y.3512], NaaS services are divided into NaaS application services, NaaS platform services, and NaaS connectivity services. As a kind of cloud service, based on its use cases and derived functional requirements specified in [ITU-T Y.3512], network connectivity service can be implemented by the traditional technologies and/or emerging technologies, such as SDN.

Both cloud computing and SDN have their own reference architectures, whose mapping is presented in Figure III.1. NaaS connectivity is a kind of cloud service, which is located in the services layer of the cloud reference architecture. If it is supported and implemented by SDN, a NaaS connectivity service can be regarded as one kind of SDN application in SDN architecture and seen as a bridge between the cloud computing and SDN architectures.

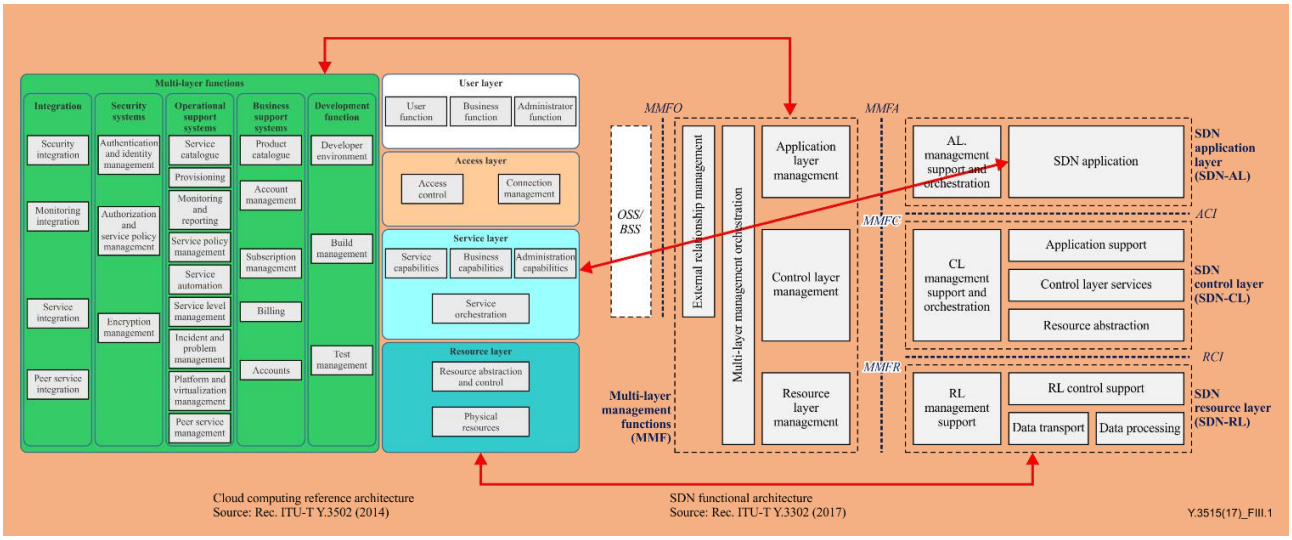


Figure III.1 – Mapping of architectures of cloud computing and SDN

Figure III.2 presents the positioning of a NaaS connectivity service as an application in the SDN architecture. Such NaaS connectivity service interacts with SDN management functionalities and SDN control layer functionalities including application support entity, orchestration entity, abstraction entity.

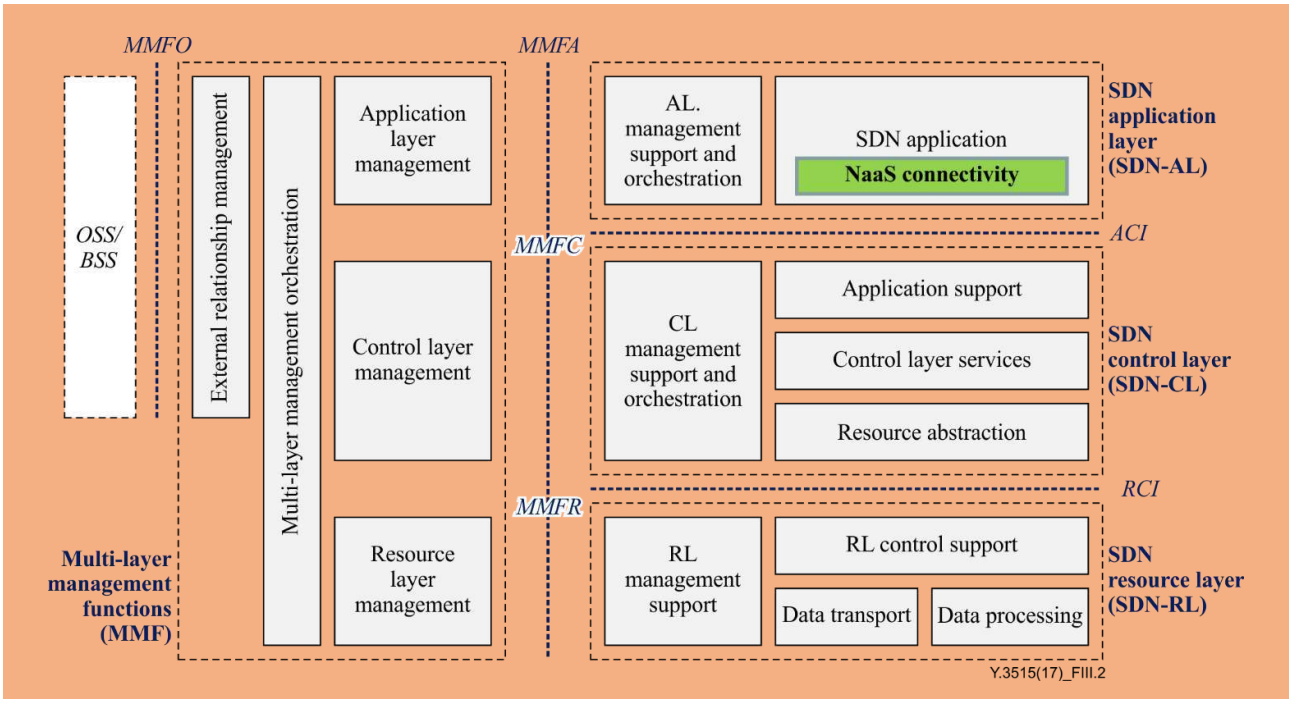


Figure III.2 – NaaS connectivity and relationships SDN functional entities

In the use cases of [ITU-T Y.3512], SDN is not mentioned, although it can be regarded as one of the implementation technologies especially in NaaS connectivity use cases.

Appendix IV

Example of NFV and SDN usage in support of NaaS architecture

(This appendix does not form an integral part of this Recommendation.)

This appendix provides an example of how NFV and SDN can be used in realizing the NaaS functional architecture.

The NFV architectural framework as defined in [b-ETSI NFV-arch] and [b-ETSI NFV-mano] provides a high-level functional architectural framework and design philosophy of virtualized network functions and of the supporting infrastructure. It identifies functional blocks and the main reference points between such blocks. In particular, the following functional blocks are described:

– VNF;
– NFV Infrastructure (NFVI), including:
  • Hardware and virtualized resources; and
  • Virtualization layer.
– Virtualized infrastructure manager (VIM);
– NFV orchestrator (NFVO);
– VNF manager (VNFM);
– WAN infrastructure manager (WIM).

[ITU-T Y.3300] describes the framework of SDN specifying fundamental aspects of SDN and providing a high-level architecture consisting of the following layers:

– SDN application layer;
– SDN control layer;
– SDN resource layer.

Figure IV.1 shows how elements of the NFV and SDN architectures (represented using dotted boxes) can be mapped to the functional components of the NaaS architecture defined in clause 8 of this Recommendation.

Regarding the use of SDN, the scenario illustrated in Figure IV.1 assumes that SDN is used to control network connectivity between NFVI PoPs. The resources controlled by SDN are also assumed to be physical resources in a wide area network (e.g., physical switches or routers) and therefore does not cover the case where the SDN resource layer can itself be virtualized (e.g., virtual switches or routers supported as virtualized network functions). The potential use of SDN in the NFVI is not shown in Figure IV.1. The SDN control layer (e.g., the SDN controller) and the SDN resource layer (e.g., switches and routers) can also be virtualized as well elements of the NFV architecture (e.g., VNFM).

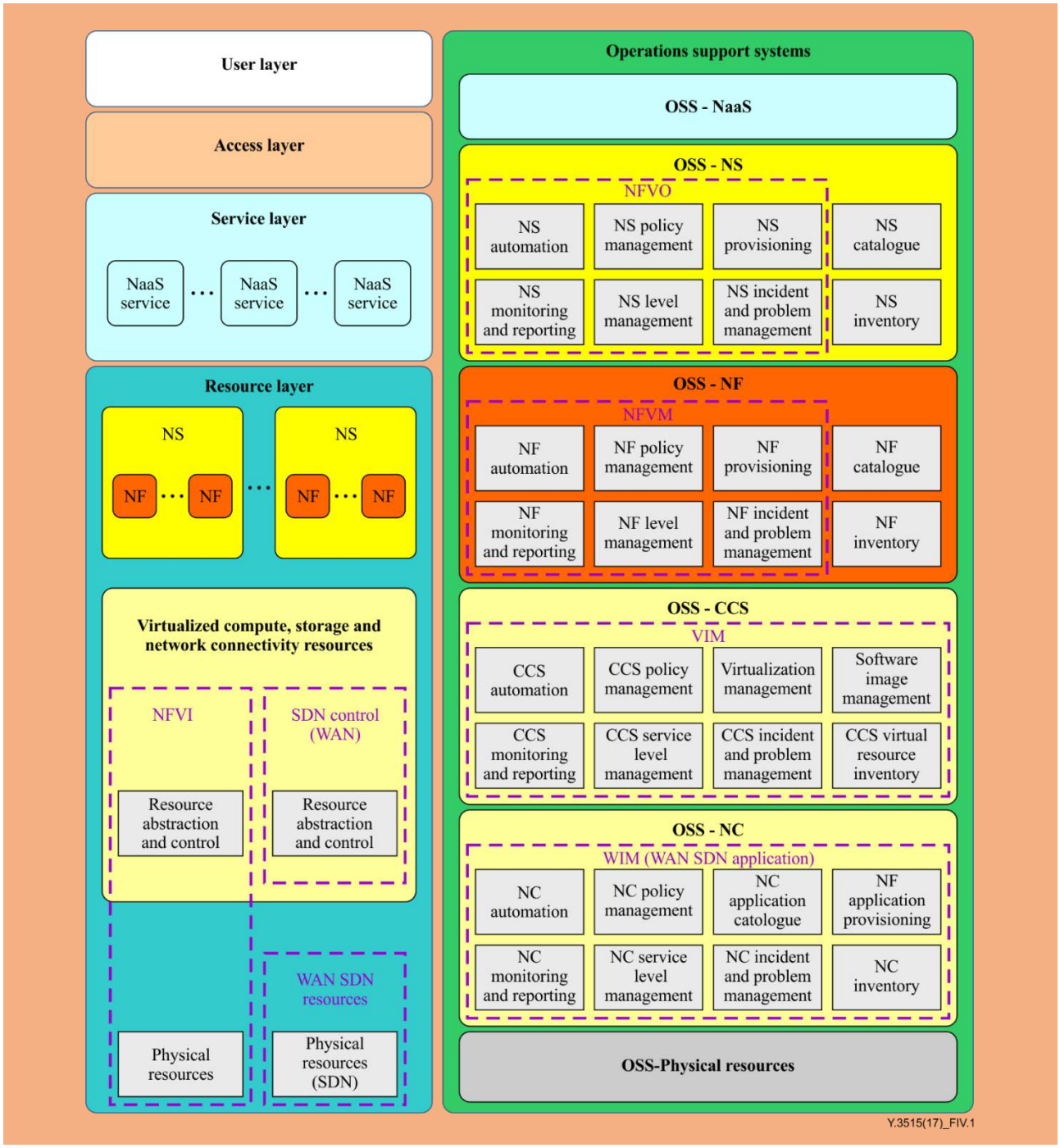


Figure IV.1 – Example of NFV and SDN usage to support NaaS

Bibliography

[b-ETSI NFV-arch] ETSI GS NFV 002 V1.2.1 (2014), *Network Functions Virtualisation (NFV); Architectural Framework*.

[b-ETSI NFV-mano] ETSI GS NFV-MAN 001 V1.1.1 (2014), *Network Functions Virtualisation (NFV); Management and Orchestration*.

[b-ETSI NFV-term] ETSI GS NFV 003 V1.2.1 (2014), *Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV*.


Big Data
Macro
Shift

Cloud computing – Functional architecture of big data as a service

Recommendation ITU-T Y.3519

(12/2018)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Summary

Recommendation ITU-T Y.3519 describes the functional architecture for big data as a service (BDaaS). The functional architecture is defined on the basis of the analysis of requirements and activities of cloud computing-based big data described in Recommendation ITU-T Y.3600.

Following the methodology of Recommendation ITU-T Y.3502, the BDaaS functional architecture is described from a set of functional components and cross-cutting aspects. The specified functional components consist of sets of functions that are required to perform the BDaaS activities for the roles and sub-roles described in Recommendation ITU-T Y.3600.

Keywords

Big data, big data as a service, cloud computing, functional architecture, functional component.

Table of Contents

1 Scope

This Recommendation provides an overview of the big data as a service (BDaaS) functional architecture and defines the BDaaS functional architecture and cross-cutting aspects by specifying the functional components for the support of BDaaS.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014) | ISO/IEC 17789:2014, *Information technology – Cloud computing – Reference architecture*.

[ITU-T Y.3600] Recommendation ITU-T Y.3600 (2015), *Big data – Cloud computing based requirements and capabilities*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 activity [ITU-T Y.3502]: A specified pursuit or set of tasks.

3.1.2 big data [ITU-T Y.3600]: A paradigm for enabling the collection, storage, management, analysis and visualization, potentially under real-time constraints, of extensive datasets with heterogeneous characteristics.

NOTE – Examples of datasets characteristics include high-volume, high-velocity, high-variety, etc.

3.1.3 big data as a service (BDaaS) [ITU-T Y.3600]: A cloud service category in which the capabilities provided to the cloud service customer are the ability to collect, store, analyse, visualize and manage data using big data.

3.1.4 cloud computing [b-ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

3.1.5 cloud service [b-ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.6 cloud service customer (CSC) [b-ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

3.1.7 cloud service partner (CSN) [b-ITU-T Y.3500]: Party which is engaged in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer, or both.

3.1.8 cloud service provider (CSP) [b-ITU-T Y.3500]: Party which makes cloud services available.

3.1.9 functional component [ITU-T Y.3502]: A functional building block needed to engage in an activity, backed by an implementation.

3.1.10 metadata [b-ISO/IEC 2382]: Data about data or data elements, possibly including their data descriptions, and data about data ownership, access paths, access rights and data volatility.

3.1.11 **party** [b-ITU-T Y.3500]: Natural person or legal person, whether or not incorporated, or a group of either.

3.1.12 **role** [ITU-T Y.3502]: A set of activities that serves a common purpose.

3.1.13 **sub-role** [ITU-T Y.3502]: A subset of the activities of a given role.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

BDaaS Big Data as a Service

BDAP Big Data Application Provider

BDIP Big Data Infrastructure Provider

BDSU Big Data Service User

CSC Cloud Service Customer

CSN Cloud Service Partner

CSP Cloud Service Provider

DP Data Provider

OSS Operations Support Systems

5 Conventions

This Recommendation follows the conventions regarding the diagrams shown in Figure 5-1 of [ITU-T Y.3502].

6 Overview of BDaaS functional architecture

Big data as a service (BDaaS) is a cloud service category, which provides cloud service customers (CSCs) the ability to collect, store, analyze, visualize and manage data using a big data paradigm. BDaaS services utilize capabilities of the cloud computing infrastructure, platform and applications, which are necessary to build a big data ecosystem.

6.1 Framework of BDaaS functional architecture

BDaaS provides big data services based on a cloud service environment. The BDaaS functional architecture defined in this Recommendation follows the concept of constructing the user view, the functional view and aspects defined in [ITU-T Y.3502]. The user view and functional view are specified as follows:

– user view: The system context, parties, roles, sub-roles and cloud computing activities;

– functional view: The functions necessary for the support of cloud computing activities.

The user view and requirements of BDaaS are defined in [ITU-T Y.3600].

This Recommendation defines:

– functional components required for the functional view based on the requirements in [ITU-T Y.3600];

– cross-cutting aspects for BDaaS.

6.1.1 User view for BDaaS architecture

The user view of BDaaS (See [ITU-T Y.3600]) identifies the system context including roles, sub-roles and activities as well as data and service flows as shown in Figure 6-1.

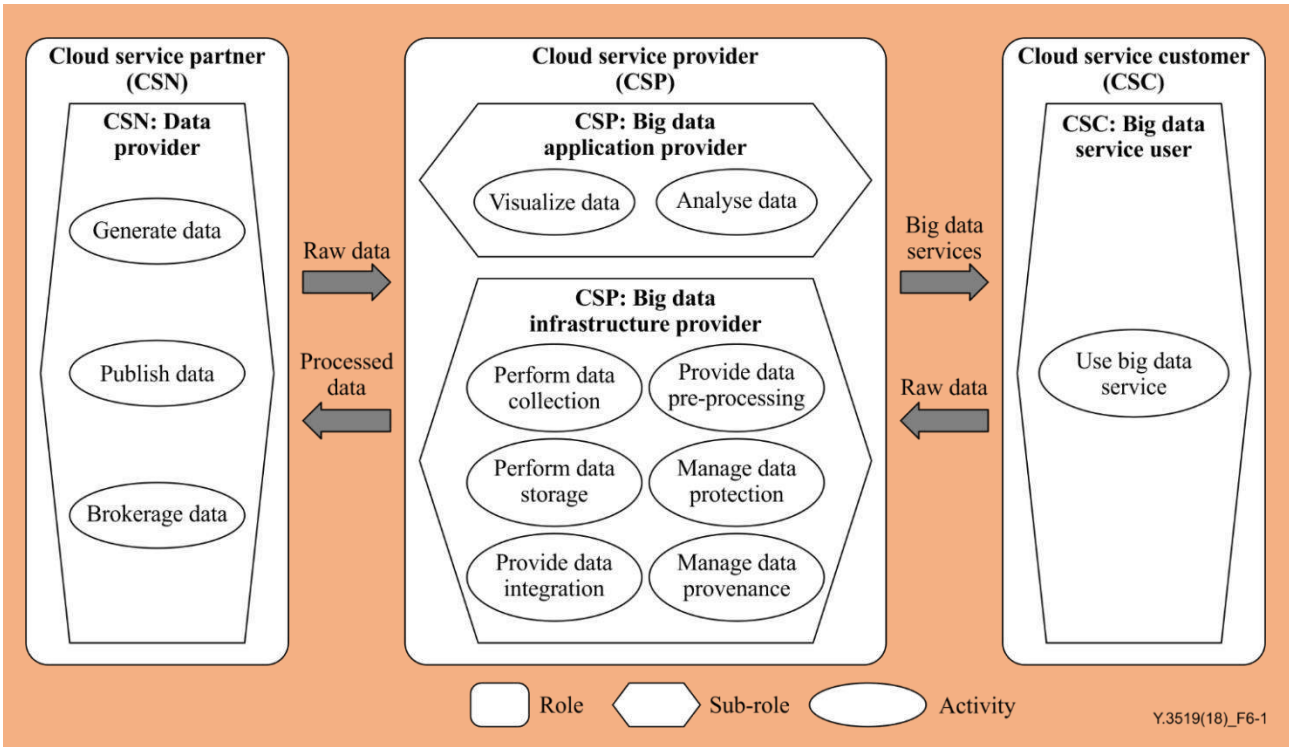


Figure 6-1 – Cloud computing based big data system context

6.1.2 Functional view for BDaaS

The functional architecture of cloud computing in [ITU-T Y.3502] describes functional components in terms of a layering framework where specific types of functions are grouped into each layer and where there are interfaces between the functional components in successive layers.

The functional components for BDaaS represent sets of functions that are necessary to perform the BDaaS activities for various roles and sub-roles.

6.1.3 Cross-cutting aspects for BDaaS

Cross-cutting aspects include both architectural and operational considerations. Cross-cutting aspects for BDaaS apply to multiple elements within the description of the functional architecture or in connection with its operation as an instantiated system. These cross-cutting aspects for BDaaS are shared issues across roles, activities and functional components.

6.2 Relationship between user view and functional view

Figure 6-2 illustrates the relationship between the user view and functional view for BDaaS.

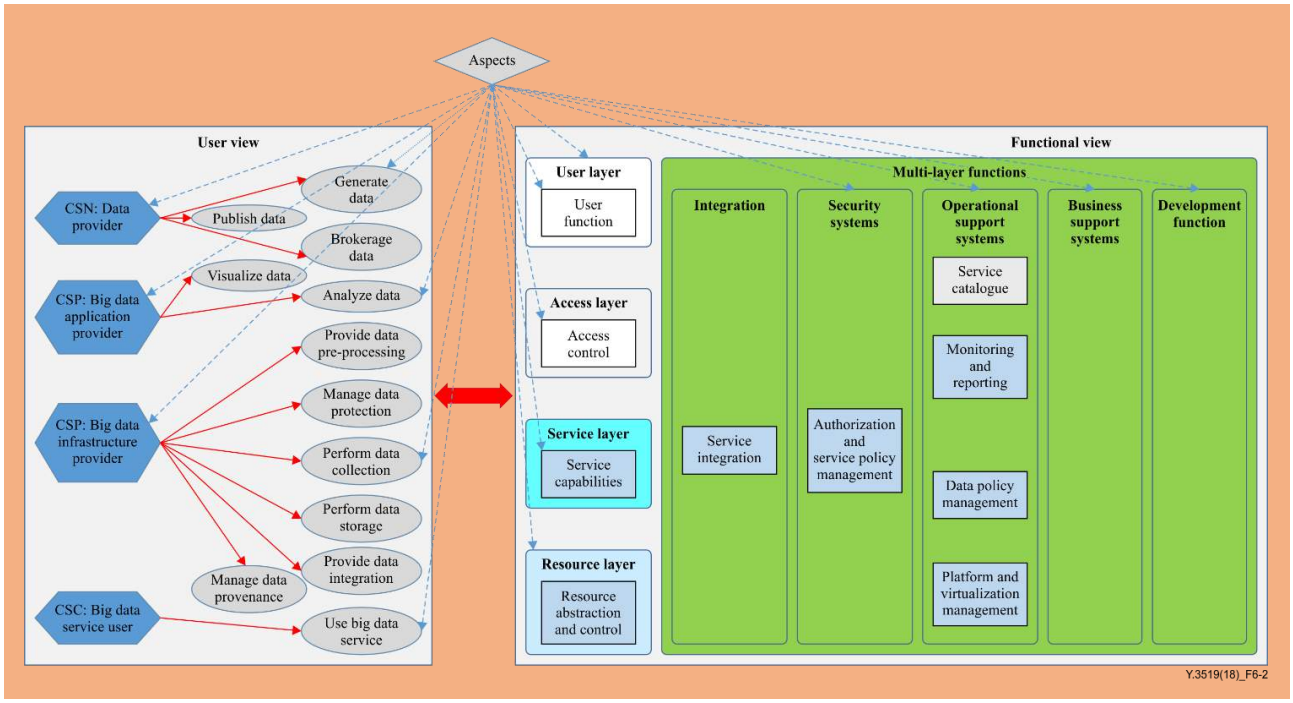


Figure 6-2 – Relationship between user view and functional view

In terms of user view, 4 sub-roles and 12 activities are defined in [ITU-T Y.3600]. These activities in the user view are supported by functional components in the functional view. Clause 7 identifies the functional components needed for support of the activities and of the requirements defined in [ITU-T Y.3600].

NOTE – Appendix I provides the mapping between requirements, activities and functional components.

7 Functional architecture for BDaaS

This clause defines the functional architecture for support of the BDaaS cloud service category. The functional architecture is identified on the basis of the analysis of requirements and capabilities of cloud computing based big data described in [ITU-T Y.3600].

According to the cloud computing layering framework [ITU-T Y.3502], the functions in the cloud computing functional architecture are divided into four layers and a division called multi-layer functions, which spans across the four layers.

Following the methodology of [ITU-T Y.3502], the BDaaS functional architecture is described from a set of functional components. The functional components consist of sets of functions that are required to perform BDaaS activities for the roles and sub-roles described in [ITU-T Y.3600].

Figure 7-1 shows the functional architecture for BDaaS. The BDaaS architecture is defined by leveraging cloud computing reference architecture (CCRA) ([ITU-T Y.3502]) with:

– extensions to the existing functional components;

– adding new functional component.

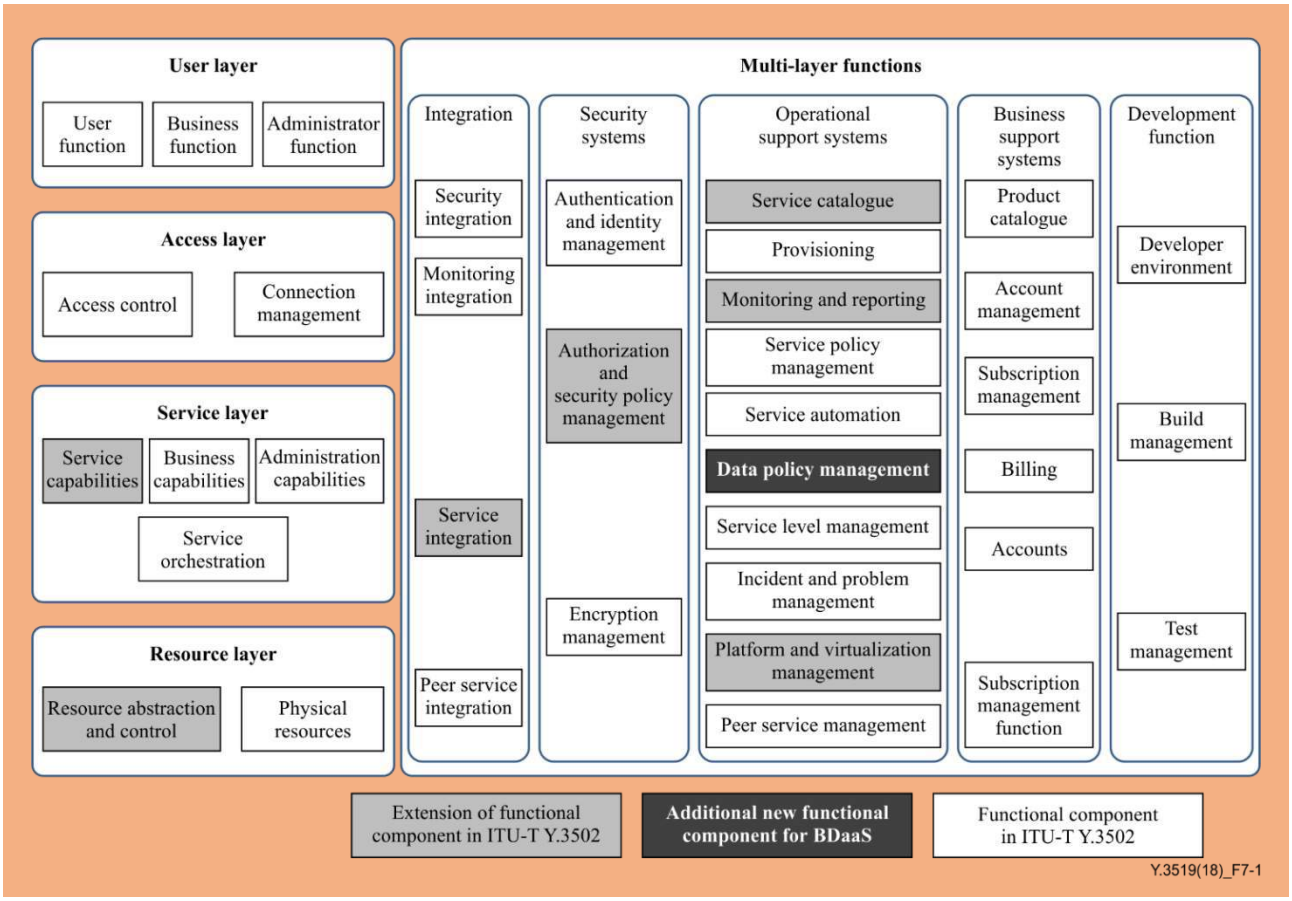


Figure 7-1 – Functional architecture for BDaaS

7.1 Service layer functional components

The service layer functional components for BDaaS (see Figure 7-2) include:

– data collection functional component (see clause 7.1.1);
– data visualization functional component (see clause 7.1.2);
– data pre-processing functional component (see clause 7.1.3);
– data analysis functional component (see clause 7.1.4);
– data storage functional component (see clause 7.1.5).

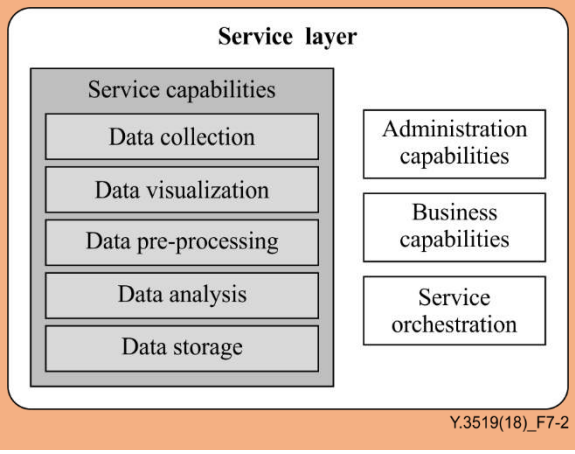


Figure 7-2 – Service capabilities functional components extended for BDaaS

7.1.1 Data collection functional component

The data collection functional component performs data collection based on various data collection configurations. The data collection functional component provides:

– setting up various data collection configurations, such as data amount, traffic volume, collection period, collection method;

NOTE 1 – Examples of collection methods include crawling, rich site summary collecting, log /sensor collecting.

NOTE 2 – Rich site summary is used to aggregate syndicated web content, such as online newspapers, blogs, podcasts and video blogs in one location.

NOTE 3 – Crawling is used to gather data from the world wide web, especially web indexing.

NOTE 4 – Log collecting is used to collect data from log files generated by web servers.

– gathering data based on established configurations of data collection. The collected data is stored in an appropriate storage according to the data type.

7.1.2 Data visualization functional component

The data visualization functional component makes data more intuitive and easier to understand for big data service users (e.g., CSC: big data service user (BDSU)) by using various data visualization tools. It also supports multiple user interactive reporting tools.

This functional component provides:

– presenting data with multiple styles such as statistical graphics, forms, diagrams, charts and reports;

– reporting tools that can be configured by CSC:BDSU.

7.1.3 Data pre-processing functional component

The data pre-processing functional component is responsible for preparing data for further processing such as data analysis. This functional component provides support for data cleaning, data integration, data transformation, data discretization and data extraction to improve data analysis efficiency.

This functional component provides:

– cleaning data which includes processing smoothing noise data, and identifying and removing outliers to improve data quality;

NOTE – Outlier refers to abnormal data in a dataset. If it is not trimmed out, data quality may be damaged.

– combining and integrating data from multiple sources to remove duplicated and redundant data;

– transforming the data collected in different formats and types;

– converting continuous data into discrete interval data;

– extracting the representative features from a large number of data features for data analysis.

7.1.4 Data analysis functional component

The data analysis functional component is responsible for extracting useful information or valuable insights from big data. This functional component provides support for multiple data analysis methods. This functional component also supports customization of specific analysis methods.

This functional component provides:

– registration of data analysis methods which are used for data analysis. Typical Data analysis methods are classification analysis, clustering analysis, association analysis, regression analysis, customized analysis, etc.;

NOTE 1 – Classification analysis: This supports decision tree, support vector machine, neural networks and other algorithms, to identify to which set of categories data belongs.

NOTE 2 – Clustering analysis: This supports k – means, k – center point, overlapping clustering, fuzzy clustering, etc., to classify data into different classes or clusters according to their similarity.

NOTE 3 – Association analysis: This supports some specific algorithms to find associations between stored data. Examples of association algorithms include Apriori algorithm and Frequent Pattern Growth algorithm. Apriori algorithm and Frequent Pattern Growth algorithm are two classical association analysis algorithms which can mine the associations through the frequency of data appearing together in the dataset.

NOTE 4 – Regression analysis: This supports linear regression and logistic regression and other algorithms, for estimating the relationships among data.

NOTE 5 – Customization of analysis supports the customization of detail data analysis methods according to a customer's specific requirements.

– setting up procedures which enable the analysis using registered analysis methods in the analysis function registry;

– executing analysis process according to the procedures.

7.1.5 Data storage functional component

The data storage functional component is responsible for storing data. This functional component also provides different types of storage for different data types and different database types while storing data.

This functional component provides:

– provisioning storage considering the various types of data storage, database, and different types of data such as structured data, unstructured data, and semi-structured data;

NOTE 1 – Data storage types include block storage, file storage and object storage.

NOTE 2 – Databases include Relation database, No SQL database.

NOTE 3 – Unstructured data can include mass data, such as log files, video, audio data, email, Web pages, data generated on social-media sites. Semi-structured data can include data stored in XML, HTML and other format documents. Structured data can include record data persistent in databases (see [ITU-T Y.3600]).

– allocating the appropriate storage when a storage usage request is initiated;

– releasing storage when the storage usage is terminated;

NOTE 4 – The data storage functional component interworks with the data collection functional component (see clause 7.1.1) to identify the characteristics of the data such as data type, data volume and so on.

– storing data on various storage systems. It supports storage mirroring and provides data fragmentation to distribute and store data on distributed storage systems. This provides the ability to update data;

NOTE 5 – Distributed storage system stores data on multiple independent storages. It adopts the scalable system structure, and uses multiple storage servers which are used to share the storage load.

NOTE 6 – Storage mirroring is the replication of logical storage volumes onto separate physical disks.

– data indexing, stored together with data, to improve the speed of data retrieval operations.

7.2 Resource layer functional components

The resource abstraction and control functional component, in the resource layer functional components, is extended for BDaaS (see Figure 7-3) with the following functional components:

– distributed processing functional component (see clause 7.2.1).

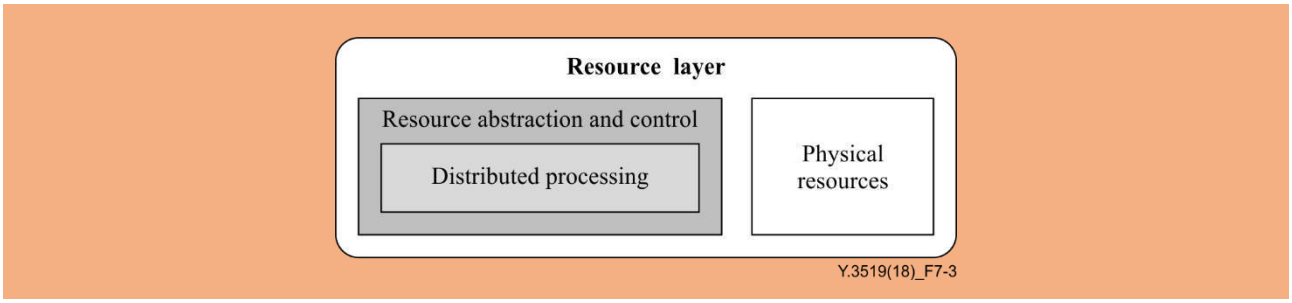


Figure 7-3 – Resource abstraction and control functional component extended for BDaaS

7.2.1 Distributed processing functional component

The distributed processing functional component is responsible for processing data by the distributed cluster resources. This functional component provides distributed computing, as well as storage options for intermediate or final processing results to satisfy the requirements of different data types and scenarios.

This functional component supports:

– processing data by the distributed cluster resources with each node containing pieces of whole datasets and processing that data locally in parallel, and write the intermediate or final processing results to file system or memory cache;

NOTE – Cluster resources refer to the physical or virtual servers of the distributed processing cluster.

– processing data by the distributed cluster resources with nodes organizing into logical topology where data flows through.

7.3 Multi-layer functional components

7.3.1 Integration functional components

The service integration functional component, in the integration functional components, is extended for BDaaS (see Figure 7-4) with the following functional components:

– third-party service integration functional component (see clause 7.3.1.1).

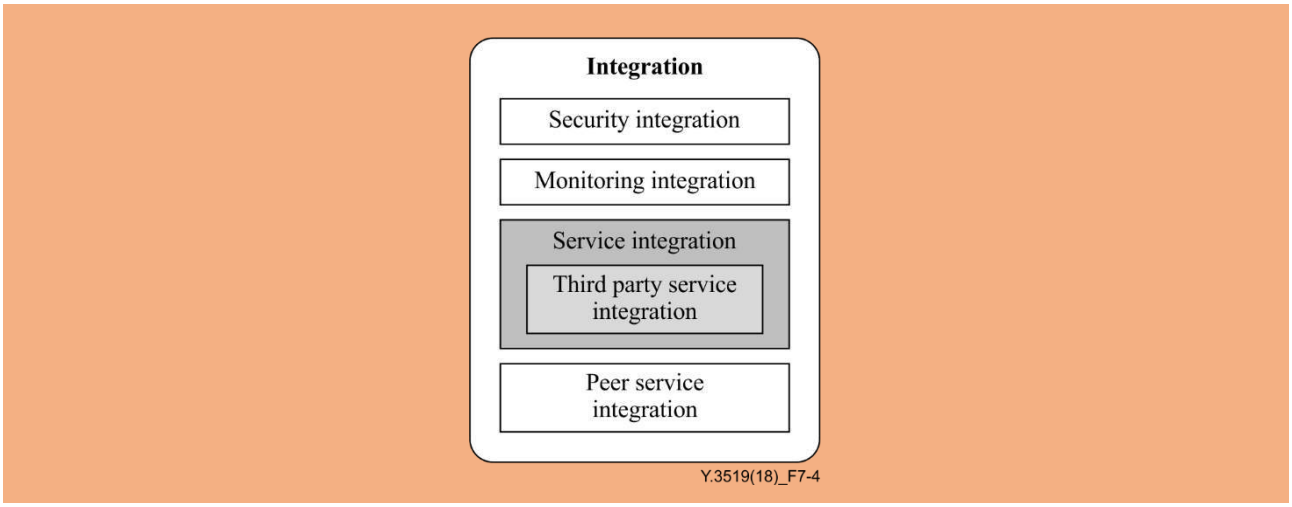


Figure 7-4 – Service integration functional component extended for BDaaS

7.3.1.1 Third-party service integration functional component

The third-party service integration functional component supports the development of service implementation tools which assist in modifying and adapting the service from a set of third-party services.

This functional component supports:

– integrating multiple big data services;

– integrating third-party services with operational systems, as well as reporting tools or systems;

– integrating, adjusting and optimizing user-defined algorithms.

7.3.2 Security systems functional components

The authorization and security policy management functional component, in the security systems functional components, is extended for BDaaS (see Figure 7-5) with the following functional components:

– security and privacy management functional component (see clause 7.3.2.1).

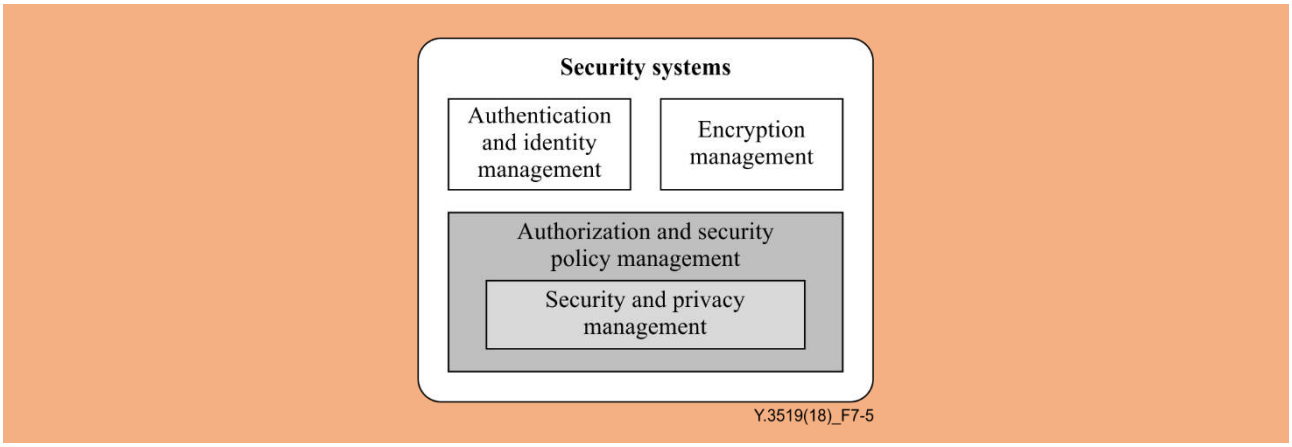


Figure 7-5 – Authorization and security policy management functional component extended for BDaaS

7.3.2.1 Security and privacy management functional component

The security and privacy management functional component is responsible for managing data provenance, personal information in data and user access authority. This functional component aims to avoid data being collected, stored by or disclosed to those who are not appropriate.

This functional component provides:

– the capability to manage identification and authorization so that only authenticated and authorized users shall access the data;

– methods to protect the privacy of confidential data and sensitive data. For example, this function supports data desensitization to protect the sensitive data.

NOTE 1 – Confidential data refers to provide for protection of data from unauthorized disclosure. (see [b-ITU-T X.509]).

NOTE 2 – Sensitive data refers to personally identifiable information or other sensitive information which is collected, stored, used, and finally destroyed or deleted.

7.3.3 Operational support systems functional components

The operational support system functional components are extended for BDaaS (see Figure 7-6) with the following functional components:

– data life-cycle monitoring functional component (see clause 7.3.3.1);

– data policy management functional component (see clause 7.3.3.2);

– data catalogue functional component (see clause 7.3.3.3);

– resource orchestration functional component for Big data (7.3.3.4).

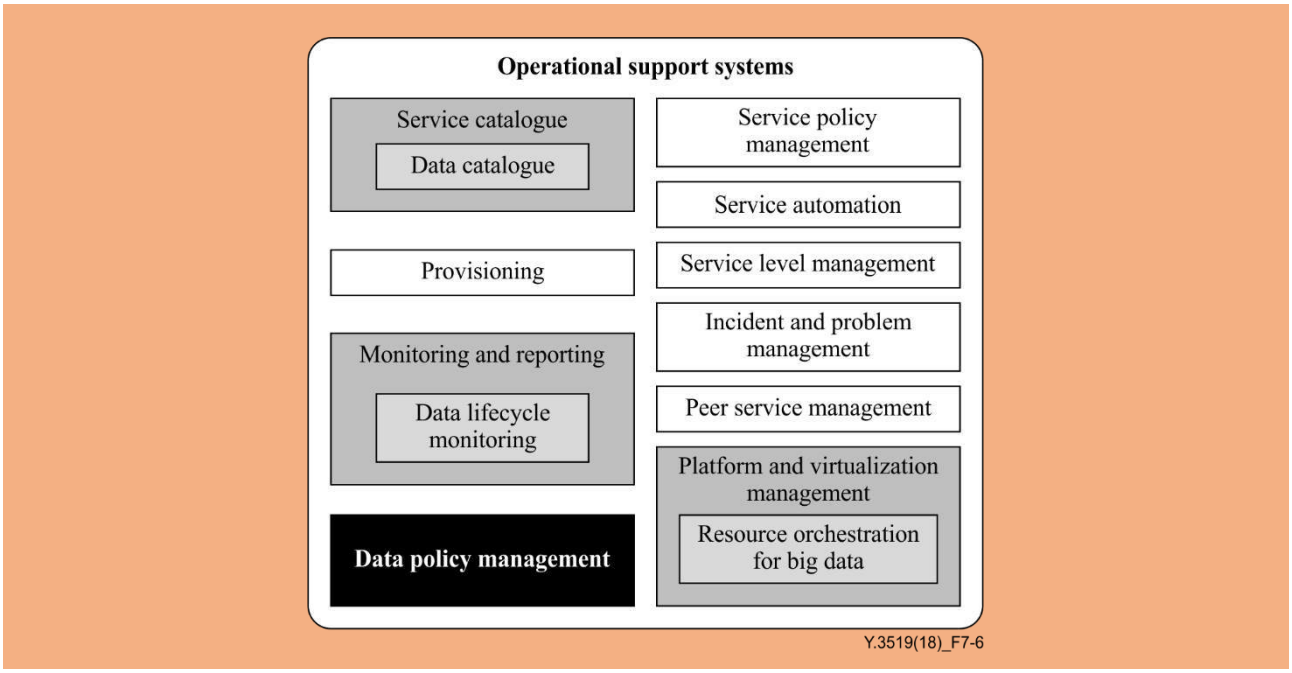


Figure 7-6 – Operational support systems functional components extended for BDaaS

7.3.3.1 Data life-cycle monitoring functional component

The data life-cycle is a sequence of steps from the initial creation or capture of the data to the final archive and/or deletion at the end of its useful life. The data life-cycle monitoring functional component is responsible for monitoring data availability, preservation and usage frequency during the entire data life-cycle from creating, storing, using, sharing, archiving, and destroying data.

This functional component is responsible for:

– monitoring data availability-related information such as expiration date, sensitivity level and sharing right of data;

– monitoring data preservation-related information (e.g., created time) and operation (e.g., data creation and data deletion). The monitoring results guide the data archive, deletion and recovery based on data preservation policy. For example, if archived data have expired, it needs to be deleted;

– checking the frequency of data usage. According to the different frequency of data usage, data processing and data management schemes are adjusted in the process of data life-cycle. For example, in the data storage process, data that are accessed more frequently will be stored on faster, but more expensive storage media, while less critical data will be stored on cheaper, but slower media.

7.3.3.2 Data policy management functional component

The data policy management functional component is responsible for creating, modifying and deleting data policies, such as data provenance sharing policy, data license policy and data preservation policy. The BDaaS service provider applies data policies to the processes of data collection, data processing, data storage, etc.

This functional component provides:

– the ability to create data policies, such as the creation of data sharing policy, data license policy and data price policy according to various usage requirements. For example, for the transmission of sensitive data, an encrypted transmission policy is created;

NOTE 1 – Data sharing policy is used to determine whether the data source can be shared or not according to the security level of the data.

NOTE 2 – Data license policy is used to set up application conditions, period of validity and authentication method for different licenses.

NOTE 3 – Data price policy is used to set reasonable prices according to data volume, data sources and other conditions. In some cases, data prices should be set by negotiating with data users.

– the ability to check and delete useless policies. For example, if a data policy is updated, obsolete ones need to be deleted;
– the ability to apply data policies to the process of data collection, data processing, data preservation, data storage, etc.

NOTE 4 – Data preservation policy is used to protect and prolong the existence and authenticity of data and its metadata.

7.3.3.3 Data catalogue functional component

The data catalogue functional component is mainly responsible for registering data catalogue, and it also supports searching data by browsing data catalogue. This functional component is a sub-function of the service catalogue functional component defined in [ITU-T Y.3502].

This functional component provides:

– registering a data catalogue to cloud service partner (CSP) for searching the appropriate data. Data catalogue provides data access methods, data use policy, etc.;
– data searching capability that allows browsing of data catalogue and searching data with keywords, application domain, specific data fields, etc.

7.3.3.4 Resource orchestration functional component for big data

BDaaS services are provisioned and maintained over underlying resources which belong to the cloud computing infrastructure, including processing resources, storage resources and network resources. The resource orchestration functional component for big data is responsible for binding, load balancing and scheduling resources provided by service providers (e.g., CSP: big data infrastructure provider (BDIP)) and requested by CSC: BDSU.

This functional component provides:

– resource binding that supports allocating resources related to data processing, data storage and data analysis;
– resource load balancing that enables automated resource movement as workload requirements change;
– resource scheduling that allocates resources to tasks required by big data services, and schedules the start- and end-time of each task according to resource availability.

8 Cross-cutting aspects for BDaaS

Cross-cutting aspects can be shared and can impact multiple roles, cloud computing activities and functional components, as described in [ITU-T Y.3502]. This clause defines cross-cutting aspects for BDaaS.

8.1 Data redundancy

Data redundancy refers to the repeated occurrence of the same data in the system. For example, in a relational database, data redundancy mainly refers to the repeated storage of the same data in the relational database, including repetition of tables, attributes, tuples, and attribute values. Necessary data redundancy can improve the anti-interference ability of data, thus preventing data loss and errors. For example, redundantly encoding data by adding several bits based on the length of the original binary code, to prevent key data loss and errors.

However, data redundancy should be minimized to improve storage space utilization, but in some cases, data redundancy should also be increased appropriately. Data compression and de-duplication are two key technologies to reduce data redundancy.

CSP: big data application provider (BDAP) and CSP: BDIP support reducing unnecessary redundant data and increase useful data redundancy appropriately.

8.2 Performance

Referring to [ITU-T Y.3502], this Recommendation identifies additional performance metrics and indicators relating to the operation of a big data service, such as:

– realtime performance metrics, such as automatic fault tolerance and database extensibility;
– elastic calculation performance indicators, such as connections per second and packets per second;
– storage performance indicators, such as bandwidth and input/output preferences per second;
– data disaster tolerance performance indicators including recovery point indicator.

9 Security considerations

Security aspects for consideration within the cloud computing environment, especially for BDaaS, are addressed by security challenges for CSPs, as described in [b-ITU-T X.1601]. In particular, [b-ITU T X.1601] analyses security threats and challenges, and describes security capabilities that could mitigate these threats and meet the security challenges.

[b-ITU-T X.1631] provides guidelines supporting the implementation of information security controls for CSCs and CSPs. Many of the guidelines guide the CSPs to assist the CSCs in implementing the controls, and guide the CSCs to implement such controls. Selection of appropriate information security controls, and the application of the implementation guidance provided, will depend on a risk assessment as well as any legal, contractual, regulatory or other cloud-sector specific information security requirements.

It is also recommended that the guidelines for CSC data security described in [b-ITU-T X.1641] are considered. It provides generic security guidelines for the CSC data in cloud computing, analyses the CSC data security life-cycle and proposes security requirements at each stage of the data life-cycle.

Appendix I

Mapping between requirements, activities and functional components

(This appendix does not form an integral part of this Recommendation.)

This appendix (see Table I.1) describes the mapping between BDaaS functional requirements, activities (described in [ITU-T Y.3600]) and functional components in this Recommendation. The related layers with [ITU-T Y.3502] are also shown in Table I.1.

Table I.1 – Mapping between requirements, activities and functional components

Requirements in [ITU-T Y.3600]	Activities in [ITU-T Y.3600]	Functional components in this Recommendation	Related layers with [ITU-T Y.3502]
<Clause 8.1 requirement (4)> It is recommended for CSN: data provider (DP) to provide a brokerage service to CSP:BDIP for searching accessible data.	Brokerage data (7.1.1.3)	Data collection functional component (7.1.1)	Service layer
<Clause 8.1 requirement (1)> It is required for the CSP:BDIP to support collecting data from multiple CSN: DPs in parallel.	Perform data collection (7.1.3.1)	Data collection functional component (7.1.1)	Service layer
<Clause 8.1 requirement (3)> It is recommended that the CSP:BDIP supports collecting data from different CSN: DPs with different modes.	Perform data collection (7.1.3.1)	Data collection functional component (7.1.1)	Service layer
<Clause 8.1 requirement (6)> Data collection can optionally be performed by the CSP:BDIP in realtime.	Perform data collection (7.1.3.1)	Data collection functional component (7.1.1)	Service layer
<Clause 8.6 requirement (1)> It is required for the CSP:BDIP to manage metadata information such as creating, controlling, attributing, defining and updating.	Publish data (7.1.1.2)	Data catalogue functional component (7.3.3.3)	Operations support systems (OSS)
<Clause 8.1 requirement (2)> It is recommended for the CSN: DP to expose data to the CSP:BDAP by publishing metadata.	Publish data (7.1.1.2)	Data catalogue functional component (7.3.3.3)	OSS
<Clause 8.3 requirement (5)> It is recommended for the CSN: DP to expose APIs for data delivery.	Perform data storage (7.1.3.2)	Data catalogue functional component (7.3.3.3)	OSS
<Clause 8.1 requirement (4)> It is recommended for the CSN: DP to provide a brokerage service to the CSP:BDIP for searching accessible data.	Brokerage data (7.1.1.3)	Data collection functional component (7.1.1)	Service layer
<Clause 8.1 requirement (5)> It is recommended that the CSP:BDIP integrates data delivered by the CSC and data publicly available.	Brokerage data (7.1.1.3)	Data collection functional component (7.1.1)	Service layer

Table I.1 – Mapping between requirements, activities and functional components

Requirements in [ITU-T Y.3600]	Activities in [ITU-T Y.3600]	Functional components in this Recommendation	Related layers with [ITU-T Y.3502]
<Clause 8.5 requirement (2)> It is recommended that the CSP:BDAP supports different tools or plug-ins with multiple styles of data visualization.	Visualize data (7.1.2.1)	Data visualization functional component (7.1.2)	Service layer
<Clause 8.5 requirement (3)> It is recommended that the CSP:BDAP supports customization of the reporting tools.	Visualize data (7.1.2.1)	Data visualization functional component (7.1.2)	Service layer
<Clause 8.5 requirement (4)> It is recommended that the CSP:BDAP supports integration of reporting tools with the CSC reporting systems.	Visualize data (7.1.2.1)	Data visualization functional component (7.1.2)	Service layer
<Clause 8.5 requirement (5)> It is recommended that the CSP:BDAP supports integration of reporting tools with the CSC operational systems.	Visualize data (7.1.2.1)	Data visualization functional component (7.1.2)	Service layer
<Clause 8.2 requirement (1)> It is required for the CSP:BDIP to support data aggregation.	Provide data integration (7.1.3.4)	Data pre-processing functional component (7.1.3)	Service layer
<Clause 8.2 requirement (2)> It is recommended that the CSP:BDIP provides the dedicated resources for pre-processing.	Provide data pre-processing (7.1.3.3)	Data pre-processing functional component (7.1.3)	Service layer
<Clause 8.2 requirement (3)> It is recommended that the CSP:BDIP supports unification of data collected in different formats.	Provide data pre-processing (7.1.3.3)	Data pre-processing functional component (7.1.3)	Service layer
<Clause 8.2 requirement (4)> It is recommended for the CSP:BDIP to support extraction of data from unstructured data or semi-structured data into structured data.	Provide data pre-processing (7.1.3.3)	Data pre-processing functional component (7.1.3)	Service layer
<Clause 8.1 requirement (2)> It is recommended for the CSN: DP to expose data to the CSP:BDAP by publishing metadata.	Publish data (7.1.1.2)	Data catalogue functional component (7.3.3.3)	Service layer
<Clause 8.3 requirement (5)> It is recommended for the CSN: DP to expose APIs for data delivery.	Perform data storage (7.1.3.2)	Data storage functional component (7.1.5)	Service layer
<Clause 8.4 requirement (1)> It is required for the CSP:BDAP to support analysis of various data types and formats.	Analyze data (7.1.2.2)	Data analysis functional component (7.1.4)	Service layer
<Clause 8.4 requirement (2)> It is required for the CSP:BDAP to support batch processing.	Analyze data (7.1.2.2)	Data analysis functional component (7.1.4)	Service layer

Table I.1 – Mapping between requirements, activities and functional components

Requirements in [ITU-T Y.3600]	Activities in [ITU-T Y.3600]	Functional components in this Recommendation	Related layers with [ITU-T Y.3502]
<Clause 8.4 requirement (3)> It is required for the CSP:BDAP to support association analysis.	Analyze data (7.1.2.2)	Data analysis functional component (7.1.4)	Service layer
<Clause 8.4 requirement (4)> It is required for the CSP:BDAP to support different data analysis algorithms.	Analyze data (7.1.2.2)	Data analysis functional component (7.1.4)	Service layer
<Clause 8.4 requirement (5)> It is recommended that the CSP:BDAP supports customization of analytical applications.	Analyze data (7.1.2.2)	Data analysis functional component (7.1.4)	Service layer
<Clause 8.4 requirement (6)> It is recommended for the CSP:BDAP to support user defined algorithms.	Analyze data (7.1.2.2)	Data analysis functional component (7.1.4)	Service layer
<Clause 8.4 requirement (7)> It is recommended for the CSP:BDAP to support data processing in distributed computing environments.	Analyze data (7.1.2.2)	Data analysis functional component (7.1.4)	Service layer
<Clause 8.4 requirement (9)> It is recommended that the CSP:BDAP supports data classification in parallel.	Analyze data (7.1.2.2)	Data analysis functional component (7.1.4)	Service layer
<Clause 8.4 requirement (10)> It is recommended that the CSP:BDAP provides different analytical applications.	Analyze data (7.1.2.2)	Data analysis functional component (7.1.4)	Service layer
<Clause 8.4 requirement (11)> It is recommended that the CSP:BDAP supports customization of analytical applications.	Analyze data (7.1.2.2)	Data analysis functional component (7.1.4)	Service layer
<Clause 8.4 requirement (12)> It is recommended for the CSP:BDAP to support real-time analysis of streaming data.	Analyze data (7.1.2.2)	Data analysis functional component (7.1.4)	Service layer
<Clause 8.4 requirement (13)> It is recommended for the CSP:BDAP to support user behavior analysis.	Analyze data (7.1.2.2)	Data analysis functional component (7.1.4)	Service layer
<Clause 8.4 requirement (14)> The CSP:BDAP can optionally perform analysis of different data types and formats in realtime.	Analyze data (7.1.2.2)	Data analysis functional component (7.1.4)	Service layer
<Clause 8.6 requirement (2)> It is required for the CSP:BDIP to track a data history which contains source of data and data processing method.	Analyze data (7.1.2.2)	Data analysis functional component (7.1.4)	Service layer

Table I.1 – Mapping between requirements, activities and functional components

Requirements in [ITU-T Y.3600]	Activities in [ITU-T Y.3600]	Functional components in this Recommendation	Related layers with [ITU-T Y.3502]
<Clause 8.3 requirement (1)> It is required for the CSP:BDIP to support different data types with sufficient storage space, elastic storage capacity, and efficient control methods.	Perform data storage (7.1.3.2)	Data storage functional component (7.1.5)	Service layer
<Clause 8.3 requirement (2)> It is required for the CSP:BDIP to support storage for different data formats and data models.	Perform data storage (7.1.3.2)	Data storage functional component (7.1.5)	Service layer
<Clause 8.3 requirement (4)> It is recommended that the CSP:BDIP provides different types of databases.	Perform data storage (7.1.3.2)	Data storage functional component (7.1.5)	Service layer
<Clause 8.4 requirement (8)> It is recommended for the CSP:BDAP to support data indexing.	Perform data storage (7.1.3.2)	Data storage functional component (7.1.5)	Service layer
<Clause 8.4 requirement (7)> It is recommended for the CSP:BDAP to support data processing in distributed computing environments.	Manage data provenance (7.1.3.6)	Data storage functional component (7.1.5)	Service layer
<Clause 8.5 requirement (6)> It is recommended that the CSP:BDAP supports composed services which could combine two or more big data services to the CSC: BDSU.	Use big data service (7.1.4.1)	Third-party service integration functional component (7.3.1.1)	Integration
<Clause 8.4 requirement (6)> It is recommended for the CSP:BDAP to support user defined algorithms.	Analyze data (7.1.2.2)	Data analysis functional component (7.1.4)	Service layer
<Clause 8.7 requirement (2)> It is required for the CSP:BDIP to support data protection.	Manage data protection (7.1.3.5)	Security and privacy management functional component (7.3.2.1)	Security systems
<Clause 8.7 requirement (5)> It is recommended that the CSP:BDIP supports redundancy mechanism and transaction logging.	Use big data service (7.1.4.1)	Cross-cutting aspect (8.1)	Multiple layers for cross-cutting aspect
<Clause 8.7 requirement (1)> It is required for the CSP:BDIP to protect data collection, data storage, data transmission, and data processing with security mechanisms.	Manage data protection (7.1.3.5)	Security and privacy management functional component (7.3.2.1)	Security systems
<Clause 8.3 requirement (6)> It is recommended that the CSP:BDIP fulfils storage and database performance demands.	Perform data storage (7.1.3.2)	Cross-cutting aspect (8.2)	Multiple layers for cross-cutting aspect

Table I.1 – Mapping between requirements, activities and functional components

Requirements in [ITU-T Y.3600]	Activities in [ITU-T Y.3600]	Functional components in this Recommendation	Related layers with [ITU-T Y.3502]
<Clause 8.6 requirement (3)> It is required for the CSP:BDAP to support distributed cluster monitoring tools to monitor the health and status of computing clusters.	–	Distributed processing functional component (7.2.1)	Resource layer
<Clause 8.6 requirement (5)> It is recommended for the CSP:BDIP to support network resource monitoring.	–	Distributed processing functional component (7.2.1)	Resource layer
<Clause 8.3 requirement (3)> It is required that the CSP:BDIP provides flexible licensing policy for the database.	Use big data service (7.1.4.1)	Data policy management functional component (7.3.3.2)	OSS
<Clause 8.3 requirement (7)> It is recommended that the CSP:BDIP supports data retention policy covering data retention period before its destruction after termination of a contract, to protect the big data service customer from losing private data through an accidental lapse of the contract.	Manage data protection (7.1.3.5)	Data policy management functional component (7.3.3.2)	OSS
<Clause 8.7 requirement (4)> It is recommended that the CSP supports implementing the CSC's data protection and security policies over data and analytical results.	Manage data protection (7.1.3.5)	Data policy management functional component (7.3.3.2)	OSS
<Clause 8.7 requirement (3)> It is required that the CSP deletes CSC related data and analytical results according to the lifetime defined by the CSC or on the CSC's demand.	Manage data protection (7.1.3.5)	Data policy management functional component (7.3.3.2)	OSS
<Clause 8.6 requirement (6)> It is recommended for the CSP:BDIP to support management of data life-cycle operations.	–	Data life-cycle monitoring functional component (7.3.3.1)	OSS
<Clause 8.6 requirement (4)> It is required for the CSP:BDIP to support data preservation policy management rules.	–	Data life-cycle monitoring functional component (7.3.3.1)	OSS
<Clause 8.1 requirement (4)> It is recommended for the CSN: DP to provide a brokerage service to the CSP:BDIP for searching accessible data.	Brokerage data (7.1.1.3)	Data collection functional component (7.1.1)	Service layer

Table I.1 – Mapping between requirements, activities and functional components

Requirements in [ITU-T Y.3600]	Activities in [ITU-T Y.3600]	Functional components in this Recommendation	Related layers with [ITU-T Y.3502]
<Clause 8.3 requirement (1)> It is required for the CSP:BDIP to support different data types with sufficient storage space, elastic storage capacity, and efficient control methods.	Perform data storage (7.1.3.2)	Resource orchestration functional component for big data (7.3.3.4)	OSS
<Clause 8.3 requirement (6)> It is recommended that the CSP:BDIP fulfils storage and database performance demands.	Perform data storage (7.1.3.2)	Data storage functional component (7.1.5)	Service layer
<Clause 8.3 requirement (3)> It is required that the CSP:BDIP provides flexible licensing policy for the databases.	Perform data storage (7.1.3.2)	Data policy management functional component (7.3.3.2)	OSS
<Clause 8.4 requirement (5)> It is required that the CSP:BDAP provides a flexible licensing policy for the analytical applications.	Analyze data (7.1.2.2)	Data policy management functional component (7.3.3.2)	OSS
<Clause 8.5 requirement (1)> It is required that the CSP:BDAP provides a flexible licensing policy for the reporting tool.	Publish data (7.1.1.2)	Data policy management functional component (7.3.3.2)	OSS

NOTE – In Table I.1, ''–'' means ''There is no specific activity related to the requirements in [ITU-T Y.3600]''.

Bibliography

[b-ITU-T X.509] Recommendation ITU-T X.509 (2016), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing*.

[b-ITU-T X.1631] Recommendation ITU-T X.1631 (2015) | ISO/IEC 27017:2015, *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services*.

[b-ITU-T X.1641] Recommendation ITU-T X.1641 (2016), *Guidelines for cloud service customer data security*.

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary*.

[b-ISO/IEC 2382] ISO/IEC 2382:2015, *Information technology – Vocabulary*.


SAAS

Security requirements for software as a service application environments

Recommendation ITU-T X.1602

(03/2016)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Summary

Recommendation ITU-T X.1602 analyses the maturity levels of software as a service (SaaS) application and proposes security requirements to provide a consistent and secure service execution environment for SaaS applications. These proposed requirements originate from cloud service providers (CSP) and cloud service partners (CSN) as they need a SaaS application environment to meet their demands on security. The requirements are general and independent of any service or scenario specific model (e.g., web services, or representational state transfer (REST)), assumptions or solutions.

Keywords

Security requirement, software as a service (SaaS) application environment, SaaS maturity level.

Table of Contents

1 Scope

This Recommendation focuses mainly on the security requirements of software as a service (SaaS) application environments based on the SaaS application maturity level. The target audiences of this Recommendation are cloud service providers (CSPs) and cloud service partners (CSNs) such as application developers.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 cloud service [b-ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.2 cloud service category [b-ITU-T Y.3500]: Group of cloud services that possess some common set of qualities.

3.1.3 cloud service customer [b-ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

3.1.4 cloud service partner [b-ITU-T Y.3500]: Party which is engaged in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer, or both.

3.1.5 cloud service provider [b-ITU-T Y.3500]: Party which makes cloud services available.

3.1.6 cloud service user [b-ITU-T Y.3500]: Natural person, or entity acting on their behalf, associated with a cloud service customer that uses cloud services.

3.1.7 desktop as a service [b-ITU-T Y.3500]: The capabilities provided to the cloud service customer are the ability to build, configure, manage, store, execute, and deliver users' desktop functions remotely.

3.1.8 infrastructure as a service (IaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer is an infrastructure capabilities type.

3.1.9 software as a service (SaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer is an application capabilities type.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ASP	Application Service Provider
CaaS	Communications as a Service
CRM	Customer Relationship Management
CSC	Cloud Service Customer
CSN	Cloud Service Partner
CSP	Cloud Service Provider
DaaS	Desktop as a Service

IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IdM	Identity Management
OLAP	OnLine Analytical Processing
OS	Operating System
PaaS	Platform as a Service
PKI	Public Key Infrastructure
REST	Representational State Transfer
SaaS	Software as a Service
SAP	Service Access Point
SLA	Service Level Agreement

5 Conventions

None.

6 Overview

A software as a service (SaaS) application environment is a service-oriented multi-tenant development, deployment and execution environment in which software and its associated data are hosted centrally and are typically accessed on-demand by users using a client, e.g., a web browser, over the Internet.

While this Recommendation is primarily concerned with SaaS, some of the concepts in this Recommendation may also be applicable to other cloud service categories that also include the application capabilities type, for example communications as a service (CaaS).

Figure 1 depicts a conceptual model of a SaaS application environment. The underlying capabilities from infrastructure as a service (IaaS), platform as a service (PaaS) and desktop as a service (DaaS) will be encapsulated into services and provide consistent secure access using exported service access point (SAP). In this Recommendation, IaaS could provide computing services, storage services and network services; PaaS could provide platform service, and DaaS could provide desktop service for a SaaS application environment. All these services constitute the basic building blocks of an application development.

The environment also provides some necessary service management functions including service registration, service configuration, service orchestration, service dependency checking, service access control, service isolation, service monitoring and other service control functions.

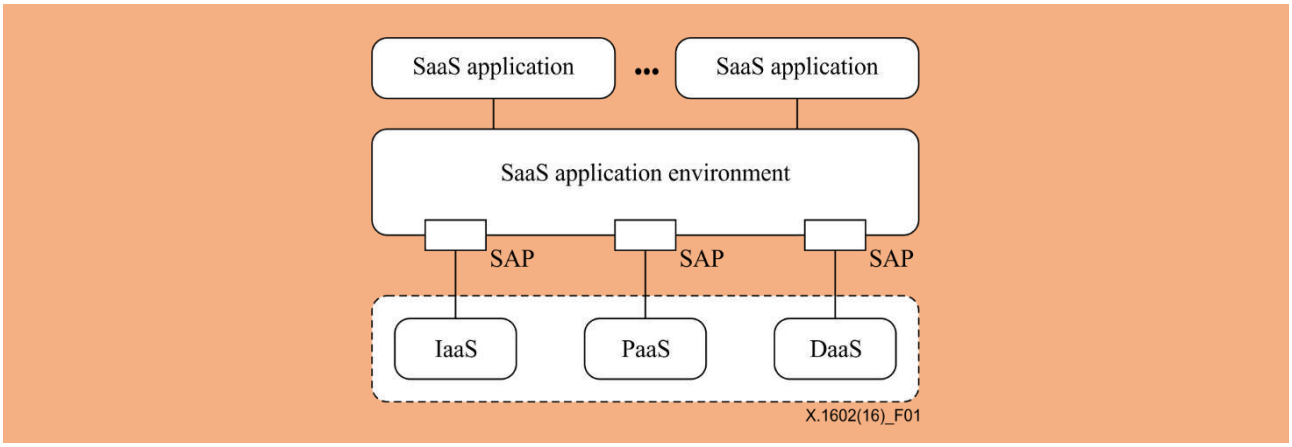
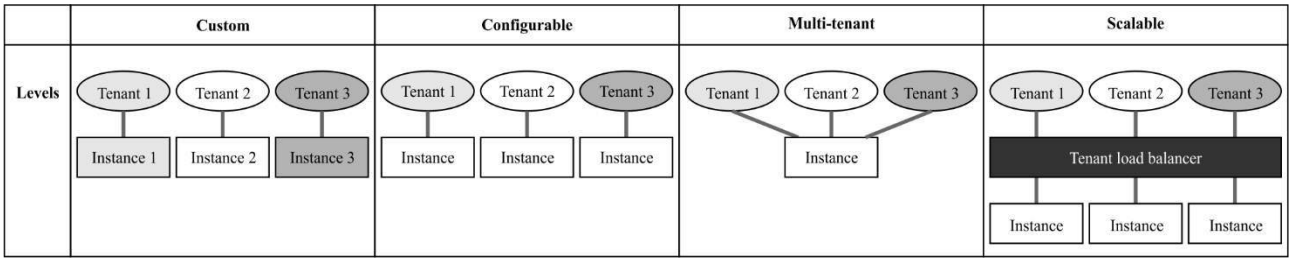


Figure 1 – Conceptual model for the SaaS application environment

7 Maturity levels of SaaS application

In the industry, the maturity of SaaS is classified into four levels which could be shortly named as custom level, configurable level, multi-tenant level, and scalable level. Each level covers characteristics of the previous one and provides extended characteristics. The diagram that represents the characteristics of the different SaaS maturity models is shown in Table 1.

Table 1 – Diagram of SaaS application maturity level



Different maturity levels of the SaaS application have different security requirements to SaaS application environments, and the requirements will be illustrated from the viewpoint of CSPs and CSNs in clause 8.

7.1 Level 1: Custom SaaS application

Custom SaaS application is similar to the traditional application service provider (ASP) model of software delivery. Each customer has its own customized solution for SaaS application and runs its individual application instance on the cloud server. As illustrated in Figure 2, the custom application instance comprises the whole execution environment including the operating system (OS), the data management system and the middleware that are specific to each tenant, and the SaaS environment provider has to maintain multiple instances. This model is difficult to scale in order to satisfy the increasing requirement demands of customers, and it can be costly to operate.

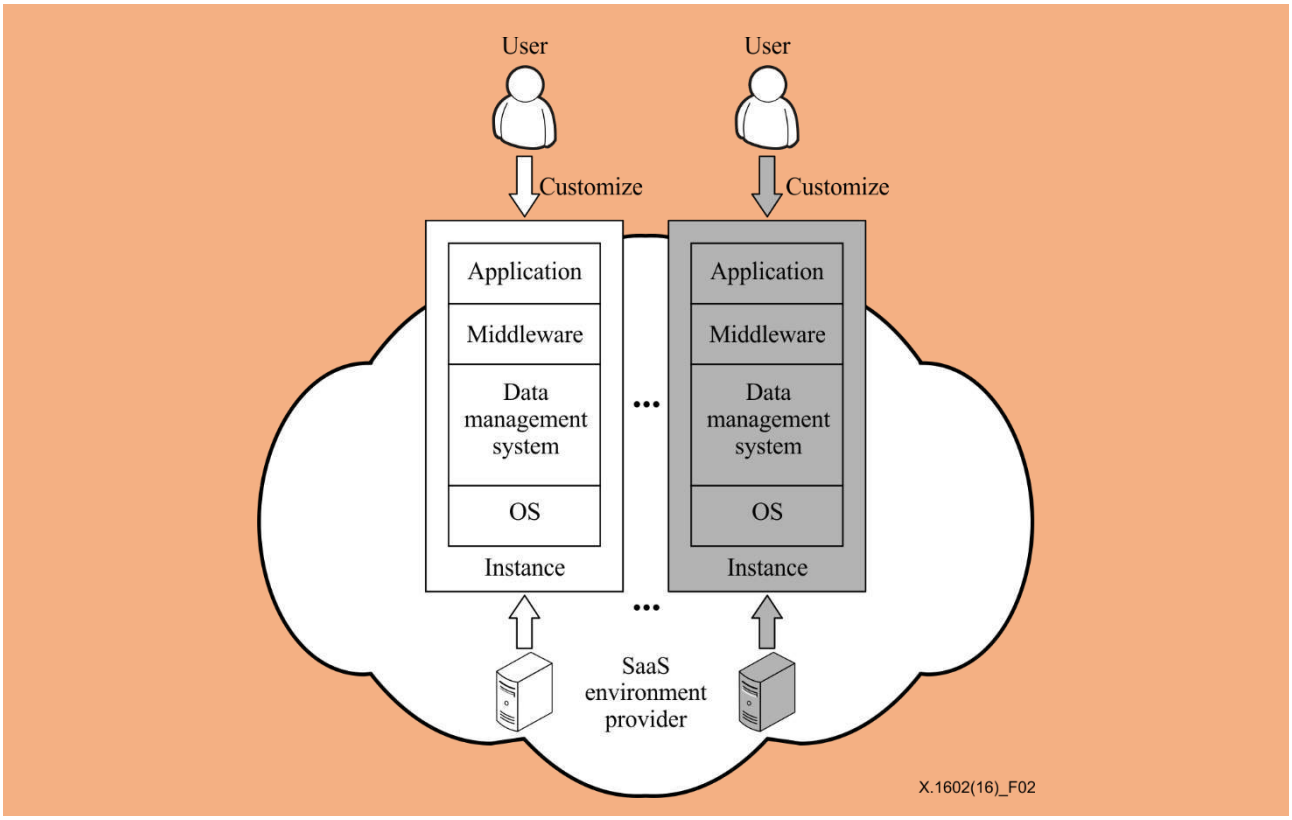


Figure 2 – Architecture of custom SaaS application

The typical client-server model applications can be easily transformed into custom SaaS applications by moving servers to the cloud with relatively little modification. The applications suitable for this scenario are usually developed with special requirements from the enterprise or organization. Top consideration will be given to security in the system itself, thus the usual way is to group a set of physical machines into a private zone and to deploy a data management system (which provides abstracted methods of persistence and operations for different kinds of data) and associated software on it. The system is solely for internal usage with strict access control. The template of application instance is the same for all customers, and it provides limited configuration ability. However, the instance for each customer is totally independent of any other instance.

7.2 Level 2: Configurable SaaS application

For some commonly used applications that are not customized, such as self-service website building system, SaaS application providers offer common templates for these applications and several sets of run-time environment for the instances of these applications. Based on the same template, customers are able to create multiple separated instances of the application by configuring the application's appearance and behaviour, which are deployed and executed on individual virtual or physical machines to meet their customized requirements. Application instances are isolated from each other. The architecture is shown in Figure 3.

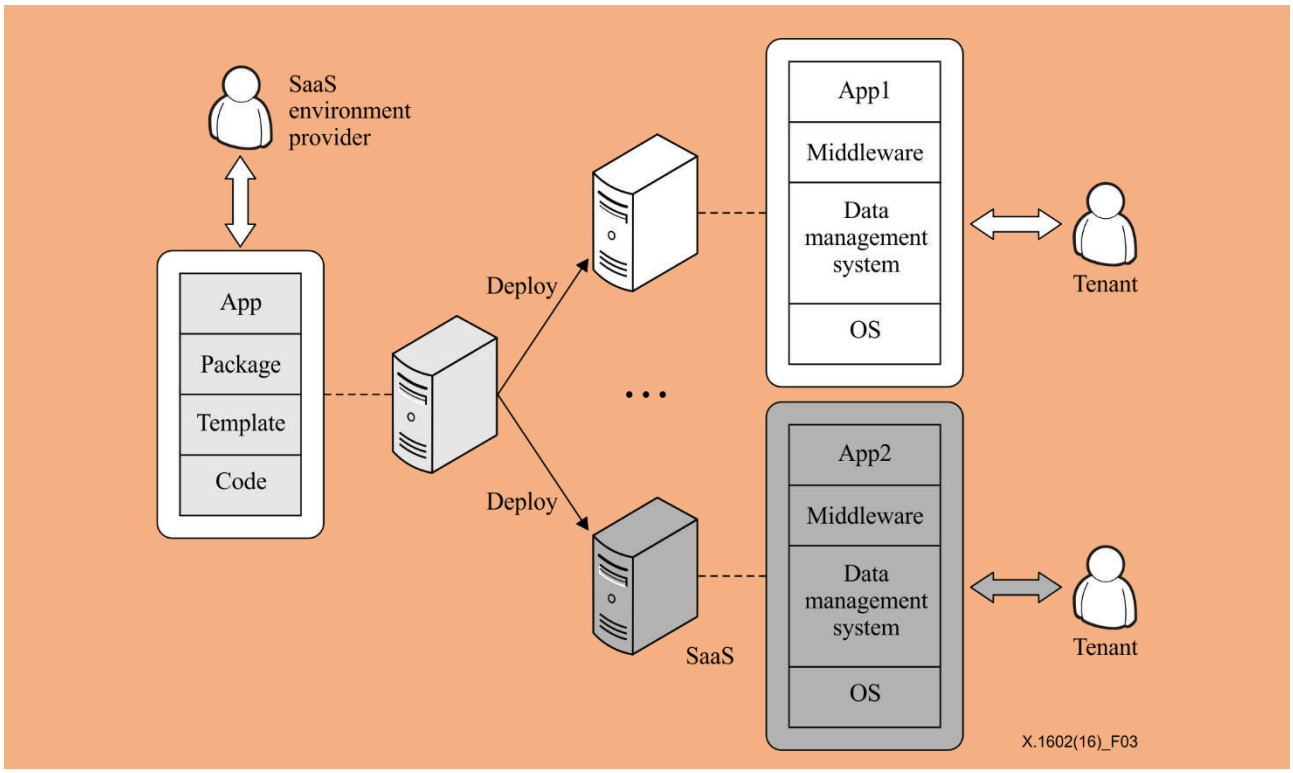


Figure 3 – Architecture of configurable SaaS application

The configurable SaaS application has the following characteristics:

1) Application in the initial deployment is a copy of a standard product, and tenants configure the application to suit their own requirements. However, the configuration options of the product are limited.

2) For SaaS application providers, any modifications to the product codes can be easily applied to all tenants immediately. However, only a little update or optimization to the product codes are suitable for each instance because the forward compatibility problem incurred by the update or optimization may occur.

3) Tenants store data in their own virtual machines or physical machines, which are isolated from each other. As a result, the SaaS environment provider has to provide sufficient resources such as storage to support a potentially large number of application instances running concurrently.

With the development and improvement of software technology, the application will be provided with enough configuration options to meet the users' customized requirements, and the configuration and usage process should be more intelligent and automated. SaaS application providers will divide the products into different versions to match different tenant levels.

7.3 Level 3: Multi-tenant SaaS application

In this level, with the help of configurable metadata, a SaaS application provider is able to provide a single instance that serves multiple tenants concurrently. The multi-tenancy can be enabled at different layers including OS, the data management system, middleware and application. A tenant identifier is introduced to distinguish between the different customers. When a database is used in a data management system, the database schema is extended to include tenant identity parameter for storing all customers' data into the same set of tables. A tenant identity is also needed in database queries in order to retrieve data for a specified customer. Figure 4 illustrates the general architecture of multi-tenant SaaS application.

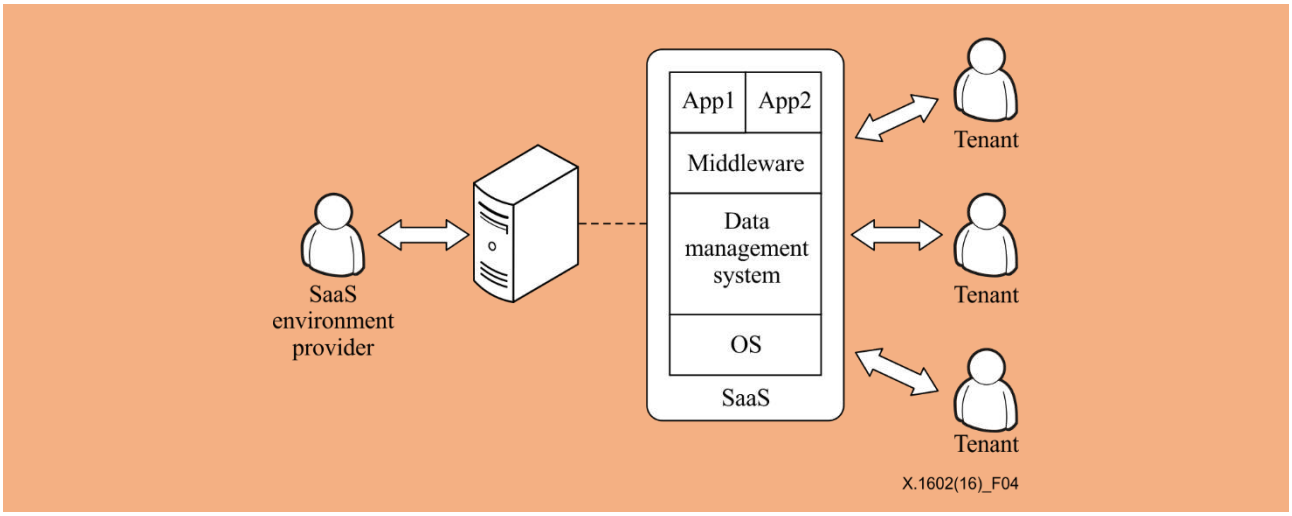


Figure 4 – Architecture of multi-tenant SaaS application

Business intelligence SaaS, for example customer relationship management (CRM), is considered to be a typical implementation of this level. Until now, more efforts have been taken to combine data warehousing and cloud computing with SaaS in order to provide online business intelligence applications. Data warehouse are hosted in the data centre, and business intelligence applications and the data models are predefined to use with very little customization. For the tenants, all they need to do are selecting the data elements required by business intelligence applications and defining the data mapping from data sources to the data warehouse and data model. The system will integrate data from multiple source systems into data warehouse to support the online analytical processing (OLAP) applications by using automatically generated scripts. Usually in the run time, a single instance of business intelligence application serves multiple tenants concurrently by using metadata techniques. Authorizations and security policies ensure that each customer's data and application access are isolated from that of other customers.

This level provides much more efficiency in the use of computing and storage resources, and therefore can be able to accommodate more tenants. It is also possible to achieve comparable performance, scalability and elasticity with the help of data partitioning and parallel techniques.

Configurability and multi-tenant efficiency are the distinctive characteristics for this level of SaaS application.

7.4 Level 4: Scalable SaaS application

Most public web service providers serve an arbitrarily large number of customers as multiple tenants. Consequently, each layer of the underlying platform architecture, from hardware to application, is required to be easily scalable for applications and services as shown in Figure 5. Hence, more tenants and more per-tenant users can be added without requiring additional re-architecting of the applications.

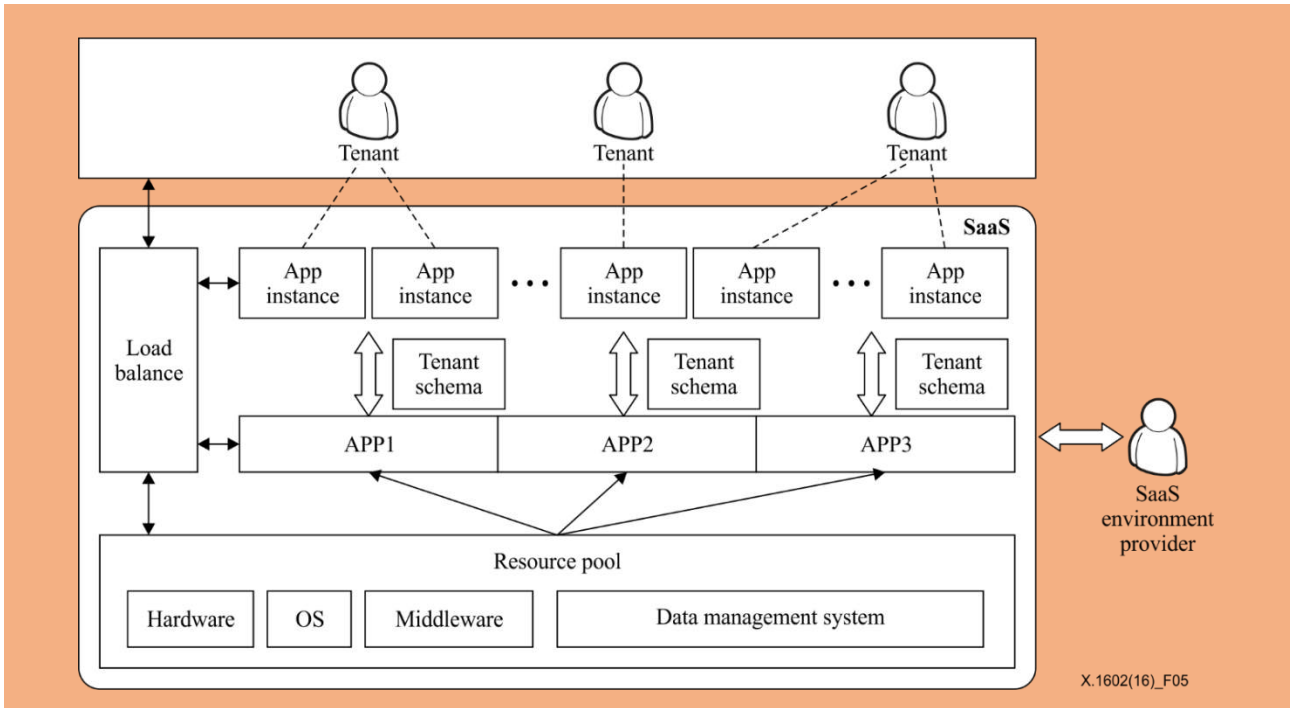


Figure 5 – Architecture of scalable SaaS application

For the application layer, when there is a new tenant, one or more application instances will be generated according to the tenant-specific requirements, or a suitable existing instance will be chosen in accordance with the requirement based on load balance mechanism. All the instances of the applications in such an environment are required to be created dynamically.

The underlying resources of scalable SaaS applications also support elastic scaling. Any hardware, middleware, software, and data are needed to be managed in the resource pool. The applications get all resources they need from the resource pool dynamically. New resources can be added without any recombination or re-architecting when needed.

There are multiple design considerations about the dynamic scaling technologies, including scaling choices, resource allocation, the service level agreement (SLA), etc. A new tenant can be executed as a single instance or can coexist with other tenants on a shared instance. Different instances, which run different types of tenants, can be allocated to varied resources. The SaaS environment provider should consider different SLAs for different tenants when using load balance and shared resources.

8 Security requirements for SaaS application environment

Figure 6 shows the relationship among the cloud service customer (CSC), CSP and CSN with respect to the SaaS application environment, in which CSP and CSN play different roles in performing different functions. CSN can serve CSP as a content provider, software provider, system integrator or auditor, while both CSN and CSP can develop applications for CSC. CSP and CSN have interfaces with the SaaS application environment, while CSC only interacts with applications built upon it. As a result, this Recommendation focuses mainly on the security requirements of the SaaS application environment for CSP and CSN in a different maturity model. The security requirements for the SaaS application environment originate from CSP and CSN as they need a SaaS application environment to have the capability to meet their demands on security.

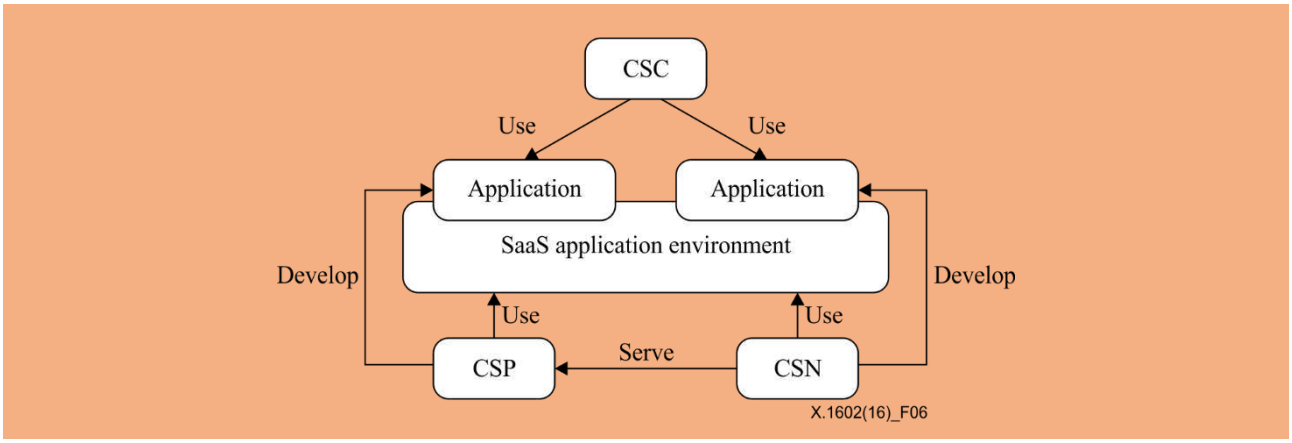


Figure 6 – Relationship among CSC, CSP and CSN

CSP and CSN have their own security requirements about the environment in different levels of SaaS. Table 2 illustrates the security requirements of CSP and CSN in the SaaS application environment. The requirements applicable for both CSP and CSN are the common requirements.

Table 2 – Security requirements of CSP and CSN in SaaS application environment

	SaaS application environment
Common requirements	Identity and access management, data security, security assessment and audit, interface security, security hardening.
CSP	Availability, service interoperability/portability guarantee, software assets protection, legal compliance, security verification for source codes.
CSN	Audit security, software security, software maintainability.

8.1 Common security requirements

For both CSP and CSN, they have several common security requirements in the SaaS application environment.

8.1.1 Identity and access management (IAM)

8.1.1.1 Identity management (IdM)

Multiple administrators and users are involved in the SaaS application environment, which can be accessed to and used internally (CSPs) and externally (CSNs). Identity Management (IdM) is needed not only to protect identities, but also to facilitate access management, authentication, authorization and transaction audit processes in such a dynamic and open SaaS application environment.

For all maturity models, IdM should enable the implementation of single sign-on and/or identity federation for the SaaS application environment using varied authentication mechanisms in different security domains.

8.1.1.2 Trust model

The SaaS application environment is required to incorporate an overall trust model for both multi-tenant level and scalable level. This trust model will enable the creation of islands and/or federations of trusted entities. Consequently, the SaaS application environment management system, the underlying resources, hypervisors, virtual machines and applications built upon the SaaS application environment will be able to authenticate the identities and authorized rights of other entities and components. Each island or federation of trust will be based on one or more trusted authorities (e.g., a public key infrastructure (PKI) certificate authority).

8.1.1.3 Access management

SaaS application environment administrators are required to provide mechanisms, which delegate authorization to tenants' administrators. The tenants' administrators grant access rights to their corresponding resources. The access management of such a SaaS application environment should support multiple access control models, such as identity based model, strategy based model, role based model, task based model, etc.

For custom and configurable level SaaS applications, a role-based access control model is a basic requirement. For instance, CSN, which supports to build a service from CSP, may be in charge of some applications but has no rights to administer the whole cloud service system. Besides, CSN may be allowed to access only a part of the resources with granted access rights. However, CSN can share its resource by providing application interfaces to other CSNs.

For the multi-tenant and scalable level, an integration of access control model for each individual and group is needed. For the role-based access control, shared resources among multiple tenants should be utilized according to task groups in a work flow and rights granted to those tasks. Thus, when these task groups are executed, the SaaS application environment should define the support task-based access control mechanism. This mechanism is used to make sure that access right of tenants to underlying resources could be timely granted and revoked, and underlying resources are prevented from unauthorized utilization.

8.1.2 Interface security

The SaaS application environment is required to secure interfaces open to CSPs or CSNs through which various kinds of cloud computing services are delivered or developed, and it is also required to secure communications based on these interfaces. Mechanisms that are available to ensure interface security include but are not limited to: unilateral/mutual authentication, integrity checksum, digital signature, etc.

8.1.3 Data security

8.1.3.1 Data isolation

Data can be isolated physically or logically. Physical data isolation should be accomplished by the access control of physical storages. It should require the SaaS application environment to store data of different tenants in different areas of physical storage, or implement the data accesses control for different tenants through access permission, data domain or any other methods. Logical data isolation implies that different tenants should be avoided to access others' data by the means of techniques such as virtualization, even if all the data are stored together.

For custom and configurable level SaaS applications, each tenant's data are separately stored and isolated from the others at the physical level.

For multi-tenant and scalable level SaaS applications, all tenant's data are stored in the cloud. Therefore, the SaaS application environment is required to be intelligent enough to segregate data from different tenants, and maintain isolation among different tenants' data at rest, at processing or at transmission. The boundary between each tenant should be ensured at the physical level or at the logical level, which depends on the required isolation granularity and the specific deployment of the cloud computing software and hardware.

8.1.3.2 Data confidentiality

In most cases, the tenant's data is on off-premise storage and utilization, and is subjected to exposure. Therefore, the SaaS application environment is required to support encryption mechanisms to ensure data confidentiality in transmission, during processing or out of occupation, and prevent data leakage due to security vulnerabilities in the application.

Data encryption service is required for all SaaS levels. Critical data is required to be encrypted to prevent exposure.

For multi-tenant and scalable level, as tenants' data should be stored in one database or even one big table, the SaaS application environment is required to provide an appropriate key management mechanism to ensure that the data cannot be cracked by other tenants.

8.1.3.3 Data integrity

Data including system data and user data, such as logs and configuration data, require the SaaS application environment to support integrity mechanisms to prevent them from unauthorized tampering in transmission, during processing or out of occupation.

System log and application log are required not to be modified. In this case, when either fault or misuse occurs, CSP and malicious software are prevented from concealing trace by modifying logs.

SaaS application may require CSCs to configure it on demand. The configuration data, such as configuration file, is also required to not be modified without authorization.

In the SaaS application environment, users' data is stored in the cloud which is managed by CSP. In this case, the verification of data integrity becomes a remarkable security requirement. Moreover, it is required to verify the integrity of massive data.

8.1.3.4 Data reliability

To support data reliability, the SaaS application environment is required to support data backup or redundancy mechanisms to ensure that tenants can access the data even if part of the cloud storage nodes lose efficacy.

Hosted data are required to implement a multiple-site backup; otherwise, the data will be completely ineffective. The SaaS application environment is required to have the ability to fully recover data and restore the data in time as well as keep data synchronism to ensure the consistency of multiple copies.

8.1.3.5 Data traceability and control

The SaaS application environment is required to ensure that physical location of data comply with the applicable law and local regulations, and with any restrictions in the legal agreements. The SaaS application environment is required to provide methods for CSCs to specify their data storage locations and verify that their data are appropriately placed.

Major concerns in a shared and virtualized infrastructure include not only loss of control by users over their data, but also locating data and controlling its whole life cycle. At any given time, the SaaS application environment is required to know exactly where both system data and user data are stored and processed, and provide verification of data location for CSCs. Both during and after usage, it shall not be possible for unauthorized third parties (including other CSPs) to trace the movement of the data.

8.1.4 Security assessment and audit

When underlying resources are changed, cracked or worked improperly, the SaaS application environment is required to be triggered to initiate security assessment procedure to evaluate whether or not specified security services or their applied security policies are affected, and indications or instructions are suggested to provide if they cannot satisfy predetermined conditions. An authorized party should be delegated to verify that the SaaS application environment complies with the applicable security requirements. Security assessment or security audit could be performed by CSC, CSP or a third party (CSN), and security certification could be performed by an authorized third party (CSN).

Independent trusted third parties should be used to provide reliable, independent and neutral security assessments or security audit.

8.1.5 Security hardening

The SaaS application environment aims mainly at offering secure service oriented multi-tenant development, deployment and an execution environment for SaaS applications. Security features of SaaS applications are in some cases insufficient or not well developed. The SaaS application environment is required to retrieve and verify those deficient security features of the SaaS applications, and provide differentiated security hardening mechanisms to enhance SaaS applications according to those deficient security features in order to meet the security requirements of different tenants in different contexts. The security features of

applications consist of static security features when applications are in idle status and of dynamic security features when applications are running.

8.2 Security requirements of CSP

Besides common security requirements, CSP has specific security requirements in the SaaS application environment.

8.2.1 Availability

For CSP, the SaaS application environment is required to ensure that CSCs are in service all the time, which requires the handling of hardware/software failures, denial of service attacks, etc. It is essential to ensure the minimal downtime for CSCs.

8.2.2 Service interoperability/portability guarantee

When CSC wants to migrate all or a part of its system to another CSP, the original CSP requires the SaaS application environment to provide service interoperability and portability guarantee to minimize the damage to CSC's business. Besides, the SaaS application environment is required to guarantee that the related data will be deleted permanently on the previous CSP and will not be recovered by any other party.

8.2.3 Software assets protection

Software assets (such as applications, application-internal data, scripts, macros, function code library, software license, etc.) are required to be protected in the SaaS application environment.

CSP requires the SaaS application environment to protect the confidentiality and integrity of any software assets provided by CSP or CSN, which implies that these software assets cannot be copied, misappropriated, tampered with, given away, or otherwise used in an unauthorized manner.

8.2.4 Legal compliance

Though CSP can use data backup and redundancy mechanisms to ensure CSC's data reliability, the SaaS application environment is required to ensure that data copies shall not be retained for longer time than the permitted data retention period under the applicable data protection law.

8.2.5 Security verification for source codes

As in the SaaS application environment, CSN may provide the applications' codes, content or software to CSP, the SaaS application environment is required to provide mechanisms that assist CSP to verify the codes and to prevent malicious codes.

8.3 Security requirements of CSN

In the SaaS application environment, CSN can be an application developer, content provider, software provider, system integrator and auditor. Besides common security requirements, CSN has its own security requirements in the SaaS application environment.

8.3.1 Audit security

When CSN is an auditor, the SaaS application environment is required to provide mechanisms that assist CSN to collect audit events, logging and reporting information at the granularity of tenant and application. These information are used to assure that CSP's service complies with governmental regulatory requirements and legal agreements contracted with tenants. The SaaS application environment is also required to provide mechanisms that assist CSN to ensure that the information collected and reported by the audit components within the CSP system are correct and not subject to tampering or manipulation.

Besides, the SaaS application environment is required to provide the capability for CSN to record the changes of important data and monitor the data availability online, in order to send a security alarm in time and therefore reduce losses.

8.3.2 Software security

When CSN is a cloud content or software developer, the SaaS application environment is required to provide mechanisms that assist CSN to ensure that their codes or other components supplied to CSP comply with any programming constraints required by the CSP**,** Besides, the codes or components should not contain malware or violate the integrity of CSP's cloud services.

8.3.3 Software maintainability

When CSN is a cloud software developer, the SaaS application environment is required to support mechanisms that assist CSN to provide source codes or other functionality for CSP's system. The source codes or functionality are required to contain versioning and other appropriate methods, in order to ensure that they can be maintained during the lifetime of the service. These methods include but are not limited to providing updates to fix known vulnerabilities, removing dependency on other components with known vulnerabilities, and increasing the overall system security.

Bibliography

[b-ITU-T X.1601] Recommendation ITU-T X.1601 (2014), *Security framework for cloud computing*.

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary*.

4.

Video processing and storage


00:01:54:02

Requirements for cloud storage in visual surveillance

Recommendation ITU-T F.743.2

(07/2016)

SERIES F: NON-TELEPHONE TELECOMMUNICATION SERVICES

Summary

Recommendation ITU-T F.743.2 defines the cloud storage service requirements in visual surveillance. Cloud storage enables service users to have ubiquitous, convenient, on-demand network access to a shared pool of configurable storage resources, which can be rapidly provisioned and released with minimal management effort or service-provider interaction. Cloud storage can realize flexible and reliable data storage for large-scale visual surveillance, and its components are modularized and allocated dynamically based on real usage. This Recommendation provides the application scenarios and requirements for cloud storage in visual surveillance.

Keywords

Cloud storage, picture storage, video file uploading, video metadata management, video stream storage, visual surveillance.

Table of Contents

1 Scope

This Recommendation describes the brief functional model, application scenarios and requirements for cloud storage in visual surveillance (VS) systems, based on the requirements and architectures defined by [ITU-T F.743], [ITU-T H.626] and [ITU-T H.626.1].

A visual surveillance service is a telecommunication service focusing on video (and audio) application technology, which is used to remotely capture multimedia (e.g., audio, video, image, various alarm signals), and present this to end users in a friendly manner (including accessibility aspects), based on a broadband network with ensured quality, security and reliability. Cloud storage is a data storage model for enabling service users to have ubiquitous, convenient and on-demand network access to a shared pool of configurable storage resources, which can be rapidly provisioned and released with minimal management effort or service-provider interaction. In cloud storage systems, the physical and virtual resources can be dynamically assigned and reassigned according to user demand. Cloud storage can realize scalable, flexible and reliable data storage for large-scale visual surveillance.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T F.743] Recommendation ITU-T F.743 (2009), *Requirements and service description for visual surveillance*.

[ITU-T H.626] Recommendation ITU-T H.626 (2011), *Architectural requirements for visual surveillance*.

[ITU-T H.626.1] Recommendation ITU-T H.626.1 (2013), *Architecture for mobile visual surveillance*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 application [b-ITU-T Y.101]: A structured set of capabilities, which provide value-added functionality supported by one or more services.

3.1.2 customer [b-ITU-T M.60]: An entity which receives services offered by a service provider based on a contractual relationship. It may include the role of a network user.

3.1.3 customer unit [ITU-T F.743]: A device located at the customer part of a visual surveillance system and used to present multimedia information (such as audio, video, image, alarm signal, etc.) to the end user.

3.1.4 premises unit [ITU-T F.743]: A device located at the remote part of a visual surveillance system and used to capture multimedia information (such as audio, video, image, alarm signal, etc.) from a surveilled object.

3.1.5 service [b-ITU-T Y.101]: A structure set of capabilities intended to support applications.

3.1.6 visual surveillance [ITU-T F.743]: A telecommunication service focusing on video (but including audio) application technology, which is used to remotely capture multimedia (such as audio, video, image, alarm signals, etc.) and present them to the end user in a friendly manner, based on a managed broadband network with quality, security and reliability ensured.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 cloud storage: A data storage model for enabling service users to have ubiquitous, convenient and on-demand network access to a shared pool of configurable storage resources, which can be rapidly provisioned and released with minimal management effort or service-provider interaction. In cloud storage systems, the physical and virtual resources can be dynamically assigned and reassigned according to user demand.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AS	Application System
CU	Customer Unit
DVR	Digital Video Recorder
IPU	Intelligent Premises Unit
MCU	Mobile Customer Unit
MSU	Media Storage Unit
NVR	Network Video Recorder
PU	Premises Unit
VS	Visual Surveillance
VSCS	Visual Surveillance Cloud Storage

5 Conventions

In this Recommendation:

– The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this recommendation is to be claimed.

– The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

6 Overview

Currently, large-scale visual surveillance system deployment has contributed to the explosive growth of surveillance video data. Moreover, the massive amount of surveillance video data contains a lot of valuable information which can be mined to provide more intelligent services. Attention is needed to the efficient storage of video data and fast access to information of interest to users.

When the surveillance industry changes to all IP network usage, the network video recorder (NVR), as a main component for surveillance video storage, will gradually replace the existing digital video recorder (DVR). However, an NVR which is installed on single physical server may reach the maximum storage or throughput limitation due to predefined resource limitations. In addition, the current NVR-based storage model does not efficiently support the analysis and mining of the massive amount of video data.

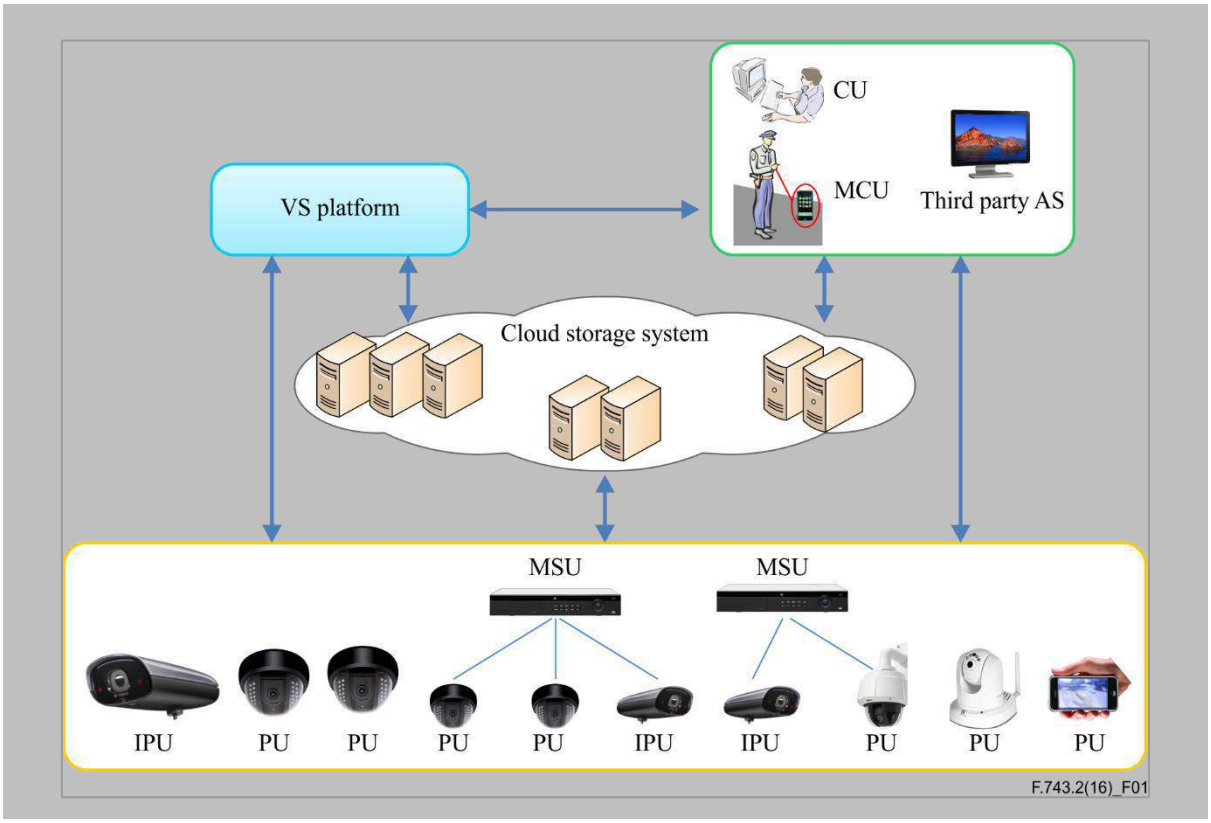


Figure 1 – Cloud storage model for visual surveillance

Cloud storage is a new model for enabling service users to have ubiquitous, convenient and on-demand network access to a shared pool of configurable storage resources, which can be rapidly provisioned and released with minimal management effort or service-provider interaction. From a telecommunication perspective, users do not buy resources but rather purchase cloud services provided by cloud environments. This can improve the system flexibility and reduce the expenditure of users' systems.

Cloud storage is used for aggregating and managing a particular data set. Figure 1 shows a cloud storage model for a visual surveillance system. A cloud storage system is a scalable, flexible and reliable video recording system that can optimize the storage resources for massive video sources. In a cloud storage system, each component is modularized and allocated dynamically based on actual usage, and data protection mechanisms are supported to improve system reliability. A cloud storage system enables convenient and fast access to a wealth of data across distributed and heterogeneous data sources in the cloud. Furthermore, this data storage system can be easily integrated with cloud computing frameworks which support efficient intelligent video analysis tasks. For the premises unit (PU) devices, video data can be uploaded to a cloud storage system by online/offline modes using streaming or other network data transfer protocols. The data sources can be IP cameras, mobile devices or other media storage units (MSUs), such as DVRs with networking capability, NVRs, and vehicle DVRs installed on cars. The visual surveillance (VS) platform can call the cloud storage service through standard interfaces provided by the cloud storage system. All types of authorized customer units (CUs) or authorized third-party application systems (ASs) can access the data stored in the cloud storage system.

7 Scenarios

This clause describes typical service scenario examples illustrating the cloud storage in visual surveillance and deriving its service requirements.

7.1 Video stream storage

Surveillance cameras capture video data continuously. User Bob has subscribed to the visual surveillance cloud storage (VSCS) service from the VS service provider, and wants to store streaming video data in the cloud directly.

Step 1: Bob logs into the VS system via his PC. He clicks a cloud storage menu function and goes to a video stream storage plan form. A camera list appears on the screen, which displays detailed information for each camera that Bob can access. Bob chooses the cameras whose captured video data needs to be stored in the cloud, and then sets the time interval during which the data should be recorded. The VS management system receives Bob's submitted video stream cloud storage plan, and forwards the plan to the cloud storage system.

Step 2: According to the video stream storage plan, the cloud storage system gets the video stream directly from the monitoring cameras, and then writes the video data to the cloud storage resource pool built on the storage device clusters.

Step 3: Bob can browse the camera's video data recorded in the cloud; he can also choose the camera name and the video starting time, and replay the video of interest stored in the cloud.

7.2 Video file uploading

Case 1: Video file uploading from NVR

An NVR is usually used as the local storage devices for continuously recording surveillance video from network cameras. NVR has a maximum storage capacity or throughput limitation due to predefined resource limitations. For example, an NVR can receive video streams from 16 cameras simultaneously, and can record the video data from those cameras for one month. In addition, the data reliability is difficult to guarantee when the NVR fails.

The public security department of a city has deployed a VS system in the city. Tom is the system administrator and is responsible for operating the visual surveillance system to carry out public security tasks. Currently, the surveillance video is recorded on the local NVRs. However, Tom's supervisor lets him retain the video data from some cameras for at least six months.

Step 1: Tom logs into the VS system. He chooses the surveillance cameras, sets the time interval to 12 months and sets the video file uploading period to 12 hours. Tom submits the video file uploading plan to the visual surveillance management system. This plan is then forwarded to the cloud storage system.

Step 2: According to the video file uploading plan, the cloud storage system retrieves the video files from the corresponding NVRs every 12 hours, and then writes this video data to the cloud storage resource pool built on the storage device clusters. The storage space assigned to this plan is large enough to store the video data for 12 months.

Step 3: Tom can download the video files from the cloud; he can also replay the videos stored in the cloud on demand.

Case 2: Video file uploading from mobile devices

Mobile visual surveillance devices are widely used today. The storage capacity of a mobile device is limited, and the user wants to access the video captured by a mobile device using any terminals, e.g., PC, anywhere. The user can then upload the captured video files from the mobile device to the cloud.

Step 1: Bob logs into the VS system through a mobile device. He often uses the camera of the mobile device to capture videos; these video files are stored in the mobile device.

Step 2: Since the storage space of the mobile device is limited, Bob applies for video cloud storage space in order to save more surveillance video data. He chooses the video files from his mobile device, and then uploads the files to the cloud through wireless channels.

Step 3: Bob logs into the visual surveillance system using a PC, and can download the video files (which were uploaded from his mobile device) from the cloud. He can also replay the videos, stored in the cloud, on demand.

7.3 Video metadata management

The VS system can provide various intelligent services by using video/image analysis technologies. The intelligent traffic service is an example. For realizing these intelligent services, some video/image analysis algorithms are embedded in the traffic surveillance cameras, and these cameras can directly output video content metadata, such as: vehicle plate number, vehicle type, speed of vehicle, colour of vehicle. In addition, video analysis servers can be deployed in the data centre, and the surveillance video stream or the recorded video files can be processed to obtain the video content metadata on these servers.

Step 1: Model the surveillance video metadata, and design and implement the video metadata management system in cloud.

Step 2: The surveillance video metadata is obtained from the intelligent video/image analysis devices, and is sent to the cloud.

Step 3: An authorized user can browse and retrieve the surveillance video metadata stored in the cloud. Likewise, authorized application systems can access the video metadata in the cloud, and provide the various intelligent services based on the video metadata.

7.4 Picture storage

Case 1: Picture upload from surveillance camera

High-definition cameras are widely deployed on streets to capture high-resolution pictures. These pictures may contain useful information and can be processed further. For example, vehicle plate numbers can be extracted accurately from a picture by using a vehicle plate recognition algorithm.

Step 1: Network cameras continuously capture pictures, and send these pictures directly to the cloud.

Step 2: The cloud storage system receives the pictures, and writes the pictures to the cloud storage resource pool built on the storage device clusters.

Step 3: An authorized user or application system can access the pictures stored in the cloud.

Case 2: Picture uploading from mobile device

John is a traffic police officer, and one of his routine tasks is to find illegally parked vehicles and record the infraction.

Step 1: John logs into the surveillance system through a mobile device. He captures the picture of an illegally parked vehicle using the camera of the mobile device.

Step 2: The captured picture is then sent to the cloud through wireless channels.

Step 3: An authorized user or application system can access the pictures stored in the cloud.

8 Requirements for cloud storage in visual surveillance

8.1 User requirements

There are two types of cloud storage service users : the service consumer and the service provider.

8.1.1 Cloud storage service consumer requirements

– USR-001: A VSCS system is required to support registration and de-registration of the end user through the interface provided by the system, and the end user can view and modify personal information.

– USR-002: A VSCS system is required to support end-user login and logout from the system conveniently. The user name and password are required when an end user logs into the system.

– USR-003: A VSCS system is recommended to support end-user view of the user access logs or other system logs.

– USR-004: A VSCS system is required to support user's data uploading from a client device, including video files, pictures and video metadata.
– USR-005: A VSCS system is required to support the user's view and downloading of stored data via a client device, including video files, pictures and video metadata.
– USR-006: A VSCS system is recommended to support the video on demand and picture presentation for end users.
– USR-007: A VSCS system is recommended to support information retrieval for end users.
– USR-008: A VSCS system is recommended to support flexible storage space application for end users.
– USR-009: A VSCS system is required to support the view of a user's storage space status, including the storage space occupancy rate, the remaining storage space.

8.1.2 Cloud storage service provider requirements

– USR-010: A VSCS system is required to support the provider's login and logout from the system conveniently. The provider's name and password are required when logging into the system.
– USR-011: A VSCS system is required to support the provider's view of the cloud storage system operating status from the beginning to then-present time, including the system storage space occupancy rate, the system's remaining storage space, the storage space occupancy rate of individual users, the remaining storage space of individual users, etc.
– USR-012: A VSCS system is required to support flexible storage space assignment for individual users.

8.2 Service requirements

8.2.1 Video storage service requirements

– SER-001: A VSCS system is required to support directly writing video streams, from multiple PUs, through the network.
– SER-002: A VSCS system is required to support video file uploading from multiple local video storage devices through the network, including NVRs, mobile video capturing devices, etc.
– SER-003: A VSCS system is required to support video file deletion.
– SER-004: A VSCS system is required to support video file browsing and searching; the searching conditions can be the source of video files, the capture time of video files, etc.
– SER-005: A VSCS system is required to support video file downloading through the network.
– SER-006: A VSCS system is required to support automatic video file overwriting when a user's storage space is full; the overwriting principle is that the oldest data is replaced first.
– SER-007: A VSCS system is recommended to support video playback for end users according to the source of the video file and the capture time of the video file. Video playback operations include fast forward, slow forward, pause, and stop.

8.2.2 Picture storage service requirements

– SER-008: A VSCS system is required to support direct writing of pictures, from multiple PUs, through the network.
– SER-009: A VSCS system is required to support picture uploading from multiple local video storage devices through the network, including PCs, mobile picture capturing devices, etc.
– SER-010: A VSCS system is required to support picture deletion.
– SER-011: A VSCS system is required to support picture browsing and searching; the searching conditions can be the source of the pictures, the capture time of the pictures, etc.
– SER-012: A VSCS system is required to support picture downloading through the network.

8.2.3 Video metadata storage service requirements

– SER-013: A VSCS system is required to support video metadata writing through the network.

– SER-014: A VSCS system is required to support video metadata deletion.

– SER-015: A VSCS system is required to support video metadata browsing and searching; the searching condition can be the source of video metadata, the creation time of video metadata, video metadata content, etc.

8.3 Security requirements

8.3.1 Authentication security requirements

– SEC-001: A VSCS system is required to provide the mechanisms for authentication and authorization, and it is required to only permit authorized users to access the system and use system services. A VSCS system is required to forbid an unauthorized user to handle any resources of the system.

8.3.2 Access security requirements

– SEC-002: A VSCS system is required to operate in environments where network address translation (NAT) and/or firewall devices are present. It is recommended to utilize specified firewalls, gatekeepers and other network devices to ensure security for access to some special cloud storage services.

8.3.3 Content security requirements

– SEC-003: A VSCS system is required to ensure the security of stored data such as video, picture, video metadata, etc. It is recommended to provide the mechanisms to protect the copyrights of the stored data, and to protect the stored data from being corrupted.

– SEC-004: A VSCS system is required to provide data protection mechanisms such as data backup, coding, etc. It is required to be able to recover the destroyed data.

– SEC-005: A VSCS system is required to protect user privacy.

8.3.4 System security requirements

– SEC-006: A VSCS system is required to have the capability of resisting various attacks.

– SEC-007: A VSCS system is required to provide the mechanisms for troubleshooting. It is required that a structural single-node problem be avoided (i.e., a problem at a single node should not cause failure of the entire system).

8.4 Management requirements

8.4.1 Storage management requirements

– MAN-001: A VSCS system is required to support storage space management. The storage space can be increased and decreased flexibly.

8.4.2 Equipment management requirements

– MAN-002: A VSCS system is required to provide the unified management of the storage equipment.

8.4.3 Service management requirements

– MAN-003: A VSCS system is required to provide the various storage service subscription means for users, and to provide the capabilities of querying, viewing and modifying their subscription information.

– MAN-004: A VSCS system is recommended to provide the capability of accounting, charging and billing for the service operation.

– MAN-005: A VSCS system is recommended to provide various alternative accounting modes, and to support flexible combinations of payment modes, billing modes, billing cycles, preferential pricing, etc.

8.4.4 Data management requirements

– MAN-006: A VSCS system is required to support data management in the cloud, including adding, deleting, browsing, indexing, searching.

8.4.5 System management requirements

– MAN-007: A VSCS system is required to provide a unified system management interface which can be called conveniently.

– MAN-008: A VSCS system is required to provide a visual interface for users.

8.4.6 Operation management requirements

– MAN-009: A VSCS system is required to monitor, record and display the running status of the system.

8.5 Scalability requirements

– SCA-001: A VSCS system is required to provide storage resource scalability. When the storage equipment is increased or decreased in the system, the storage capacity is increased or decreased accordingly, and the system service is uninterrupted.

– SCA-002: A VSCS system is required to provide storage space scalability for users. The storage space of individual users can be increased or decreased according to each user's demands.

– SCA-003: A VSCS system is required to provide user scalability. The number of supported users can be increased or decreased dynamically.

8.6 Reliability requirements

– REL-001: A VSCS system is required to ensure service reliability. When storage equipment fails or the storage system network operation is abnormal, the system service can be used normally.

– REL-002: A VSCS system is required to ensure data reliability. When data is destroyed, the system can recover it based on the data protection mechanism, e.g., data backup, data coding.

8.7 Performance requirements

– PER-001: A VSCS system is required to support concurrent user operations. The system can serve a large number of users simultaneously, while ensuring the service quality.

Bibliography

[b-ITU-T M.60] Recommendation ITU-T M.60 (1993), *Maintenance terminology and definitions*.

[b-ITU-T Y.101] Recommendation ITU-T Y.101 (2000), *Global Information Infrastructure terminology: Terms and definitions*.

[ITU-T FG TR] ITU-T FG Technical Report: Part 1 (2012), *Introduction to the cloud ecosystem: definitions, taxonomies, use cases and high-level requirements*.

Requirements for a cloud computing platform supporting a visual surveillance system

Recommendation ITU-T F.743.8

(05/2019)

SERIES F: NON-TELEPHONE TELECOMMUNICATION SERVICES

Summary

Recommendation ITU-T F.743.8 specifies the requirements for a cloud computing platform supporting visual surveillance. Cloud computing is an emerging technology aimed at providing various computing services over the Internet. Using virtualization technology, a cloud computing platform realizes a ubiquitous and flexible shared resources pool that can be rapidly provisioned and released with minimal management effort or service-provider interaction based on the needs of users. By using the cloud computing technology, the visual surveillance system can conveniently manage various functional components and services, such as video distribution, video transcoding and intelligent video processing. This Recommendation provides the application scenarios and requirements for a cloud computing platform supporting a visual surveillance system.

Keywords

Cloud computing, requirements, scenarios, visual surveillance.

Table of Contents

1 Scope

This Recommendation specifies the application scenarios and requirements for a cloud computing platform supporting a visual surveillance system.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 application [b-ITU-T Y.101]: A structured set of capabilities, which provide value-added functionality supported by one or more services.

3.1.2 cloud computing [b-ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications and storage equipment.

3.1.3 customer [b-ITU-T M.60]: An entity which receives services offered by a service provider based on a contractual relationship. It may include the role of a network user.

3.1.4 customer unit [b-ITU-T H.626]: A device located at the customer part of a visual surveillance system and used to present multimedia information (such as audio, video, image, alarm signal, etc.) to the end user.

3.1.5 mobile customer unit (M_CU) [b-ITU-T H.626.1]: Mobile client software installed in a customer's mobile devices. The M_CU is used to initiate the service and provide customers with video viewing.

3.1.6 premises unit [b-ITU-T H.626]**:** A device located at the remote part of a visual surveillance system and used to capture multimedia information (such as audio, video, image, alarm signal, etc.) from a surveilled object.

3.1.7 visual surveillance [b-ITU-T H.626]: A telecommunication service focusing on video (but including audio) application technology, which is used to remotely capture multimedia (such as audio, video, image, alarm signals, etc.) and present them to the end user in a user-friendly manner, based on a managed broadband network with ensured quality, security and reliability.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CU	Customer Unit
IVS	Intelligent Visual Surveillance
MCU	Mobile Customer Unit
MSU	Media Storage Unit
PU	Premises Unit
VS	Visual Surveillance
VSCC	Visual Surveillance Cloud Computing

5 Conventions

In this Recommendation:

– The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

– The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

6 Scenarios

This clause describes typical scenarios illustrating the cloud computing platform supporting visual surveillance and deriving its service requirements.

6.1 Video distribution

The cloud computing platform in a visual surveillance (VS) system can support large-scale real-time video forwarding. For example, many surveillance cameras are deployed in the Great Wall Scenic Area, and the remote monitoring function of the cameras is open to the public. If users wants to see current images of the Great Wall remotely, they can view the network video information on their local devices through the cloud-based real-time video distribution function.

Step 1: Users enter the customer unit (CU) which supports remote live video viewing of the Great Wall Scenic Area, and submit their request to the VS system.

Step 2: After receiving a video-viewing request, the VS system authenticates the user information, and obtains the related information from a video-forwarding function unit that is deployed on the cloud computing platform. The cloud computing platform can dynamically create or destroy the video-forwarding function according to current user requests. The VS system then responds to the CU with the information about the video-forwarding function on the cloud computing platform.

Step 3: After receiving the VS system response, the CU sends a video-viewing request to the cloud computing platform.

Step 4: The cloud computing platform obtains the video stream from the corresponding camera, and then forwards the video stream to the CU.

6.2 Video transcoding

The cloud computing platform in a VS system can support video-transcoding functions, e.g., code rate transformation and video format conversion. The traffic department of a city has deployed a large-scale VS system in the city streets with high-definition network cameras. Users want to view the current traffic situation on their way home with their mobile phones. Due to the limited bandwidth of mobile devices and mobile data traffic limits, high-definition surveillance video needs to be transcoded to low-resolution video before forwarding to the CU. The video-transcoding operation can be carried out on the cloud computing platform.

Step 1: Users log into the VS system via their mobile customer unit (MCU), and select the appropriate network camera. The MCU then sends a video-viewing request to the VS system with the video format description.

Step 2: After receiving the video-viewing request, the VS system authenticates the user information, and obtains the related information from a video-forwarding function unit that is deployed on the cloud computing platform. The VS system then responds to the MCU with the information from the video-forwarding function in the cloud computing platform.

Step 3: After receiving the response of the VS system, the MCU sends a video-viewing request to the cloud computing platform.

Step 4: The cloud computing platform obtains the video stream from the corresponding camera. Then, according to the video format description of the MCU, the surveillance video stream is transcoded by the video-transcoding component deployed in the cloud computing platform. The cloud computing platform can

dynamically create and destroy the video-forwarding function according to the current requests of the MCU. After that, the transcoded video stream is sent to the MCU.

6.3 Online intelligent video processing

6.3.1 Case 1: Traffic flow analysis

The traffic department of a city has deployed an intelligent visual surveillance (IVS) system for city roads. The system administrator is responsible for operating the IVS system to carry out traffic management tasks. The work of the administrator is to monitor real-time traffic flow of key road sections in the traffic rush hour. A traffic flow analysis function can be developed based on computer vision technology, and is virtualized as functional components in the cloud computing platform. When a user needs to obtain the traffic flow situation of certain road sections, the system can call the traffic flow analysis function to process the relevant surveillance video streams.

Step 1: Users log into the IVS system through the CU. They choose certain surveillance cameras that are deployed on key road sections of interest and set the traffic flow analysis function. They then submit traffic flow analysis requests to the IVS system.

Step 2: After receiving the traffic flow analysis request, the IVS system authenticates the user information, and obtains the relevant information from the traffic flow analysis function that is deployed on the cloud computing platform. The cloud computing platform can dynamically create and destroy the traffic flow analysis function components according to current user requests. The IVS system then responds to the CU with the information from the traffic flow analysis function.

Step 3: After receiving the response of the IVS system, the CU sends the request to the cloud computing platform.

Step 4: The cloud computing platform obtains the relevant video streams from the corresponding cameras, online processes the video streams and then sends the real-time traffic flow analysis results back to the CU.

6.3.2 Case 2: Perimeter prevention

An electricity company uses an IVS system to monitor key power transmission equipment deployed in a city. Surveillance cameras are deployed around the power transmission equipment and the IVS system online analyses the captured surveillance video by calling the perimeter prevention function. Once someone approaches the power transmission equipment, the IVS system generates an alarm message to alert the user to the exception. The perimeter prevention function is virtualized as functional components in the cloud computing platform, and can be dynamically created and destroyed according to current user requests. The working step of the online perimeter prevention scenario is similar to that of the online traffic flow analysis scenario.

6.4 Offline intelligent video processing

6.4.1 Case 1: Human recognition

A public security department has deployed an IVS system in a city street. The system administrator is responsible for operating the IVS system to carry out public security tasks. When there is a robbery in front of a bank, the administrator reviews the relevant surveillance video captured by the cameras deployed around the bank and obtains a picture of the robber. To find the escape route of the robber as soon as possible, the administrator uses the intelligent human recognition function of the IVS system to process the massive related historical surveillance video. The intelligent human recognition function can be virtualized as functional components in the cloud computing platform and can be dynamically created according to user demand.

Step 1: Users log into the IVS system through the CU. To quickly find robber information in the massive surveillance video data, the user needs to set several functional parameters, such as the camera channel numbers, the time period of interest in the historical video and the picture of the robber, and then sends an intelligent human recognition request to the IVS system.

Step 2: After receiving the human recognition request, the IVS system authenticates the user information, requests the cloud computing platform to create the intelligent human recognition function, and then responds to the CU with the information from the intelligent human recognition function.

Step 3: After receiving the response of the IVS system, the CU sends the request to the cloud computing platform.

Step 4: The cloud computing platform downloads the relevant video files from the media storage unit (MSU), processes the video files in parallel and then sends the human recognition results back to the CU.

Step 5: When the intelligent human recognition task finishes, the cloud computing platform destroys the intelligent human recognition function to release the corresponding resources.

6.4.2 Case 2: Video synopsis

The IVS system deployed by a public security department produces massive surveillance video continuously and the cost of data storage is high. However, the public security department is usually interested in moving objects in the surveillance video. Therefore, to save storage space, surveillance video is usually processed to generate synopsis video before long-term storage. The objective of video synopsis is to shorten the video time by reorganizing moving video objects in temporal and spatial dimensions. For example, by using the video synopsis operation, a 24 h surveillance video file is transformed into a 30 min video file that contains all moving objects in the original video file. The intelligent video synopsis function can be virtualized as functional components in the cloud computing platform, and can be dynamically created according to user demand.

Step 1: Users log into the IVS system through the CU, and set several functional parameters of the video synopsis, such as the camera channel numbers, the time period of interest in the historical video and the density of the objects. Then users send an intelligent video synopsis request to the IVS system.

Step 2: After receiving the video synopsis request, the IVS system authenticates the user information, requests the cloud computing platform to create the intelligent video synopsis function and then responds to the CU with the information from the intelligent video synopsis function.

Step 3: After receiving the response of the IVS system, the CU sends the request to the cloud computing platform.

Step 4: The cloud computing platform downloads the relevant video files from the MSU, processes the video files in parallel and then uploads the video synopsis results back to the MSU.

Step 5: When the intelligent video synopsis task finishes, the cloud computing platform destroys the intelligent video synopsis function to release the corresponding resources.

7 Requirements for cloud computing platform supporting visual surveillance

7.1 User requirements

There are two types of user: cloud computing service consumers and cloud computing service providers.

7.1.1 Cloud computing service consumer requirements

– USR-01: A visual surveillance cloud computing (VSCC) platform is required to support registration and de-registration of the end user through the interface provided by the system and the end user can view and modify personal information.

– USR-02: A VSCC platform is required to support convenient end-user login to and logout from the system. A username and password are required when an end user logs into the system.

– USR-03: A VSCC platform is recommended to support end-user view of the user access logs or other system logs.

– USR-04: A VSCC platform is recommended to support real-time surveillance video distribution.

– USR-05: A VSCC platform is recommended to support the online or offline surveillance video-transcoding function.
– USR-06: A VSCC platform is recommended to support online or offline intelligent surveillance video analysis functions.
– USR-07: A VSCC platform is required to support the configuration of computing resources for video surveillance tasks on demand.
– USR-08: A VSCC platform is required to support the user view of the status of user computing tasks and computing resources.

7.1.2 Cloud computing service provider requirements

– USR-09: A VSCC platform is required to support convenient provider login to and logout from the system. The provider name and password are required when logging into the system.
– USR-10: A VSCC platform is required to support the provider view of the system operating status from the beginning to now, including the system computing resource occupancy rate, the remaining computing resources of the system, the computing resource occupancy rate of individual users and the remaining computing resources of individual users.
– USR-11: A VSCC platform is required to support flexible computing resource assignment for individual users.

7.2 Service requirements

7.2.1 Online intelligent video processing service requirements

– SER-01: A VSCC platform is recommended to support online intelligent video processing. The video processing components deployed on a VSCC platform can receive video streams from premises units (PUs) and process the video in real time.
– SER-02: A VSCC platform is recommended to support online management of video processing tasks, such as creation, pause, restart and deletion.
– SER-03: A VSCC platform is recommended to view the progress of online video processing tasks.
– SER-04: A VSCC platform is recommended to view the status of resources utilized by online intelligent video processing tasks.
– SER-05: A VSCC platform is recommended to support the viewing of log files that record the operations of online intelligent video processing tasks.

7.2.2 Offline intelligent video processing service requirements

– SER-06: A VSCC platform is recommended to support offline intelligent video processing. The video processing components deployed on the VSCC platform can download the video files from the MSU and carry out their batch processing.
– SER-07: A VSCC platform is recommended to support offline management of video processing tasks, such as creation, pause, restart and deletion.
– SER-08: A VSCC platform is recommended to view the progress of offline video processing tasks.
– SER-09: A VSCC platform is recommended to view the status of resources utilized by offline intelligent video processing tasks.
– SER-10: A VSCC platform is recommended to support the viewing of log files that record the operations of offline intelligent video processing tasks.

7.2.3 Video transcoding

– SER-11: A VSCC platform is recommended to support video transcoding. The video-transcoding components deployed on the VSCC platform can receive video streams from PUs and transcode the video in real time. In addition, the video-transcoding components can download video files from the MSU and carry out their transcoding in batches.

– SER-12: A VSCC platform is recommended to support the management of video-transcoding tasks, e.g., creation, pause, restart and deletion.
– SER-13: A VSCC platform is recommended to view the progress of video-transcoding tasks.
– SER-14: A VSCC platform is recommended to view the status of resources utilized by video-transcoding tasks.
– SER-15: A VSCC platform is recommended to support the viewing of log files that record the operations of video-transcoding tasks.

7.3 Security requirements

7.3.1 Authentication security requirements

– SEC-01: A VSCC platform is required to provide the mechanisms for authentication and authorization, and to permit only authorized users to access the system and use system services. A VSCC platform is required to forbid unauthorized users to handle any system resources.

7.3.2 Access security requirements

– SEC-02: A VSCC platform is required to operate in an environment where network address translation (NAT) or firewall devices are present. It is recommended to utilize specified firewalls, gatekeepers and other network devices to ensure security for access to some special cloud computing services.

7.3.3 Content security requirements

– SEC-03: A VSCC platform is recommended to ensure the security of processed video data, the results of the video processing, etc.
– SEC-04: A VSCC platform is required to protect user privacy.

7.3.4 System security requirements

– SEC-05: A VSCC platform is required to have the capability to resist various attacks.
– SEC-06: A VSCC platform is required to provide troubleshooting mechanisms. It is required that a structural single-node problem be avoided (i.e., a problem at a single node should not cause failure of the entire system).

7.4 Management requirements

7.4.1 Resources management requirements

– MAN-01: A VSCC platform is required to support resource management of the cloud computing platform. Resources can be increased and decreased flexibly according to service requests.

7.4.2 Equipment management requirements

– MAN-02: A VSCC platform is required to provide unified management of the computing equipment.

7.4.3 Service management requirements

– MAN-03: A VSCC platform is required to provide various computing service subscription means for users, and to provide the capabilities to query, view and modify their subscription information.
– MAN-04: A VSCC platform is recommended to provide the capability of accounting, charging and billing for the computing service operation.
– MAN-05: A VSCC platform is recommended to provide various alternative accounting modes, and to support flexible combination of payment modes, billing modes, billing cycles, preferential pricing, etc.

7.4.4 System management requirements

– MAN-06: A VSCC platform is required to provide a unified system management interface that can be called conveniently.
– MAN-07: A VSCC platform is required to provide a visual interface for users.

7.4.5 Operation management requirements

– MAN-08: A VSCC platform is required to monitor, record and display the running status of the system.

– MAN-09: A VSCC platform is required to monitor, record and display usage of cloud computing cluster resources.

7.5 Scalability requirements

– SCA-01: A VSCC platform is required to provide computing resource scalability. When computing equipment is increased or decreased in the system, the computing capacity of the VSCC platform is increased or decreased accordingly, and the system service is uninterrupted.

– SCA-02: A VSCC platform is required to provide computing resources scalability for users. The computing resources of individual users can be increased or decreased according to each user's demand.

– SCA-03: A VSCC platform is required to provide user scalability. The number of supported users can be increased or decreased dynamically.

7.6 Reliability requirements

– REL-01: A VSCC platform is required to ensure service reliability. When computing equipment fails or the system network operation is abnormal, the system service can be used normally.

7.7 Performance requirements

– PER-01: A VSCC platform is required to support concurrent user operations. The system can serve a large number of users simultaneously, while ensuring service quality.

Bibliography

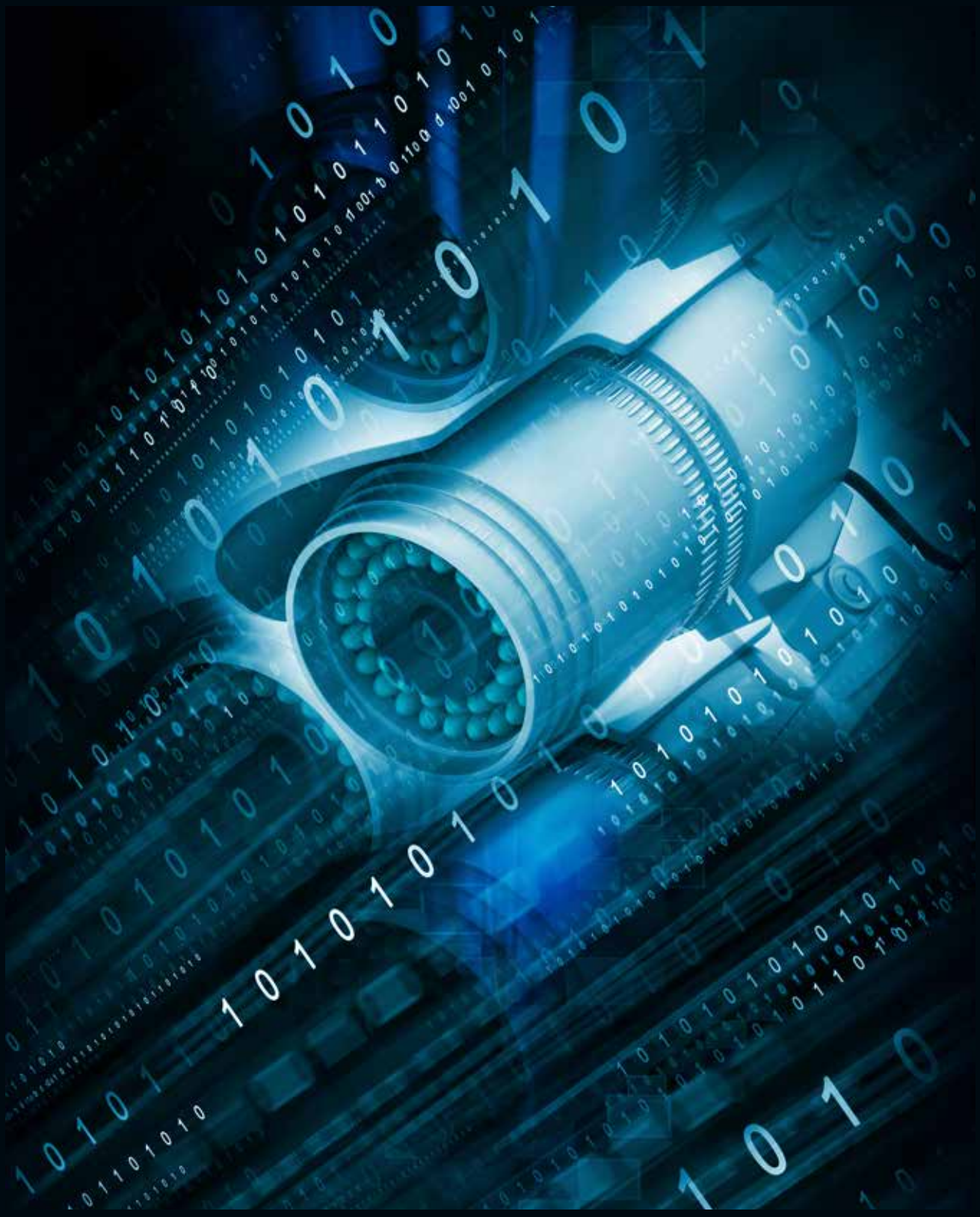
[b-ITU-T H.626] Recommendation ITU-T H.626 (2011), *Architectural requirements for visual surveillance*.

[b-ITU-T H.626.1] Recommendation ITU-T H.626.1 (2013), *Architecture for mobile visual surveillance*.

[b-ITU-T M.60] Recommendation ITU-T M.60 (1993), *Maintenance terminology and definitions*.

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014), *Information technology – Cloud computing – Overview and vocabulary*.

[b-ITU-T Y.101] Recommendation ITU-T Y.101 (2000), *Global Information Infrastructure terminology: Terms and definition*s.



Architecture for cloud storage in visual surveillance

Recommendation ITU-T H.626.2

(12/2017)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Summary

Recommendation ITU-T H.626.2 defines a cloud storage architecture in visual surveillance. Cloud storage enables the service users to have ubiquitous, convenient and on-demand network access to a shared pool of the configurable storage resources, which can be rapidly provisioned and released with the minimal management effort or service-provider interaction. Cloud storage can realize flexible and reliable data storage for large-scale visual surveillance and its components are modularized and allocated dynamically based on the real usage. This Recommendation provides the architecture, entities, reference points and service control flow for cloud storage in visual surveillance.

Keywords

Architecture, cloud storage, entity, reference point, service control flow, visual surveillance.

Table of Contents

1 Scope

This Recommendation describes architecture, functional entities, reference points and service control flow of cloud storage in visual surveillance.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T H.626] Recommendation ITU-T H.626 (2011), *Architectural requirements for visual surveillance*.

[ITU-T F.743.2] Recommendation ITU-T F.743.2 (2016), *Requirements for cloud storage in visual surveillance*.

[ITU-T M.60] Recommendation ITU-T M.60 (1993), *Maintenance terminology and definitions*.

[ITU-T Y.101] Recommendation ITU-T Y.101 (2000), *Global Information Infrastructure terminology: Terms and definitions*.

[ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 application [ITU-T Y.101]: A structured set of capabilities, which provide value-added functionality supported by one or more services.

3.1.2 cloud storage [ITU-T F.743.2]: A data storage model for enabling service users to have ubiquitous, convenient and on-demand network access to a shared pool of configurable storage resources, which can be rapidly provisioned and released with minimal management effort or service-provider interaction. In cloud storage systems, the physical and virtual resources can be dynamically assigned and reassigned according to user demand.

3.1.3 customer [ITU-T M.60]: An entity which receives services offered by a service provider based on a contractual relationship. It may include the role of a network user.

3.1.4 customer unit [ITU-T H.626]: A device located at the customer part of a visual surveillance system and used to present multimedia information (such as audio, video, image, alarm signal, etc.) to the end user.

3.1.5 functional architecture [ITU-T Y.2012]: A set of functional entities and the reference points between them, used to describe the structure of an NGN. These functional entities are separated by reference points, and thus, they define the distribution of functions.

NOTE 1 – The functional entities can be used to describe a set of reference configurations. These reference configurations identify which reference points are visible at the boundaries of equipment implementation and between administrative domains.

NOTE 2 – The definition is not only applicable to NGNs, but also to other IP packet switch based networks.

3.1.6 functional entity [ITU-T Y.2012]: An entity that comprises an indivisible set of specific functions. Functional entities are logical concepts, while groupings of functional entities are used to describe practical, physical implementations.

3.1.7 interface [ITU-T Y.101]: A shared boundary between two functional units.

NOTE – An interface is defined by various characteristics pertaining to the functions, physical interconnections, signal exchanges and other characteristics as appropriate.

3.1.8 premises unit [ITU-T H.626]: A device located at the remote part of a visual surveillance system and used to capture multimedia information (such as audio, video, image, alarm signal, etc.) from a surveilled object.

3.1.9 reference point [ITU-T Y.2012]: A conceptual point at the conjunction of two non-overlapping functional entities that can be used to identify the type of information passing between these functional entities.

NOTE – A reference point may correspond to one or more physical interfaces between pieces of equipment.

3.1.10 service [ITU-T Y.101]: A structure set of capabilities intended to support applications.

3.1.11 visual surveillance [ITU-T H.626]: A telecommunication service focusing on video (but including audio) application technology, which is used to remotely capture multimedia (such as audio, video, image, alarm signal, etc.) and present them to the end user in a user-friendly manner, based on a managed broadband network with ensured quality, security and reliability.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 cloud storage access unit (CSAU): A device located at a cloud storage system in visual surveillance. The CSAU is the key unit for implementing communication between the CSDU and the MDU, PU and the other media data related units defined in visual surveillance. The functions of the CSAU include service control function, media control function and configuration management function.

3.2.2 cloud storage data unit (CSDU): A series of devices located at a cloud storage system in visual surveillance. The CSDU is the data node in a cloud storage system that is used to store the massive multimodal data produced by the visual surveillance system. A typical visual surveillance cloud storage system consists of a number of CSDUs, which is organized in a distributed way. The CSDU can be dynamically extended according to the user's demand. The CSDU can receive the media data from the CSAU and write the data onto its local storage device. In addition, the CSDU can read and transmit the stored data to the CSAU according to the data reading requests.

3.2.3 cloud storage management unit (CSMU): A device located at the central part of a cloud storage system in visual surveillance. The CSMU is used to provide the management services of the cloud storage system and respond to the service requests of the visual surveillance system. The main functions of the CSMU include supporting storage resource management, data management, user management, service management, log management and security control.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CMU Centre Management Unit

CSAU Cloud Storage Access Unit

CSDU Cloud Storage Data Unit

CSMU Cloud Storage Management Unit

CU Customer Unit

IPU Intelligent Premises Unit

MDU	Media Distribution Unit
MSU	Media Storage Unit
NVR	Network Video Recorder
PU	Premises Unit
SCU	Service Control Unit
VS	Visual Surveillance

5 Conventions

None.

6 Overview of cloud storage in visual surveillance

The large-scale deployment of visual surveillance systems has contributed to the explosive growth of surveillance video data. It induces stringent needs for the efficient storage of massive video data and fast access of information of interest to users. Cloud storage is a data storage model for enabling service users to have ubiquitous, convenient and on-demand network access to a shared pool of configurable storage resources, which can be rapidly provisioned and released with minimal management effort or service-provider interaction. In the cloud storage system, the physical and virtual resources can be dynamically assigned and reassigned according to the users' demands.

7 Functional architecture for cloud storage in visual surveillance

7.1 Architectural framework

Figure 7-1 shows the architectural framework for cloud storage in visual surveillance. The cloud storage based visual surveillance platform consists of two parts, which are respectively the traditional visual surveillance (VS) system and the cloud storage system. The cloud storage system can also be integrated with intelligent visual surveillance, mobile visual surveillance and other visual surveillance subsystems and the architecture is similar to that defined in this clause and is not described in this Recommendation.

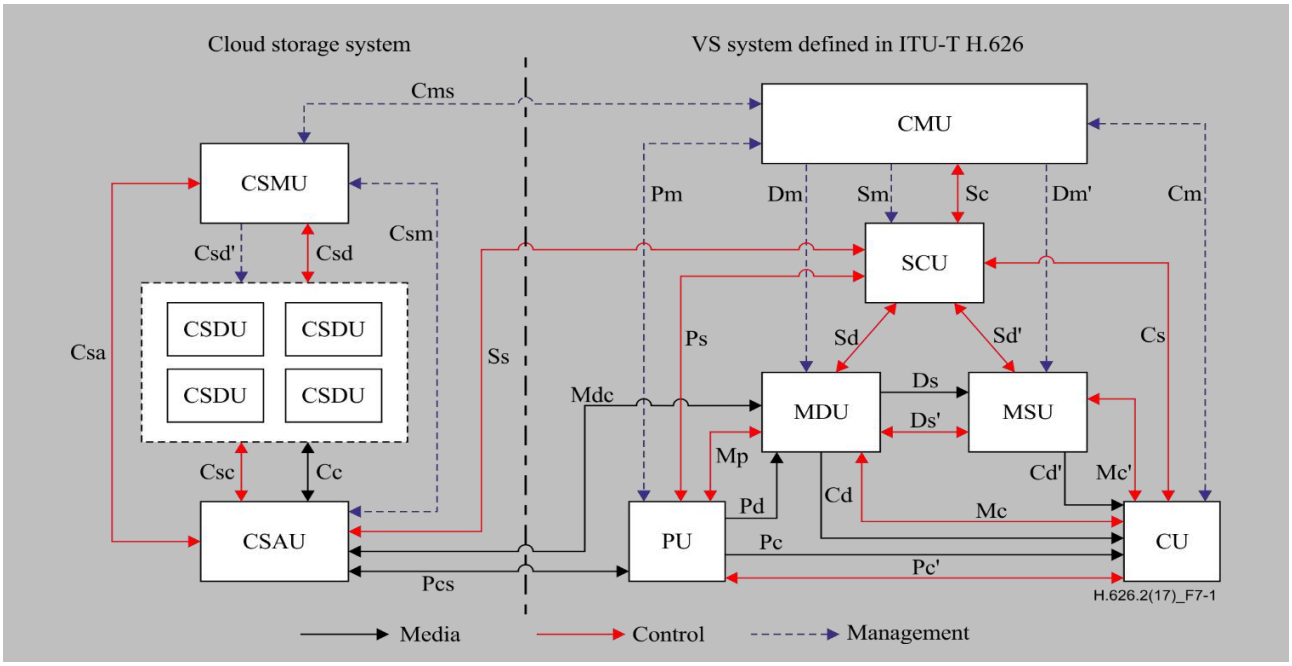


Figure 7-1 – Architectural framework for cloud storage in visual surveillance

The traditional VS service is a telecommunication service focusing on video (and audio) application technology, which is used to remotely capture multimedia (such as audio, video, image and various alarm signals) and present them to end users in a friendly manner (including accessibility aspects). The traditional VS system mainly includes six functional entities, which are the centre management unit (CMU), the service control unit (SCU), the media distribution unit (MDU), the media storage unit (MSU), the premises unit (PU) and the customer unit (CU). The function description of each functional entity is defined in [ITU-T H.626].

A visual surveillance cloud storage can provide a shared pool of configurable storage resources and related data storage functions to the VS applications. In a cloud storage system, the storage resources can be dynamically assigned and reassigned according to the users' demands. The cloud storage part mainly includes three functional entities, which are the cloud storage management unit (CSMU), the cloud storage data unit (CSDU) and the cloud storage access unit (CSAU).

– CSMU is used to provide the management services for the cloud storage system in the VS system.
– CSDU is the data node in a cloud storage system. A number of CSDUs are organized in a distributed way as a storage resource pool by using virtualization technology and the virtualized storage resource can be dynamically provided to the users on demand. The CSDUs are used to store the massive multimodal data produced by the VS system.
– CSAU is the key unit for implementing communication between the CSDU and the media data related units defined in the traditional VS system [ITU-T H.626]. The main functions of the CSAU include: receiving and responding to the control information of the CSMU, receiving and responding to the control information of the SCU, receiving the media data from MDU or PU, sending the media data to the MDU or other related visual surveillance entities, writing the media data into the CSDU cluster and reading the media data from the CSDU cluster.

7.2 Functional entities

7.2.1 Cloud storage management unit

The cloud storage management unit (CSMU) is used to provide the management services for the cloud storage system and respond to service requests of the VS system. The main functions of the CSMU include storage resource management, data management, user management, service management, log management and security control. The CSMU is used to achieve collaboration among the different storage devices and guarantee better access performance of the multimodal surveillance data.

7.2.2 Cloud storage data unit

The cloud storage data unit (CSDU) is the data node in a cloud storage system which is used to store the massive multimodal data produced by the VS system. A typical visual surveillance cloud storage system has a number of CSDUs, which are organized in a distributed way as a storage resource pool by using virtualization technology. The CSDU can be dynamically extended according to the user's demand and the virtualized storage resource can be dynamically provided to the users on demand. The CSDU can receive media data from the CSAU and write the data onto its local storage device. In addition, the CSDU can read and transmit the stored data to the CSAU according to the data reading requests.

7.2.3 Cloud storage access unit

The cloud storage access unit (CSAU) is the key unit for implementing communication between the CSDU and the media data related units defined in the VS system [ITU-T H.626]. As shown in Figure 7-2, the functions of the CSAU are divided into three categories, which are the service control function, the media control function and the configuration management function.

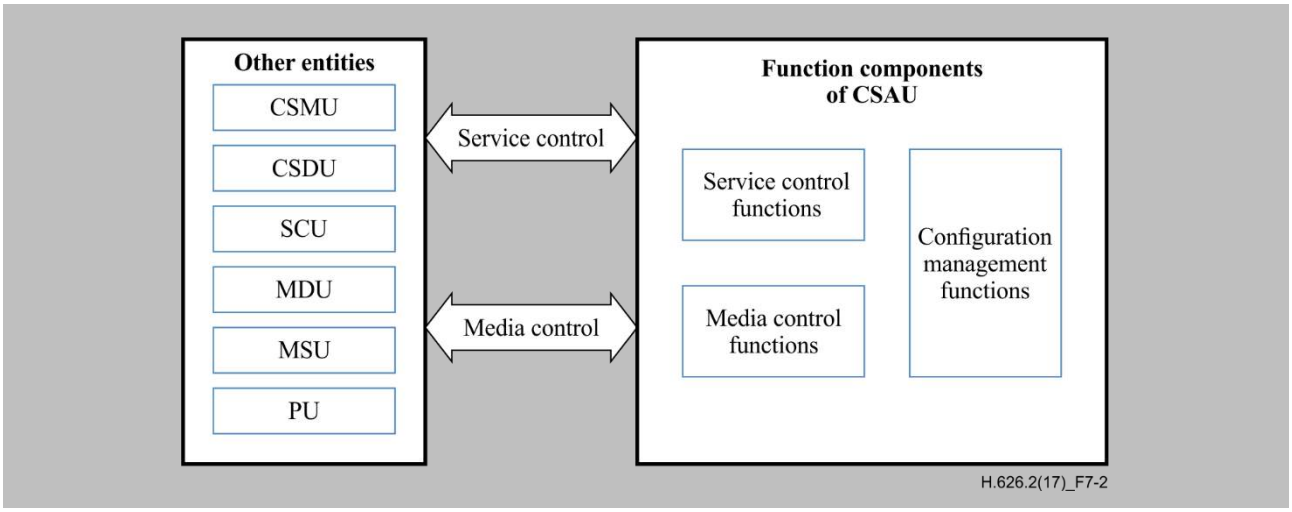


Figure 7-2 – Function components of CSAU

Service control function

– initiate, maintain and release the connection with the SCU;

– process the service requests from the CSMU, forward them to the SCU and respond to the CSMU.

Media control function

– receive media data from the MDU, the PU, the MSU and/or other data source entities of the VS system;

– transmit or forward media data into the CSDU cluster;

– receive media data distributed in the CSDU cluster;

– transmit or forward media data to the MDU, the CU and/or other related entities of the VS system.

Configuration management function

– manage the overall configuration in the CSAU, including the service control, data transmission and other media storage control.

7.3 Reference points

7.3.1 Reference point Pcs: PU-CSAU

The reference point Pcs is located between the PU and the CSAU. It is used to deliver the media data directly from the PU to the CSAU according to the media storage requests.

7.3.2 Reference point Mdc: MDU-CSAU

The reference point Mdc is located between the MDU and the CSAU. It is used for the media data transmission between the MDU and the CSAU according to the media reading and writing requests.

7.3.3 Reference point Ss: CSAU-SCU

The reference point Ss is located between the CSAU and the SCU. It is used to control the CSAU registration, access authentication, authorization and accounting by the SCU and is used for the control signal transmission between the CSAU and the SCU.

7.3.4 Reference point Cms: CMU-CSMU

The reference point Cms is located between the CMU and the CSMU. It is used for the management signal transmission between the CMU and the CSMU.

7.3.5 Reference point Csm: CSMU-CSAU

The reference point Csm is located between the CSMU and the CSAU. It is used by the CSMU to manage the service control function, the media control function and the configuration management function of the CSAU.

7.3.6 Reference point Csd: CSMU-CSDU

The reference point Csd is located between the CSMU and the CSDU. It is used for the control signal transmission between the CSMU and the CSDU.

7.3.7 Reference point Csd': CSMU-CSDU

The reference point Csd' is located between the CSMU and the CSDU. It is used to support the storage space management. The main functions are as follows.

– increase or decrease the storage space flexibly according to the users' demands;

– support data management in the CSDU, including data addition, data deletion, data browsing and data retrieval, etc.

7.3.8 Reference point Csc: CSDU-CSAU

The reference point Csc is located between the CSDU and the CSAU. It is used for the media access control signal transmission between the CSAU and the CSDU.

7.3.9 Reference point Cc: CSDU-CSAU

The reference point Cc is located between the CSAU and the CSDU. It is used for the media data transmission between the CSAU and the CSDU.

7.3.10 Reference point Csa: CSMU-CSAU

The reference point Csa is located between the CSAU and the CSMU. It is used for the access control signal transmission between the CSMU and the CSAU.

7.4 Service control flow

7.4.1 Real-time media storage

When a user wants to store the real-time media obtained from the PU into the cloud storage system, the CU initiates a storage request and sends it to the SCU to start the media storage.

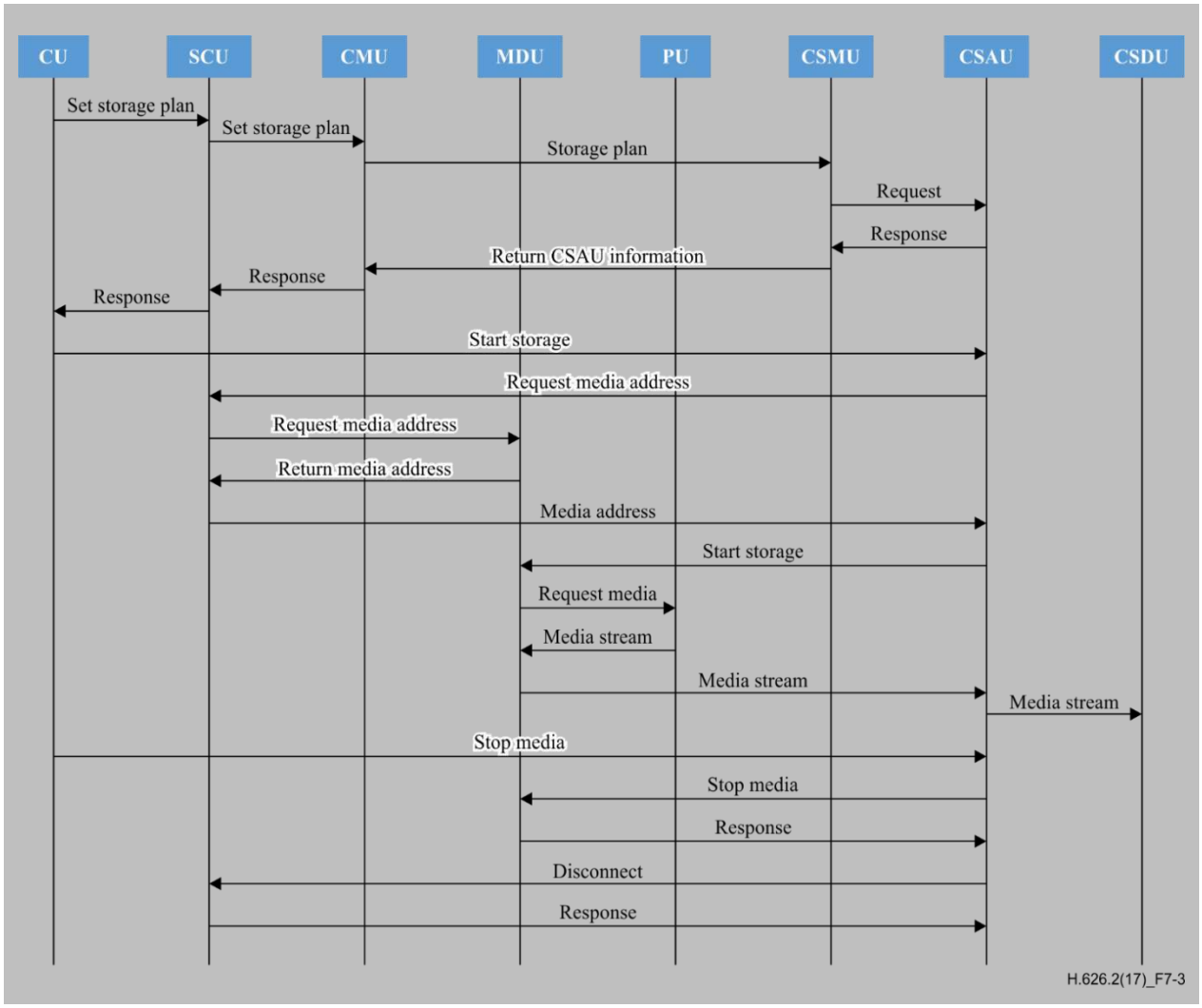


Figure 7-3 – High-level procedural flows for real-time media storage

Figure 7-3 shows the procedural flows of real-time media storage in a cloud storage system:

(1) The CU initiates a storage plan request and sends this request to the SCU.

(2) The SCU forwards this storage plan request to the CMU.

(3) The CMU authenticates the storage access permission and then sends this storage plan request to the CSMU.

(4) The CSMU authenticates the storage access permission and then sends this storage plan request to the CSAU.

(5) The CSAU returns a response to the CSMU when it is ready for this storage plan.

(6) The CSMU returns the CSAU information to the CMU.

(7) The CMU sends a response including the CSAU information to the SCU.

(8) The SCU forwards this response to the CU.

(9) When the CU receives the CSAU information, it sends the real-time media storage request to the CSAU.

(10) When the CSAU receives the storage request, it sends a request to the SCU for the media address.

(11) The SCU forwards this request to the MDU.

(12) The MDU returns the media address to the SCU.

(13) The SCU transfers the media address to the CSAU.

(14) After receiving the real-time media address, the CSAU requests the MDU to start transmitting the media stream.

(15) The MDU sends a request to the PU for initiating a media stream.

(16) The PU creates a media channel with the MDU and sends the media stream to the MDU.

(17) The MDU transfers the media stream to the CSAU.

(18) The CSAU transfers this media stream to the CSDU to store it in the cloud data nodes.

(19) When the storage plan is completed, the CU sends a stop-media request to the CSAU.

(20) The CSAU transfers this stop request to the MDU.

(21) The MDU returns a response to the CSAU.

(22) The CSAU requests the SCU to disconnect.

(23) The SCU returns a response to end this real-time media storage.

7.4.2 Video file storage

A network video recorder (NVR) is usually used as a typical MSU for continuously recording the surveillance video from network cameras. When a user wants to upload a video file from the NVR to the cloud storage system, the CU initiates a storage request and sends it to the SCU to start the media storage.

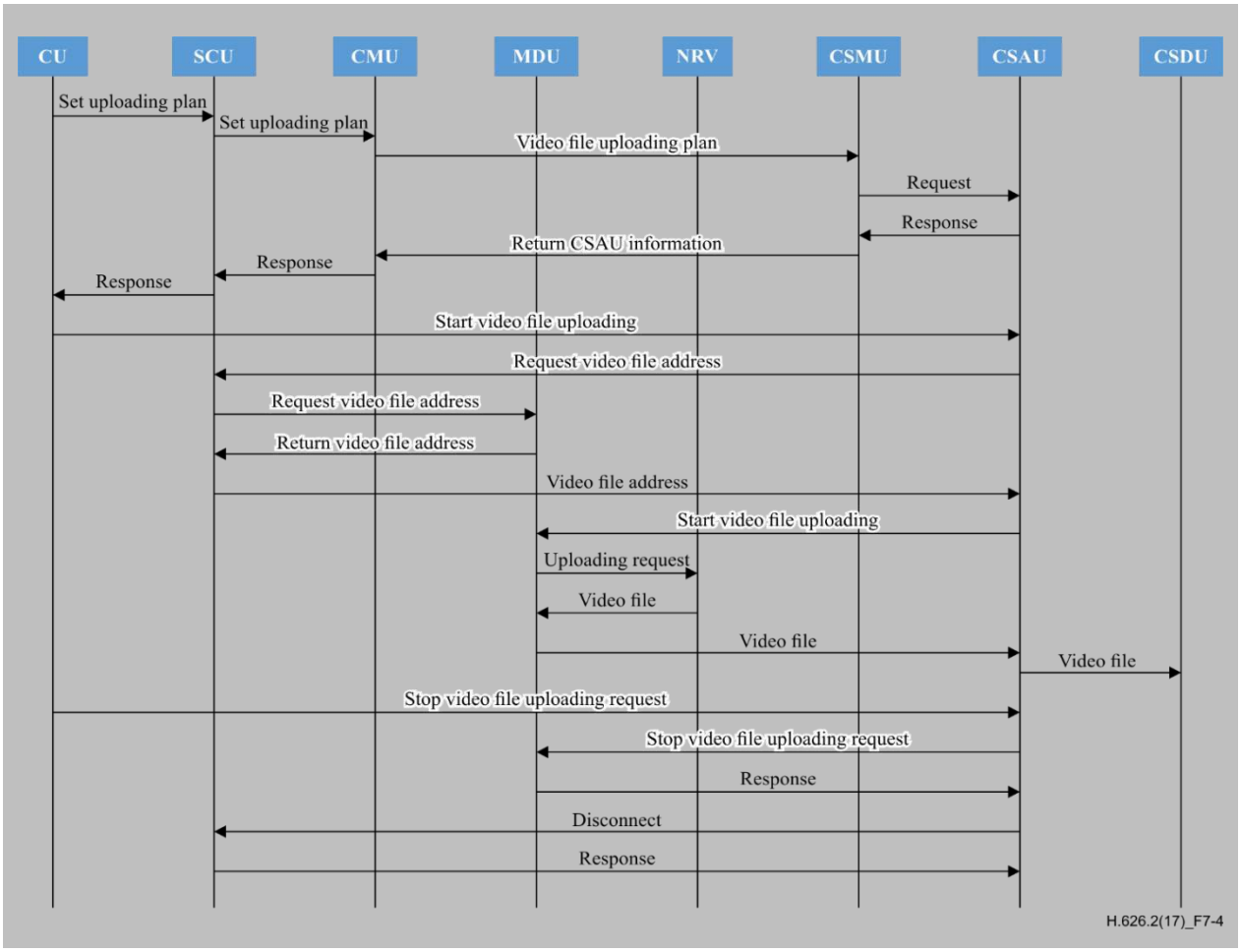


Figure 7-4 – High-level procedural flows for video file uploading from NVR

Figure 7-4 shows the procedural flows of video file uploading from the NVR to the cloud storage system:

(1) The CU initiates a video file uploading plan request and sends this request to the SCU.

(2) The SCU forwards this uploading plan request to the CMU.

(3) The CMU authenticates the uploading access permission and then sends this uploading plan request to the CSMU.

(4) The CSMU authenticates the uploading access permission and then sends this uploading plan request to the CSAU.

(5) The CSAU returns a response to the CSMU when it is ready for this video file uploading plan.

(6) The CSMU returns the CSAU information to the CMU.

(7) The CMU sends a response to the SCU.

(8) The SCU forwards this response to the CU.

(9) When the CU receives the CSAU information, it sends the video file uploading request to the CSAU.

(10) When the CSAU receives the uploading request, it sends a request to the SCU for the data source address.

(11) The SCU forwards the request to the MDU.

(12) The MDU returns the file address to the SCU.

(13) The SCU transfers the file address to the CSAU.

(14) After receiving the file address, the CSAU requests the MDU to start video file uploading from the NVR.

(15) The MDU sends a request to the NVR for obtaining the video files.

(16) The NVR creates a video transmission channel with the MDU and sends the video files to the MDU.

(17) Then MDU transfers the video files to the CSAU.

(18) The CSAU transfers the video files to the CSDU to store them in the cloud data nodes.

(19) When the storage plan is completed, the CU sends a stop request to the CSAU.

(20) The CSAU transfers this stop-media request to the MDU.

(21) Then MDU returns a response to the CSAU.

(22) The CSAU requests the SCU to disconnect.

(23) The SCU returns a response to end this video file uploading.

7.4.3 Image storage

The network cameras continuously capture images. When a user wants to store these images directly into the cloud storage system, the CU initiates a request to the SCU to start the image storage.

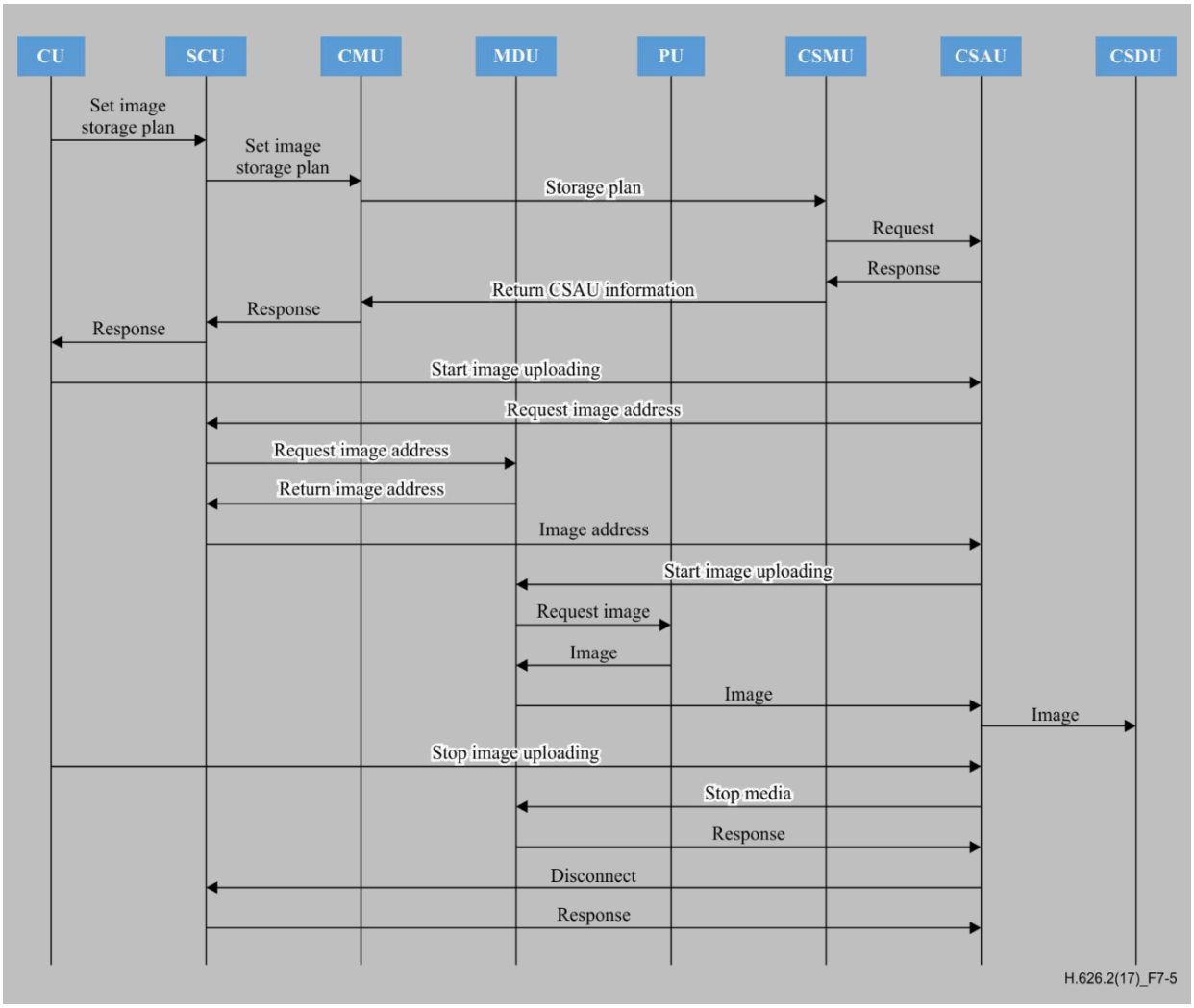


Figure 7-5 – High-level procedural flows for image uploading from surveillance camera

Figure 7-5 shows the procedural flows of the image uploading from the PU to the cloud storage system:

(1) The CU initiates an image storage request and sends this request to the SCU.

(2) The SCU forwards this image uploading plan request to the CMU.

(3) The CMU authenticates the uploading access permission and then sends this uploading plan request to the CSMU.

(4) The CSMU authenticates the uploading access permission and then sends this uploading plan request to the CSAU.

(5) The CSAU returns a response to the CSMU when it is ready for this uploading plan.

(6) The CSMU returns the CSAU information to the CMU.

(7) The CMU sends a response to the SCU.

(8) The SCU forwards this response to the CU.

(9) When the CU receives the CSAU information, it sends the image storage request to the CSAU.

(10) When the CSAU receives the request, it sends a request to the SCU for the data source address.

(11) The SCU forwards the request to the MDU.

(12) The MDU returns the address to the SCU.

(13) The SCU transfers the data source address to the CSAU.

(14) After receiving the data source address, the CSAU requests the MDU to start the image uploading from the PU.

(15) The MDU sends a request to the PU for obtaining the captured images.

(16) The PU creates an image transmission channel with the MDU and sends the captured images to the MDU.

(17) The MDU transfers the images to the CSAU.

(18) The CSAU transfers the images to the CSDU to store the received images in the cloud data nodes.

(19) When the storage plan is completed, the CU sends a stop request to the CSAU.

(20) The CSAU transfers this stop request to the MDU.

(21) The MDU returns a response to the CSAU.

(22) The CSAU requests the SCU to disconnect.

(23) The SCU returns a response to end the image uploading from the PU.

7.4.4 Video metadata or image metadata storage

The intelligent visual surveillance system can provide various intelligent services by using video or image analysis technologies. One solution is to implement some intelligent visual analysis algorithms in the PU that is defined as the intelligent premises unit (IPU). When a user wants to store video metadata or image metadata extracted from the original video or image data in the cloud storage system, the CU initiates a request to the SCU to start this procedure.

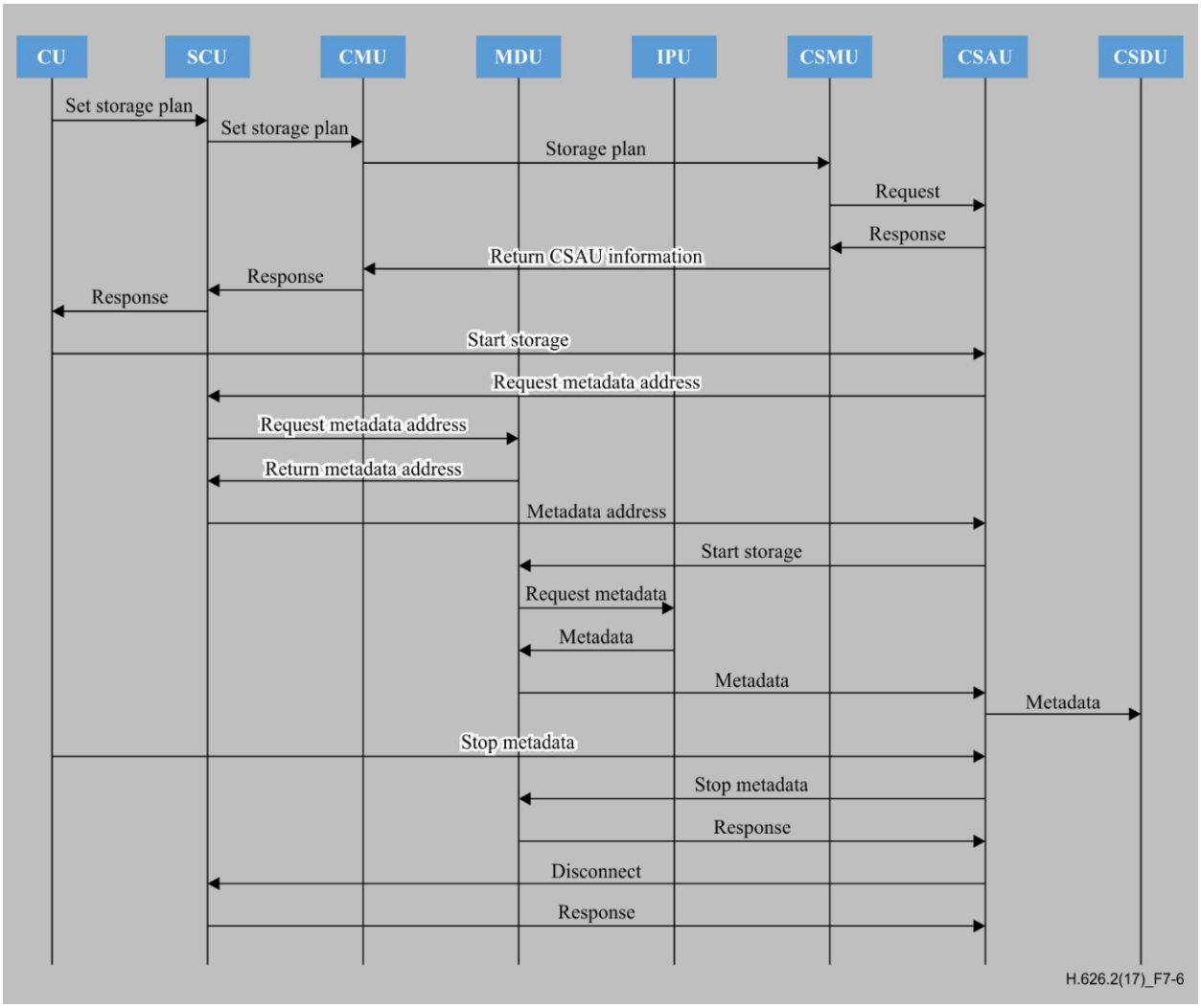


Figure 7-6 – High-level procedural flows for video metadata or image metadata storage

Figure 7-6 shows the procedural flows of the video metadata or image metadata storage in cloud storage system:

(1) The CU initiates a storage plan request and sends this request to the SCU.

(2) The SCU forwards this storage plan request to the CMU.

(3) The CMU authenticates the storage access permission and then sends this storage plan request to the CSMU.

(4) The CSMU authenticates the storage access permission and then sends this storage plan request to the CSAU.

(5) The CSAU returns a response to the CSMU when it is ready for this storage plan.

(6) The CSMU returns the CSAU information to the CMU.

(7) The CMU sends a response to the SCU.

(8) The SCU forwards this response to the CU.

(9) When the CU receives the CSAU information, it sends the video metadata or image metadata storage request to the CSAU.

(10) When the CSAU receives the storage request, it sends a request to the SCU for the metadata address.

(11) The SCU forwards the request to the MDU.

(12) The MDU returns the metadata address to the SCU.

(13) The SCU transfers the metadata address to the CSAU.

(14) After receiving the metadata address, the CSAU requests the MDU to start transmitting the metadata.

(15) The MDU sends a request to the IPU for the video metadata or image metadata.

(16) The IPU creates a media channel with the MDU and sends the metadata to the MDU.

(17) The MDU transfers the metadata to the CSAU.

(18) The CSAU transfers the metadata to the CSDU to store it in the cloud data nodes.

(19) When the storage plan is completed, the CU sends a stop request to the CSAU.

(20) The CSAU transfers this stop request to the MDU.

(21) The MDU returns a response to the CSAU.

(22) The CSAU requests the SCU to disconnect.

(23) The SCU returns a response to end this metadata storage.

7.4.5 Media acquisition from the cloud storage system

When a user wants to view the media stored in a cloud storage system, the CU initiates a request to the SCU in order to acquire the media.

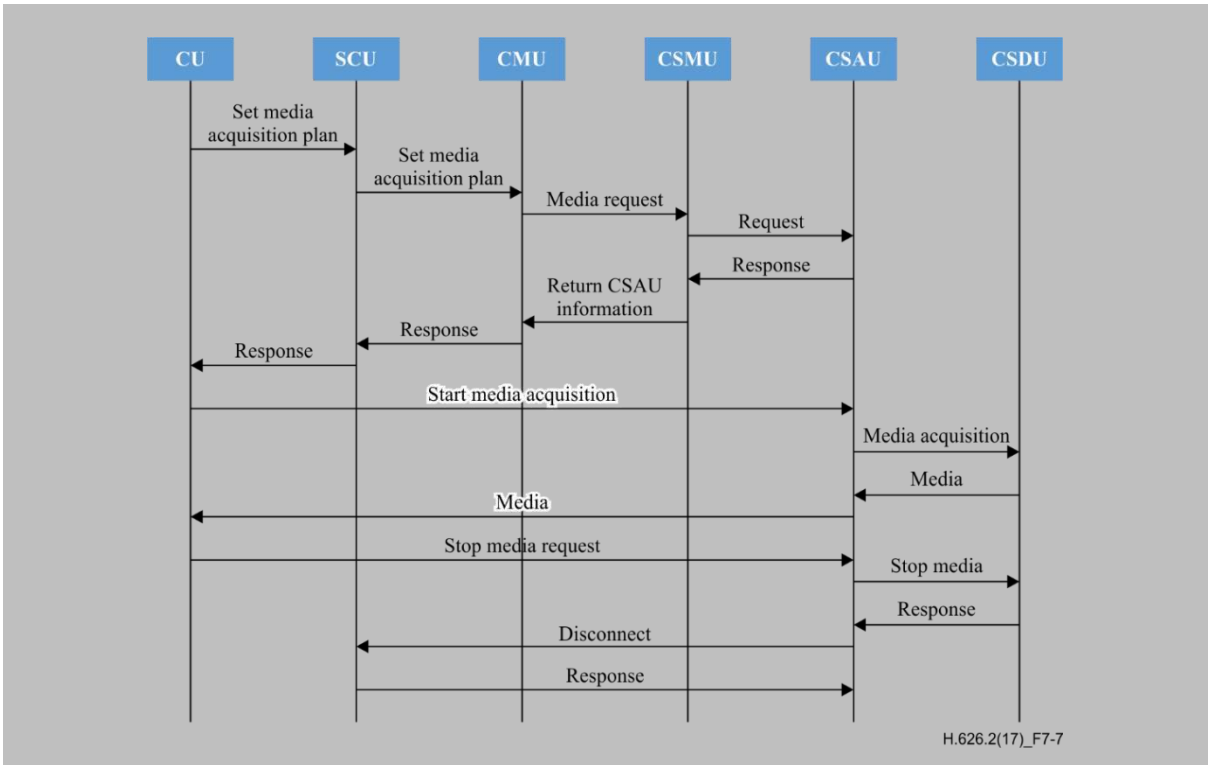


Figure 7-7 – High-level procedural flows for media acquisition

Figure 7-7 shows the procedural flows of the media acquisition from the cloud storage system to the CU:

(1) The CU initiates a media acquisition request and sends this request to the SCU.

(2) The SCU forwards this acquisition request to the CMU.

(3) The CMU authenticates the acquisition access permission and then sends this request to the CSMU.

(4) The CSMU authenticates the acquisition access permission and then sends this request to the CSAU.

(5) The CSAU returns a response to the CSMU when it is ready for this media acquisition request.

(6) The CSMU returns the CSAU information to the CMU.

(7) The CMU sends a response to the SCU.

(8) The SCU forwards this response to the CU.

(9) When the CU receives the response, it sends a media acquisition request to the CSAU.

(10) The CSAU transfers this request to the CSDU.

(11) After receiving this request, the CSDU creates a media channel with the CSAU to transmit the required media data.

(12) The CSAU transfers the media data to the CU.

(13) When the CU stops the media acquisition, it sends a stop request to the CSAU.

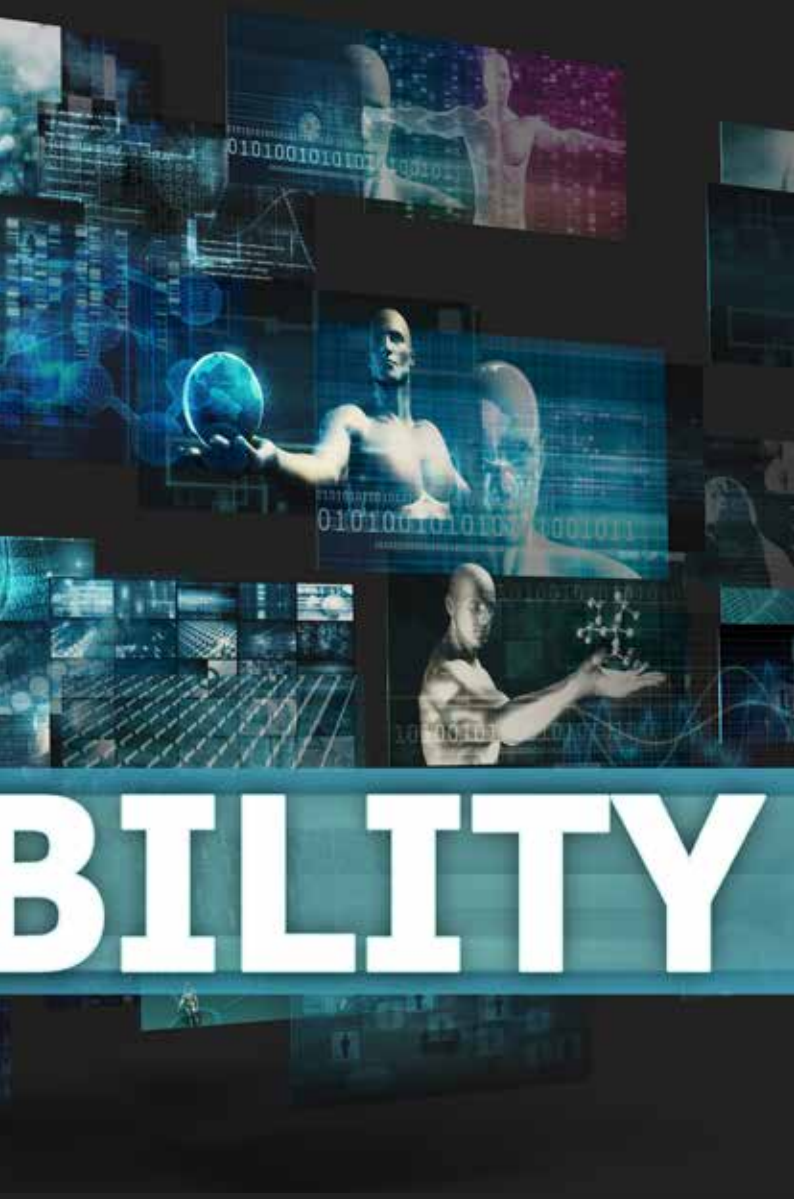
(14) The CSAU transfers this request to the CSDU.

(15) The CSDU returns a response to the CSAU.

(16) The CSAU requests the SCU to disconnect.

(17) The SCU returns a response to end this media acquisition operation.


INTEROPERA



5.

Intercloud and interoperability

Cloud computing – Trusted inter-cloud computing framework and requirements

Recommendation ITU-T Y.3514

(05/2017)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Summary

Recommendation ITU-T Y.3515 specifies a framework of trusted inter-cloud computing and relevant use cases. It provides general requirements for trusted inter-cloud and specific ones related to governance, management, resiliency, security and confidentiality of trusted inter-cloud

Keywords

Cloud computing, confidentiality, governance, inter-cloud, management, resiliency, security, trust.

Table of Contents

1 Scope

This Recommendation specifies a framework of trusted inter-cloud computing and relevant use cases, based on the framework of inter-cloud computing [ITU-T Y.3511]. The scope of this Recommendation includes:

– an overview of trusted inter-cloud computing;
– general requirements for trusted inter-cloud;
– requirements for governance of trusted inter-cloud;
– requirements for management of trusted inter-cloud;
– requirements for resiliency of trusted inter-cloud;
– requirements for security and confidentiality of trusted inter-cloud.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1601] Recommendation ITU-T X.1601 (2014), *Security framework for cloud computing.*

[ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary.*

[ITU-T Y.3501] Recommendation ITU-T Y.3501 (2016), *Cloud computing – Framework and high-level requirements.*

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014) | ISO/IEC 17789:2014, *Information technology – Cloud computing – Reference architecture.*

[ITU-T Y.3511] Recommendation ITU-T Y.3511 (2014), *Framework of inter-cloud computing.*

[ITU-T Y.3520] Recommendation ITU-T Y.3520 (2015), *Cloud computing framework for end to end resource management.*

[ITU-T Y.3521] Recommendation ITU-T Y.3521 (2016), *Overview of end-to-end cloud computing management.*

[ITU-T Y.3522] Recommendation ITU-T Y.3522 (2016), *End-to-end cloud service lifecycle management requirements.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 availability [ITU-T Y.3500]: Property of being accessible and usable upon demand by an authorized entity.

3.1.2 confidentiality [ITU-T Y.3500]: Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

3.1.3 cloud computing [ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

3.1.4 cloud service [ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.5 cloud service customer [ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

NOTE – A business relationship does not necessarily imply financial agreements.

3.1.6 cloud service partner [ITU-T Y.3500]: Party which is engaged in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer, or both.

3.1.7 cloud service provider [ITU-T Y.3500]: Party which makes cloud services available.

3.1.8 governance [b-ISO/IEC 38500:2015]: System of directing and controlling.

3.1.9 information security [b-ISO/IEC 27000:2016]: Preservation of confidentiality, integrity and availability of information.

NOTE – In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

3.1.10 integrity [ITU-T Y.3500]: Property of accuracy and completeness.

3.1.11 inter-cloud computing [ITU-T Y.3511]: The paradigm for enabling the interworking between two or more cloud service providers.

NOTE – Inter-cloud computing is also referred as inter-cloud.

3.1.12 service level agreement [ITU-T Y.3500]: Documented agreement between the service provider and customer that identifies services and service targets.

NOTE 1 – A service level agreement can also be established between the service provider and a supplier, an internal group or a customer acting as a supplier.

NOTE 2 – A service level agreement can be included in a contract or another type of documented agreement.

3.1.13 service management interface [ITU-T Y.3521]: Interface that provides a set of management capabilities exposed by a cloud service through which the cloud service can be managed.

NOTE – For additional details of SMI concepts, see [ITU-T Y.3520] and [b-TMF TR198].

3.1.14 trusted cloud service [ITU-T Y.3501]: A cloud service that satisfies a set of requirements such as transparency for governance, management and security so that a cloud service customer (CSC) can be confident in using the cloud service.

NOTE 1 – The set of requirements will vary depending on the involved cloud service customer, the nature of the cloud service and the governing jurisdiction.

NOTE 2 – The set of requirements could also be related to additional cross-cutting aspects [ITU-T Y.3502] such as performance, resiliency, reversibility, SLAs, etc.

NOTE 3 – Transparency means that the cloud service provider (CSP) should commit to the CSC that they have appropriate and clear control and reporting mechanisms for governance, management and security, such as SLA commitments, online announcements, data handling policies, etc.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 dependability: The availability performance and its influencing factors on reliability performance, maintainability performance and maintenance support performance.

3.2.2 inter-cloud governance: System by which the use of inter-cloud is directed and controlled.

3.2.3 reliability: The ability of a system, product or component to perform and maintain under stated conditions as required for a specified period of time.

3.2.4 resiliency: The ability of a system, product or component to provide, maintain, or return to an acceptable level of service in the face of faults (unintentional, intentional or naturally caused) affecting normal operation.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAA	Authentication, Authorization and Accounting
BSS	Business Support System
CSC	Cloud Service Customer
CSN	Cloud Service Partner
CSP	Cloud Service Provider
DDoS	Distributed Denial of Service
KPI	Key Performance Indicator
MSA	Master Service Agreement
NaaS	Network as a Service
NAT	Network Address Translation
NFV	Network Functions Virtualization
OSS	Operations Support System
PaaS	Platform as a Service
PII	Personally Identifiable Information
QoS	Quality of Service
SaaS	Software as a Service
SDN	Software-Defined Networking
SLA	Service Level Agreement
SMI	Service Management Interface
vFW	Virtual Firewall
vHGW	Virtual Home Gateway
vLB	Virtual Load Balancer
vNAT	Virtual Network Address Translation

5 Conventions

In this Recommendation:

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The keywords "**is recommended"** indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

6 Overview of trusted inter-cloud

The inter-cloud computing concept is based on the relationship (pattern) among multiple cloud service providers (CSPs). This pattern (peering, federation or intermediary) allows the CSP to interwork with one or more peer CSPs to assure intermediation and security of services provided by these CSPs.

The trusted inter-cloud relationship among multiple CSPs relies on confidence between cloud service customer (CSC) and CSP, or between CSPs. One of them has to delegate physical control over application, service, resource and data to the others. The appropriate security mechanisms (e.g., security access control, security of network connectivity between the CSPs) are needed during peer CSPs interactions to achieve trusted inter-cloud computing.

The relevant CSPs form a common trusted inter-cloud to establish a trust relationship between them. In particular, the multiple CSPs involved in inter-cloud may be administered by different parties. In case of an inter-cloud federation, the involved CSPs may establish trust relationships among them prior to any interactions between them or during inter-cloud interactions (e.g., service requests between CSPs).

The specifics of trusted inter-cloud computing are different depending on the technologies used by CSC or CSP. Therefore, the management of trusted inter-cloud takes into account different levels of security.

Trusted inter-cloud relationships can be expressed through cross-cutting aspects (identified in [ITU-T Y.3502]), such as the **governance, management, resiliency** and **security** of inter-cloud.

Trusted inter-cloud computing covers security threats for CSC and threats for CSP. The specific threats depend on the level of responsibilities and control between the CSC and CSP, or between CSPs (such as those identified in [ITU-T X.1601]). In trusted inter-cloud systems, the control can be exchanged between CSC and CSP or between CSPs to achieve security continuum. The **security** of inter-cloud can be realized based on:

a) self-service security which enables self-service management of security in heterogeneous cloud infrastructures and provides flexible mechanisms to let CSC or CSP control the security of their cloud computing resources in a fine-grained manner;

b) self-managed security which enables full automation of security management in order to reduce operational costs while adding more flexibility and providing a unified view of security in heterogeneous cloud computing environments;

c) end-to-end security which implements a distributed security abstraction layer between endpoints defined by the CSC to overcome the heterogeneity of security technologies across multi-cloud environments and to manage trust relationships between different layers and across CSPs, to provide a unified user experience of security.

The **governance** of inter-cloud means the system by which inter-cloud is directed and controlled. A governance system has to monitor and to control usage of cloud computing system in both horizontal (cross-provider) and vertical (cross-layer) dimensions with a high level of automation.

The **resiliency** of inter-cloud means the ability of multi-cloud environment to provide and to maintain an acceptable quality level of service in the face of faults (unintentional, intentional or naturally caused) affecting normal operations.

6.1 Governance of trusted inter-cloud

One of the main challenges in inter-cloud computing is to respect security, confidentiality, and compliance requirements of cloud services hosted in a multi-cloud environment. The governance aspects become key parts of service level agreements (SLAs) for cloud services as they allow for usage of cloud services in a transparent manner over all their lifecycle. The governance roles guarantee security and appropriate treatment of cloud applications and cloud data independently of the deployment model. They are specified and targeted for an operational area of cloud computing.

The governance of trusted inter-cloud is based on specific policies and principles which allow for the use of particular cloud services in a trustworthy manner. This needs strongly isolated (physically or logically) instances of cloud services for aspects including identity management, geographic redundancy, support for hybrid scenarios, and effective inter-cloud data (workloads) management. The CSPs establishing a trusted inter-cloud relationship are obliged to determine their policies of decision-making roles, and implement these policies in their management systems.

The governance of trusted inter-cloud can be expressed as a system of directing and controlling an inter-cloud environment to reach objectives for trust. It can be spread over the governance body and governance executive. The governance body consists of a set of representatives of CSPs (person or group of people) who are accountable for the performance and conformance of the trusted inter-cloud environment. The governance executive represents the system by which current and future use of trusted inter-cloud is directed and controlled. The governance executive also provides plans, builds and runs trusted inter-cloud enabled business.

The governance of trusted inter-cloud is a continuous process to monitor particular indicators from systems (e.g., performance, conformance), evaluate proposals and plans, and direct strategy and policies between the governance body and governance executive. The governance body takes into account external trusted inter-cloud conditions related to business pressures, regulatory obligations, source of authority, stake-holders' expectations and business needs.

The trusted inter-cloud governance is based on the following principles:

– responsibility, which indicates clearly defined roles for demand and support of the environment;
– strategy, which is strongly related to phase of plans, builds and runs trusted inter-cloud enabled business;
– acquisition of inter-cloud data, which depends on the business case;
– performance, which has to be realized according to SLAs for cloud services;
– compliance, which covers the necessary respect of laws and regulations;
– human behaviour, which addresses the dynamics of interaction in the governance process.

The governance of trusted inter-cloud can be considered with respect to internal or external aspects. Internal cloud governance allows a CSP to control its own processes in a way that it can give assurance and transparency to other CSPs participating in a trusted inter-cloud environment according to specified expectations in terms of cloud computing cross-cutting aspects [ITU-T Y.3502].

External cloud governance spans processes of monitoring and controlling the inter-cloud environment to reach objectives of trust. This can refer to a service level agreement which provides detailed information about functional and non-functional aspects of cloud services.

For both internal governance and external governance of trusted inter-cloud, these refer to matters that are decided by the governing board of a CSP, such as how policy decisions are made, and how these are converted into policies that can be implemented in the CSP’s management system.

6.2 Management of trusted inter-cloud

Management in trusted inter-cloud computing environments is based on access control mechanisms and a trust management system. They are complementary to each other. Appropriate access control mechanisms guarantee a level of confidentiality and trust between a CSC and CSPs or between CSPs.

Access control mechanisms determine authorization of shifting physical control over applications, services, resources and data. An authorization, authentication and accounting (AAA) module to control the access to cloud computing resources relies on a customisable access control policy model and its implementation requirements. The specification of the access control mechanism is usually predefined in an access control policy. This specification is used to specify permissions and access control to cloud computing resources and cloud services.

The traditional access control mechanisms (e.g., identity-based, lattice-based, role-based, organisation-based, attribute-based) cannot be successfully used in trusted inter-cloud computing due to high dynamics in cloud computing environments. Therefore, new mechanisms based on mixing traditional functionality can be used to control cross-tenant at the policy administration level.

The objectives of access control mechanisms in trusted inter-cloud environment are as follows:

– expressivity as the ability to provide appropriate mechanisms of access control policies. This depends on the implementation;
– granularity as the ability to decompose an access control mechanism into smaller size components. This is in line with granularity of the cloud computing resources and cloud services as well as the SLA established between the CSC and CSP or between CSPs;
– context-awareness as the ability of an authorization mechanism to take context information into consideration when making access decisions. Context awareness is significant in trusted inter-cloud environments due to their distributed nature: access to inter-cloud from different locations, during different time periods, etc.

Appropriate policy language implemented in the trusted inter-cloud environment provides expressiveness beyond the boundary of access control. This should respect security mechanisms of trust management systems to fulfil specified requirements.

Trust management in inter-cloud environments (as an interaction enabler in situations of risk and uncertainty) is considered in cross-provider and cross-layer dimensions. Decisions of the trust management system are typically taken based on the prediction of cloud computing actors' behaviours and are based on the SLA established between CSC and CSP or between CSPs. According to particular needs, trust management can either be CSC-related or CSP-related.

The trust management functionalities are supported by the "Authorisation and security policy management" functional component within the multi-layer functions of the cloud computing reference architecture [ITU-T Y.3502]. The positioning of trust management functionalities across the CSPs which provide inter-cloud services is presented in Figure 6-1.

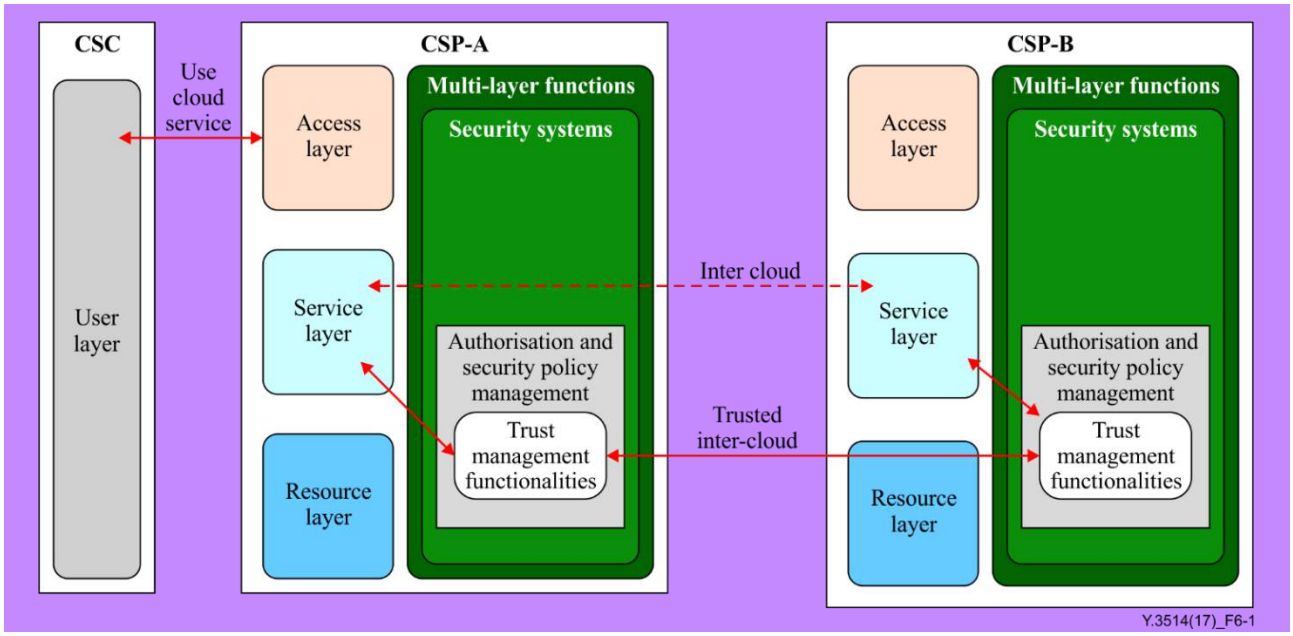


Figure 6-1 – The positioning of trust management functionalities over CSP in inter-cloud

The inter-cloud relation is realised over the particular service layers of CSP-A and CSP-B (dashed line in Figure 6-1). The trusted inter-cloud relation is realised over trust management functionalities of CSP-A and CSP-B located in the "Authorisation and security policy management" functional component, which is located within functionalities of inter-cloud security among CSPs (solid lines in Figure 6-1). The trust management functionalities play an intermediary role between service layers of CSP-A and CSP-B in inter-cloud relations.

The operational model of trust management identifies four modes as follows:

– Mode 1 – the trust management system produces simple answers (i.e., trust or no trust) that states whether the credentials provided by the CSP satisfy the policy;

– Mode 2 – extended Mode 1, with justification when the request is denied, that states which conditions in the policy the provided credentials were unable to satisfy;

– Mode 3 – the trust management system provides an answer with justifications and explanation when the policy is satisfied. The explanation contains all credentials that satisfy the policy;

– Mode 4 – extended Mode 3, with detailed explanation. The detailed explanation is obtained by providing all subsets of credentials that satisfy the policy.

The trust management functionalities are built upon elements as follows:

– **Feedback analyser** which is responsible for the collection and analysis of feedbacks and opinions from a CSC or CSP about another CSC or CSP;

– **SLA analyser** which is responsible for extracting and evaluating SLA metrics;
– **Credential analyser** which verifies chains of trust and evaluates the validity of credentials;
– **Trust requirement handler** which parses and extracts trust requirements;
– **Trust analyser** which encapsulates the policies used to compute trust;
– **Trust requests handler** which orchestrates and coordinates the collaboration of the aforementioned components.

For an overview of cloud SLA, cloud SLA metrics and the relationship between the cloud service agreement and the cloud SLA please refer to [b-ISO/IEC 19086-1].

The relationships between particular elements of trust management functionalities are presented in Figure 6-2.

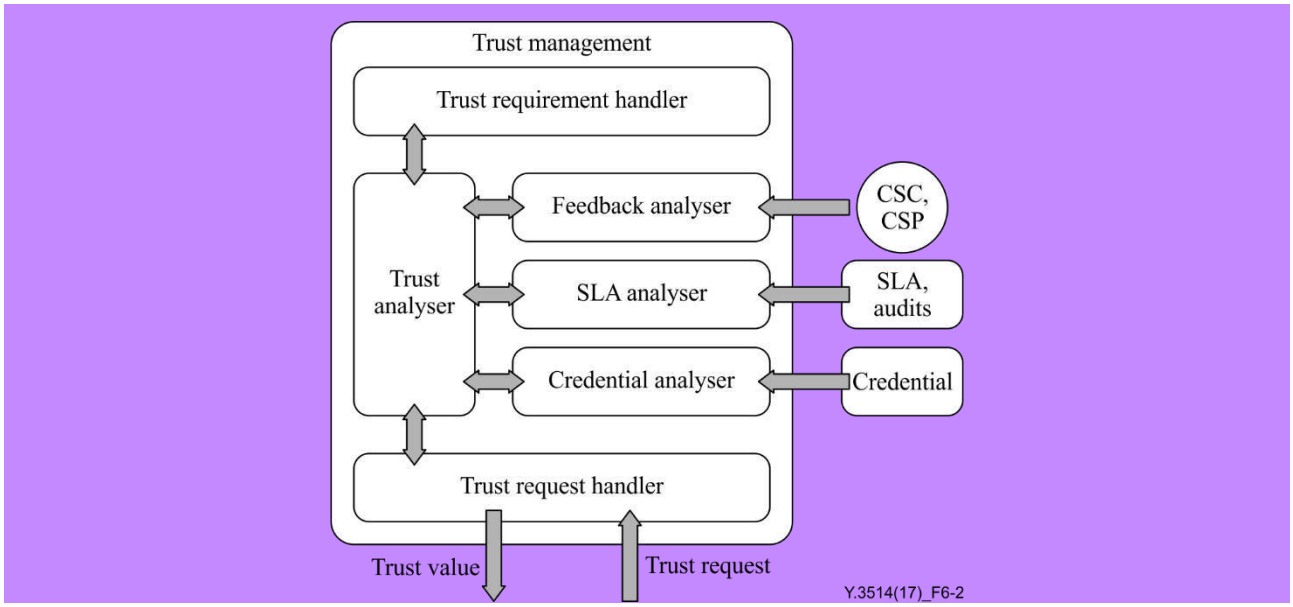


Figure 6-2 – The relationship between particular elements of trust management functionalities

Trust management relies on components for managing isolation and security mechanisms. The components managing isolation ensure cross-layer trust, while components managing security mechanism establish a chain of trust satisfying both horizontal (cross-provider) and vertical (cross-layer) dimensions.

6.3 Resiliency of trusted inter-cloud

Resiliency includes the set of monitoring, preventive and responsive processes that enable a cloud service to provide near-continuous operations, or predictable and verifiable outages (such as scheduled maintenance), through appropriate failure and recovery actions. These include hardware failures, communications and software malfunctions, and can occur as isolated incident or in combination, including cascade of failures. These processes might include both automated and manual actions, usually spanning multiple systems, and thus their description and realisation are part of the overall cloud infrastructure, and not an independent function. Inherent in resiliency is the realisation of risk management – since resiliency is determined by the least resilient component in the system, performance or other factors may limit the extent to which resiliency is achievable or effective. The association of risk to value is realised in the implementation choices to provide resiliency.

Inter-cloud resiliency is interpreted as persistence under uncertainty of performance among multiple CSPs in the face of some set of disturbances that are likely to occur during a specified timeframe.

Trusted inter-cloud resiliency is a set of technical procedures (rely on shifting control and security mechanisms) to:

– monitor CSC or CSP's environment and collect relevant data;

– analyse monitored data;

– predict faults and;

– mitigate or restore the cloud service parameters after service failure (related to certain equipment or software functionality, laws and regulations, local policies, service contracts, etc.) and availability (related to technical systems functionality).

Complementary to trusted inter-cloud resiliency is the reliability of trusted inter-cloud. This means the ability of the trusted inter-cloud environment to perform and maintain under stated conditions as required for a specified period of time.

6.4 Security and confidentiality of trusted inter-cloud

The security and confidentiality of trusted inter-cloud is the main challenge of integrating multiple CSP platforms. This is necessary to provide self-service, self-managed and end-to-end security services for the CSC, and for the CSP to guarantee a level of confidentiality, integrity, as well as availability of services and resources hosted on CSP's cloud computing environments. To establish and specify trust between different cloud computing environments as well as trust between CSC and CSPs, a dedicated security and confidentiality terminology, together with a master service agreement (MSA) is needed.

The security and confidentiality of trusted inter-cloud is based on distributed cloud management. It enables the primary CSP to provide end-to-end dynamic deployment, configuration and unified control of security and confidentiality of cloud services across multiple CSPs. In implementation, distributed cloud management supported trust can be realised by combining specialised protocol design with smart interaction with the underlying cloud network fabric (e.g., using software-defined networking (SDN) traffic engineering and cloud-tailored smart queue management).

To increase security and confidentiality of trusted inter-cloud computing, it is necessary to define a terminology (language) to annotate (or tag) workloads and data with security requirements (such as permissible storage locations). These annotations will be processed by the system during scheduling and migration to ensure that workload constraints are maintained. Additionally, annotation of workloads allows the use of appropriate network data plane mechanisms (e.g., SDN) for strong security protection and traffic isolation in order to ensure that the above constraints are reached when workloads are practically placed, executed (data accessed and stored) and migrated. Such annotation of workloads and data sets might be based on standards for data categorisation.

The security and confidentiality of trusted inter-cloud is realized based on a two dimensional (vertical and horizontal) model as follows. The vertical axis is based on the layers of the cloud computing reference architecture [ITU-T Y.3502]:

– in the higher layers focussed on user-centric security and confidentiality through a unified distribution layer for cloud resources (independently from their type and from underlying CSP), such as user identity management, authentication and authorization;

– in the lower layers focused on provider-independent control, security and confidentiality over the whole distributed inter-cloud infrastructure, such as disk and network encryption.

The horizontal axis is based on the interconnection of CSPs based on the inter-cloud framework [ITU-T Y.3511].

Consequently, security and confidentiality of trusted inter-cloud are based on satisfying both horizontal (cross-provider) and vertical (cross-layer) dimensions.

6.5 Relationship between trusted inter-cloud and the cloud computing reference architecture

The cloud computing reference architecture [ITU-T Y.3502] provides an architectural framework which defines cloud computing roles, sub-roles, cloud computing activities and cross-cutting aspects. It also describes the functional layers and functional components of a cloud computing system. According to this framework, the trusted inter-cloud relationships can be expressed by cross-cutting aspects like security, governance and resiliency that span over cloud computing multi-layer functionality. The conceptual view of cloud computing management is based on cloud computing management layers and the service management interface (SMI) approach [ITU-T Y.3520] and [ITU-T Y.3522].

Trust management in inter-cloud environments can be realized based on the common model for end-to-end cloud computing management [ITU-T Y.3521]. In particular, the operations support system (OSS) functional components encompass the set of management capabilities that are required in order to manage and control trust in an inter-cloud environment. The role of business support system (BSS) functional components remains to encompass the set of business-related management capabilities dealing with customers and supporting processes in a trusted manner (see clause 9.2.5.4 of [ITU-T Y.3502]). Therefore, in a trusted inter-cloud environment, the cloud computing management functionalities [ITU-T Y.3521] can be used to reach objectives of trust satisfying governance, security and resiliency aspects of inter-cloud.

7 General requirements for trusted inter-cloud

This clause identifies general requirements applicable to trusted inter-cloud.

7.1 Data separation

It is required that the CSP provides data separation between workloads to ensure security and confidentiality.

7.2 Data annotation

It is recommended that the CSP supports annotation (tagging) of trusted inter-cloud data (workloads) to enable compliance with regulatory obligations.

7.3 Confidentiality of data

It is required that the CSP respects the confidentiality of the CSC's or CSP's data used in trusted inter-cloud system.

7.4 Operational statistics

It is recommended that the CSP supports operational statistics for trusted inter-cloud services according to appropriate methods of measurement.

7.5 Interoperability and dependability

It is recommended that the CSP supports interoperability and dependability of trusted inter-cloud services.

7.6 Master service agreement

It is recommended that the CSP respects master service agreements to reach objectives of trust satisfying governance, security and resiliency aspects of inter-cloud.

8 Requirements for governance of trusted inter-cloud

This clause provides requirements for governance of trusted inter-cloud derived from the use cases described in Appendix I.

8.1 Geographical policies

It is required that the CSP respects all applicable geographical policies in order to realise requests from the CSC or other CSP.

It is recommended that the CSP integrates and validates cloud services from peer CSPs with respect to geographical policies.

It is recommended that the CSP validates and supports resiliency cloud services from peer CSPs with respect to geographical policies.

NOTE – A geographical policy can be conditional, for example "data shall not leave country X *unless* this movement is necessary to continue service during a major outage".

8.2 Governance policies

It is required that the CSP respects governance policies to reach objectives of trusted inter-cloud.

8.3 Governance roles

It is required that the CSP respects governance roles to reach objectives of trusted inter-cloud.

8.4 Regulatory policies

It is required that the CSP complies with applicable data regulation policies (e.g., medical, financial, defence, etc.) and business regulatory policies related to inter-cloud.

NOTE – Regulation policies concern regulations applied to particular types of businesses.

8.5 Laws and regulations

It is required that the CSP complies with applicable laws and regulations as well as local policies.

9 Requirements for management of trusted inter-cloud

This clause provides requirements for management of trusted inter-cloud derived from the use cases described in Appendix I.

9.1 Management policies

It is required that the CSP respects management policies applied to trusted inter-cloud.

9.2 Management roles

It is required that the CSP respects management roles applied to trusted inter-cloud.

9.3 Distributed data

It is recommended that the CSP supports management of distributed data in trusted inter-cloud.

9.4 Identity management

It is recommended that the CSP provides identity management to enable compliance with CSC policy in trusted inter-cloud.

9.5 Access management

It is recommended that the CSP provides access management to enable compliance with CSC policy in trusted inter-cloud.

9.6 Policy language

It is recommended that the CSP supports policy language (related to data annotation) to increase confidentiality of trusted inter-cloud.

10 Requirements for resiliency of trusted inter-cloud

This clause provides requirements for resiliency of trusted inter-cloud derived from the use cases described in Appendix I.

10.1 Service monitoring

It is recommended that the CSP monitors quality of trusted inter-cloud service in real time.

10.2 Service continuity

It is recommended that the CSP supports the resiliency of trusted inter-cloud services in order to respect service continuity in accordance with the SLA established between CSC and CSP or between CSPs.

10.3 Resiliency policies

It is recommended that the CSP integrates and validates cloud services from peer CSPs with respect to resiliency policies.

10.4 Resiliency validation

It is recommended that the CSP validates resiliency of cloud service from peer CSPs.

11 Requirements for security and confidentiality of trusted inter-cloud

This clause provides requirements for security and confidentiality of trusted inter-cloud derived from the use cases described in Appendix I.

11.1 Security and confidentiality policies

It is recommended that the CSP supports unified (commonly adopted) security and confidentiality policies and metadata.

11.2 Level of robustness

It is recommended that the CSP supports appropriate levels of robustness.

11.3 Security policy negotiation

It is recommended that the CSP supports security policy negotiation.

11.4 Security and confidentiality policy

It is required that the CSP respects the security and confidentiality policies established between CSC and CSP or between CSPs.

11.5 Data security

It is recommended that the CSP supports on-demand data security services.

11.6 Security policy monitoring

It is recommended that the CSP supports deployment and monitoring of security policies related to inter-cloud.

12 Security considerations

Security aspects for consideration within the cloud computing environment, including inter-cloud computing, are described in [ITU-T X.1601], which analyses security threats and challenges, and describes security capabilities that could mitigate these threats and meet the security challenges.

Appendix I

Use case of trusted inter-cloud computing

(This appendix does not form an integral part of this Recommendation.)

I.1 Use case template

The use cases developed in Appendix I should adopt the following unified format for better readability and convenient material organization.

Title	Note: The title of the use case
Description	Note: Scenario description of the use case
Roles	Note: Roles involved in the use case
Figure (optional)	Note: Figure to explain the use case, but not mandatory
Pre-conditions (optional)	Note: The necessary pre-conditions that should be achieved before starting the use case
Post-conditions (optional)	Note: The post-condition that will be carried out after the termination of current use case
Derived requirements	Note: Requirements derived from the use cases, whose detailed description is presented in the dedicated chapter

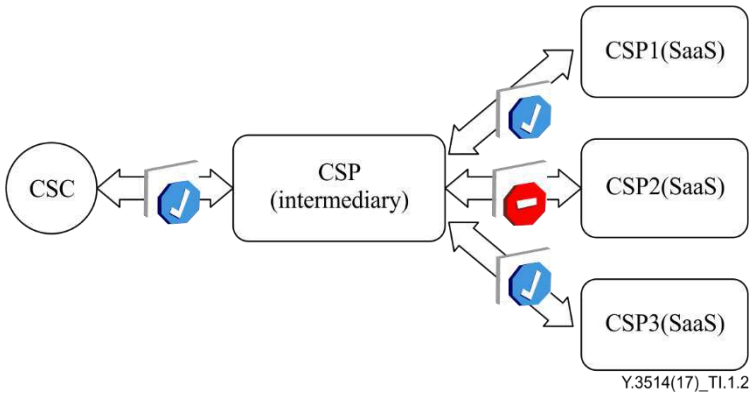
I.2 Trusted inter-cloud related use cases

I.2.1 Use case of access security in trusted inter-cloud

This use case illustrates the security aspects of trusted inter-cloud between the primary CSP and secondary CSPs. The intermediary pattern of inter-cloud used to illustrate the use case is an example only.

Table I.2.1 – Access security in trusted inter-cloud

Title	Access security in trusted inter-cloud
Description	– The CSC requests secure and malware free software as a service (SaaS). – The primary CSP in an inter-cloud intermediary pattern (acts as CSP(Intermediary)) is the contact point for CSC. – The CSP(Intermediary) integrates and validates services from multiple SaaS CSPs (secondary CSPs). – For the CSP(Intermediary), in order to guarantee secure and malware free SaaS software for CSC, it is necessary to validate SaaS from secondary CSP1(SaaS), CSP2(SaaS) and CSP3(SaaS). In case of negative SaaS validation the CSP offer of this SaaS is not presented to CSC. – In case of connectivity problem between CSP(Intermediary) and CSP1(SaaS), the service is automate established between CSP(Intermediary) and CSP3(SaaS).
Roles	CSC, CSP, CSP(SaaS)

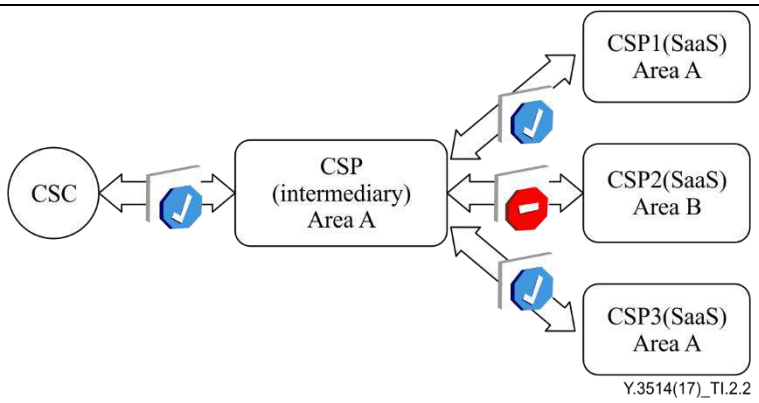
Title	Access security in trusted inter-cloud
Figure (optional)	
Pre-conditions (optional)	– The CSP1(SaaS) and CSP3(SaaS) deliver malware free software. – The CSP2(SaaS) delivers malware infected software.
Post-conditions (optional)	– The CSP(Intermediary) guarantees secure SaaS. – The CSP(Intermediary) establishes service between CSC and CSP1(SaaS). – The CSP(Intermediary) establishes service between CSC and CSP3(SaaS) in case of failed CSP1(SaaS).
Derived requirements	– access security between the CSC and CSP – integrate and validate services from multiple CSPs – resiliency service from multiple CSPs

I.2.2 Use case of geographical policy in trusted inter-cloud

This use case illustrates the governance aspect of trusted inter-cloud between the primary CSP and secondary CSPs. The intermediary pattern of inter-cloud used to illustrate the use case is an example only.

Table I.2.2 – Geographical policy in trusted inter-cloud

Title	Geographical policy in trusted inter-cloud
Description	– The CSC request SaaS service performed exactly within area A (geographical policy). – The primary CSP in an inter-cloud intermediary pattern (acts as CSP(Intermediary)) is the contact point for CSC. – The CSP(Intermediary) integrates and validates SaaS services from multiple CSPs (secondary CSPs). – For the CSP(Intermediary), in order to respect the request of CSC, it is necessary to validate governance polices from secondary CSP1(SaaS), CSP2(SaaS) and CSP3(SaaS). In case of negative validation, the secondary CSP offer is not presented to CSC. – In case of connectivity problem between CSP(Intermediary) and CSP1(SaaS), the SaaS service is automatically established between CSP(Intermediary) and CSP3(SaaS).
Roles	CSC,CSP, CSP(SaaS)

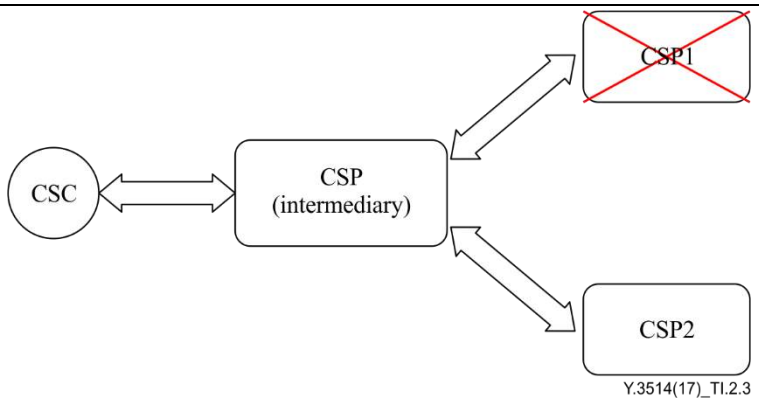
Title	Geographical policy in trusted inter-cloud
Figure (optional)	
Pre-conditions (optional)	– The primary CSP(Intermediary) and secondary CSPs are in trusted inter-cloud relationship. – The CSP1(SaaS) and CSP3(SaaS) effects geographical polices. – The CSP2 performs SaaS service out of the requested area.
Post-conditions (optional)	– The CSP(Intermediary) guarantees governance policies of SaaS. – The CSP (Intermediary) establishes service between CSC and CSP1(SaaS). – The CSP (Intermediary) establishes service between CSC and CSP3(SaaS) in case of failed CSP1(SaaS).
Derived requirements	– geographical policies – integrate and validate services from multiple CSPs – resiliency service from multiple CSPs

I.2.3 Use case of video gaming in trusted inter-cloud

This use case illustrates the resiliency aspect of trusted inter-cloud between the primary CSP and secondary CSPs. The intermediary pattern of inter-cloud used to illustrate the use case is an example only.

Table I.2.3 – Video gaming in trusted inter-cloud

Title	Video gaming service in trusted inter-cloud
Description	– The CSC requests video gaming service with quality of service (QoS) (Premium service under SLA). – The primary CSP in an inter-cloud intermediary pattern (acts as CSP(Intermediary)) is the contact point for CSC. – The CSP(Intermediary) integrates and validates video gaming services from multiple CSPs (secondary CSPs). – The CSP(Intermediary) monitors quality of service from secondary CSP1 and CSP2. In case service quality drops below premium service level, due to internal or external problems of CSP1 (e.g., overloaded resources, human error, distributed denial of service(DDoS)), the service is automatically established between CSP(Intermediary) and CSP2 without interruption.
Roles	CSC, CSP

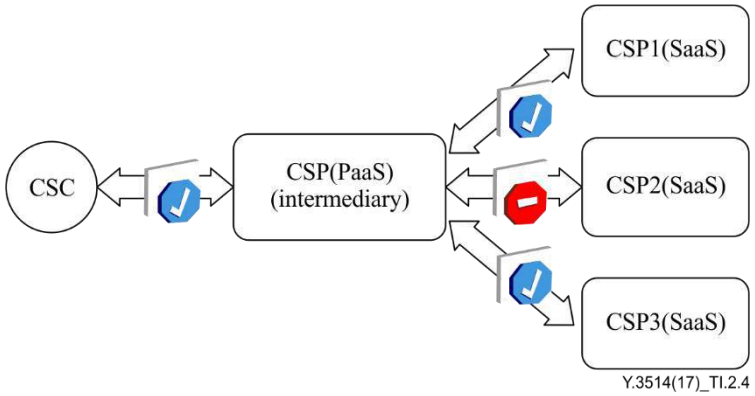
Title	Video gaming service in trusted inter-cloud
Figure (optional)	
Pre-conditions (optional)	– The primary CSP(Intermediary) and secondary CSPs are in trusted inter-cloud relationship. – The CSP1 and CSP2 offer video gaming service (Premium service). – The CSP (Intermediary) integrates and validates gaming services with QoS. – The CSP (Intermediary) establishes service between CSC and CSP1.
Post-conditions (optional)	– The CSP1 is under internal or external perturbation and quality of video gaming service drops below premium service level. – The service is automatically established between CSP(Intermediary) and CSP2 without service interruption.
Derived requirements	– real-time monitoring quality of trusted service – integrate and validate services from multiple CSPs – resiliency service from multiple CSPs

I.2.4 Use case of distributed image processing platform in trusted inter-cloud

This use case illustrates the security and confidentiality aspects of trusted inter-cloud between a primary CSP and secondary CSPs. The intermediary pattern of inter-cloud used to illustrate the use case is an example only.

Table I.2.4 – Distributed image processing platform in trusted inter-cloud

Title	Distributed image platform in trusted inter-cloud
Description	– The CSC requests the CSP for a platform to build image processing and storage systems. CSC is required to provide its own part of the software into the cloud. – The CSC request that the platform fits regulatory policy to reach safety, security and confidentiality constraints. The CSC requests QoS for data processing. – The CSC requests that the physical location (localization) for its data store as well as CSP can be chosen by CSC in an elastic manner. – The primary CSP(PaaS) in an inter-cloud intermediary pattern CSP(Intermediary) is the contact point for CSC. – The CSP(Intermediary) integrates and validates SaaS services from multiple CSPs (secondary CSPs). – The CSP2(SaaS) offers the same service as CSP1(SaaS) or CSP3(SaaS) but does not meet the required business regulatory policy. – For the CSP(Intermediary), in order to respect the request of a CSC, it is necessary to validate security and confidentiality policies from secondary CSP1(SaaS), CSP2(SaaS) and CSP3(SaaS). In case of negative validation, the secondary CSP offer is not presented to CSC.

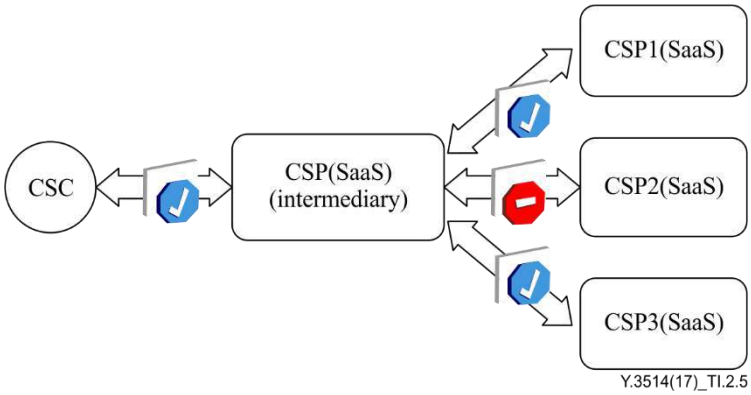
Title	Distributed image platform in trusted inter-cloud
	– In case of connectivity problem between CSP(Intermediary) and CSP1, the SaaS service is automatically established between CSP(Intermediary) and CSP3. In particular, an example of such service could be sharing information of patients' healthcare between hospitals. The hospitals can exchange all medical data of patients, while other agencies such as insurance or government have access limited to statistical information only without personally identifiable information (PII).
Roles	CSC, CSP(PaaS), CSP(SaaS)
Figure (optional)	
Pre-conditions (optional)	– The primary CSP(PaaS) and secondary CSPs are in trusted inter-cloud relationship. – The CSP1(SaaS) and CSP3(SaaS) effects security, safety and confidentiality polices. – The CSP2(SaaS) performs service out of business regulatory policy.
Post-conditions (optional)	– The CSP(Intermediary) guarantees security and confidentiality policy of SaaS. – The CSP(Intermediary) establishes service between CSC and CSP1(SaaS). – The CSP(Intermediary) establishes service between CSC and CSP3 (SaaS) in case CSP1(SaaS) fails.
Derived requirements	– security and confidentiality policies – unified (commonly adopted) security policies and metadata – interoperability and dependability – support appropriate level of robustness – security policy negotiation terminology – management of distributed data – resiliency service from multiple CSPs

I.2.5 Use case of distributed information exchange system in trusted inter-cloud

This use case illustrates the security and confidentiality aspect of trusted inter-cloud between a primary CSP and secondary CSPs. The intermediary pattern of inter-cloud used to illustrate the use case is an example only.

Table I.2.5 – Distributed information exchange system in trusted inter-cloud

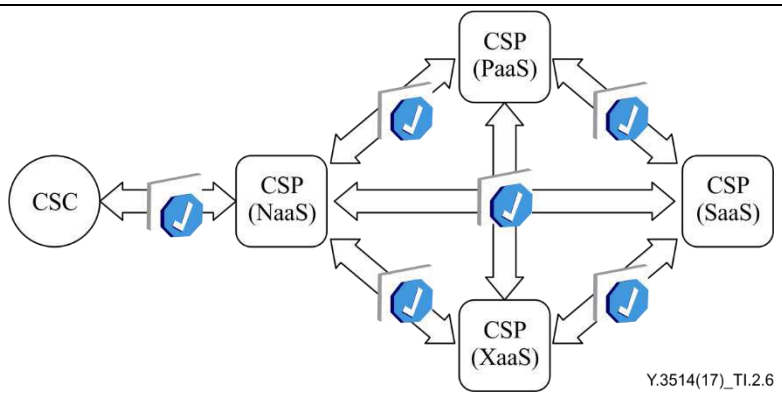
Title	Distributed information exchange system in trusted inter-cloud
Description	– The CSC from regulation business domain (e.g., healthcare, finance, defence), requests the CSP for a service to build an information exchange system. CSC requires that information will be distributed respecting business regulatory policies and data regulation policy. – The CSC requests that distributed information exchange system fits regulatory policy to reach safety, security and confidentiality constraints.

Title	Distributed information exchange system in trusted inter-cloud
	– The CSC requests that physical location (localization) for their data store as well as CSP can be chosen by CSC in an elastic manner. – The primary CSP(SaaS) in an inter-cloud intermediary pattern (acts as CSP(Intermediary)) is the contact point for CSC. – The CSP(Intermediary) integrates and validate SaaS services from multiple CSPs (secondary CSPs). – The CSP2(SaaS) offers the same service as CSP1(SaaS) or CSP3(SaaS) but does not meet the required business regulatory policy. – For the CSP(Intermediary), in order to respect the request of CSC, it is necessary to validate security and confidentiality policies from secondary CSP1(SaaS), CSP2(SaaS) and CSP3(SaaS). In case of negative validation, the secondary CSP offer is not presented to CSC. – In case of connectivity problem between CSP(Intermediary) and CSP1, the SaaS service is automatically established between CSP(Intermediary) and CSP3. In particular, an example of such service could be PaaS-based processing of satellite image data for farm crop analysis.
Roles	CSC,CSP(SaaS)
Figure (optional)	
Pre-conditions (optional)	– The primary CSP(SaaS) and secondary CSPs are in a trusted inter-cloud relationship. – The CSP1(SaaS) and CSP3(SaaS) effects security, safety and confidentiality policies. – The CSP2(SaaS) performs service out of business regulatory policy.
Post-conditions (optional)	– The CSP(Intermediary) guarantees the security and confidentiality policy of SaaS. – The CSP(Intermediary) establishes service between CSC and CSP1(SaaS). – The CSP(Intermediary) establishes service between CSC and CSP3(SaaS) in case of failed CSP1(SaaS).
Derived requirements	– security and confidentiality policies – master service agreements – on-demand data security services – deployment and monitoring of security policies around CSPs – respect data regulation policy (e.g., medical, financial, defence, etc.) NOTE – Regulation policy concern regulation applied to particular business. – respect business regulatory policies – resiliency service – respect laws and regulations, – respect local policies.

I.2.6 Use case of virtual home gateway in trusted inter-cloud

This use case illustrates management aspect of trusted inter-cloud between CSC and CSP or between CSPs. The federation pattern of inter-cloud used to illustrate the use case is an example only.

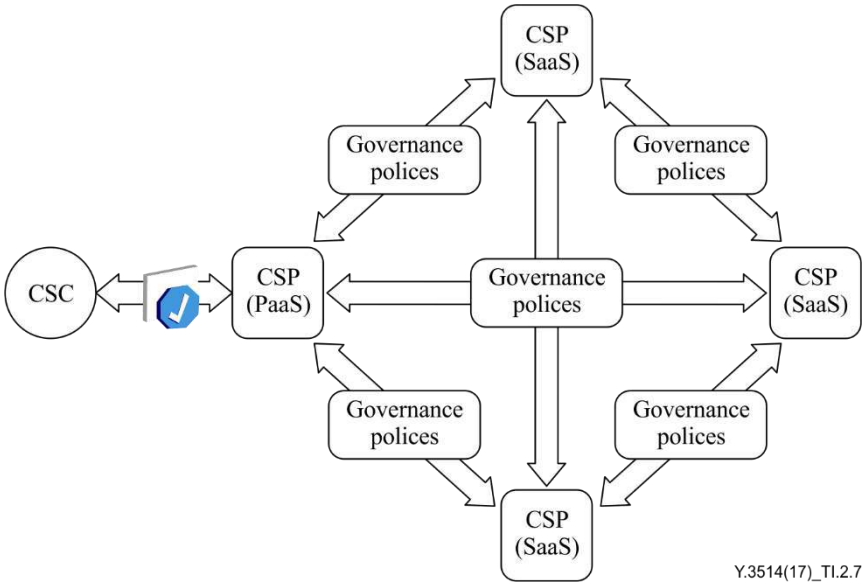
Table I.2.6 – Virtual home gateway in trusted inter-cloud

Title	Virtual home gateway in trusted inter-cloud
Description	– A large group of CSCs requests from CSP(NaaS) secured access to Internet with parental control service. A CSP(NaaS) serves such service over virtual home gateway (vHGW) facilities using network functions virtualization (NFV) and SDN technologies. – The CSP(NaaS) forms an inter-cloud federation pattern within a group of peer CSPs due to lack of own resources for request realization. According to the management of sensitive CSC's data, the CSP(NaaS) establish a trusted relationship between CSPs(PaaS) and CSPs(SaaS) involved in federation. – The CSP(NaaS) forms service chaining on parental control service from a set of network virtual functions (e.g., virtual firewall (vFW), virtual network address translation (vNAT), virtual load balancer (vLB)) hosted by CSP(PaaS) and CSP(SaaS). – The CSP(NaaS) monitors quality of service chaining and in case of quality drops below threshold or in case of the realization of particular key performance indicators (KPIs) (e.g., low power consumption, service balancing), the service is automatically reallocated within the federation, respecting policy and governance roles applied.
Roles	CSC, CSP(NaaS), CSP(PaaS), CSP(SaaS), CSP(XaaS)
Figure (optional)	
Pre-conditions (optional)	– The CSP(NaaS) and CSP(PaaS) and CSP(SaaS) are in a trusted inter-cloud relationship.
Post-conditions (optional)	– The CSP(NaaS) guarantees governance policy of SaaS. – The CSP(NaaS) establishes service chaining between CSP(PaaS) and CSP(SaaS). – The CSP(NaaS) reallocate service between CSPs among federation in case service quality drops below threshold or in case of the realization of particular KPIs (e.g., low power consumption, service balancing).
Derived requirements	– policies and governance roles – confidentiality of CSC's data – service statistics – annotation (tagging) of cloud workloads

I.2.7 Use case of distributed document exchange system in trusted inter-cloud

This use case illustrates governance aspect of trusted inter-cloud between CSC and CSP or between CSPs. The federation pattern of inter-cloud used to illustrate the use case is an example only.

Table I.2.7 – Distributed document exchange system in trusted inter-cloud

Title	Distributed document exchange system in trusted inter-cloud
Description	– The CSC requests from CSP(PaaS) cloud-based system which allows exchanging documents between their partners. – The CSC requests that these documents could be reviewed, updated and audited by the CSC or cloud service partner (CSN). – The CSC requests that distributed document exchange system fits regulatory policy to reach safety, security and confidentiality constraints. – The CSP(PaaS) forms federation pattern among CPSs(SaaS) and becomes contact point for CSC. – The CSP(PaaS) determine appropriate policies or principles which allows using of distributed document system in trustworthy manner.
Roles	CSC, CSP(PaaS), CSP(SaaS)
Figure (optional)	
Pre-conditions (optional)	– The CSP(PaaS) and CSPs(SaaS) are in trusted inter-cloud relationship.
Post-conditions (optional)	– The CSPs implements governance policy in theirs management system.
Derived requirements	– governance policies and governance roles – data separation for ensuring security and confidentiality – annotation (tagging) of cloud workloads to comply with regulatory needs – identity and access management to comply with CSC policy

Bibliography

[b-ISO/IEC 19086-1] ISO/IEC 19086-1:2016, *Information technology – Cloud computing – Service level agreement (SLA) framework – Part 1: Overview and concepts*.

[b-ISO/IEC 27000] ISO/IEC 27000:2016, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 38500:2015] ISO/IEC 38500:2015, *Information technology – Governance of IT for the organization*.

[b-TMF TR198] TM Forum TR198, *Multi-Cloud Service Management Pack – Simple Management API (SMI) Developer Primer-Service Delivery Framework Cloud Interface V2.2*. <https://www.tmforum.org/?s=TR198>

Cloud computing – Functional architecture of inter-cloud computing

Recommendation ITU-T Y.3516

(09/2017)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Summary

Recommendation ITU-T Y.3516 specifies inter-cloud computing functional architecture, including functions and functional components, based on the inter-cloud computing framework specified in Recommendation ITU-T Y.3511. The Recommendation builds upon the functional view of the cloud computing reference architecture (Recommendation ITU-T Y.3502) and makes extensions to functional components with inter-cloud functions.

Recommendation ITU-T Y.3516 also describes the mapping between functions and functional requirements of inter-cloud computing and examples of inter-cloud related reference points.

Keywords

Inter-cloud computing, functions, functional architecture, functional component.

Table of Contents

1 Scope

This Recommendation specifies inter-cloud computing functional architecture, including functions and functional components, based on the inter-cloud computing framework specified in [ITU-T Y.3511]. The Recommendation builds upon the functional view of the cloud computing reference architecture [ITU-T Y.3502] and makes extensions to functional components with inter-cloud functions.

The scope of this Recommendation consists of:

– overview of inter-cloud computing functional architecture;

– functions of inter-cloud computing;

– functional components of inter-cloud computing architecture.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing*.

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014) | ISO/IEC 17789: 2014, *Information technology – Cloud computing – Reference architecture*.

[ITU-T Y.3511] Recommendation ITU-T Y.3511 (2014), *Framework of inter-cloud computing*.

[ITU-T Y.3514] Recommendation ITU-T Y.3514 (2017), *Cloud computing – Trusted inter-cloud computing framework and requirements*.

[ITU-T Y.3522] Recommendation ITU-T Y.3522 (2016), *End-to-end cloud service lifecycle management requirements.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 activity [ITU-T Y.3502]: A specified pursuit or set of tasks.

3.1.2 cloud service [b-ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.3 cloud service customer [b-ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

NOTE – A business relationship does not necessarily imply financial agreements.

3.1.4 cloud service provider [b-ITU-T Y.3500]: Party which makes cloud services available.

3.1.5 functional component [ITU-T Y.3502]: A functional building block needed to engage in an activity, backed by an implementation.

3.1.6 inter-cloud computing [ITU-T Y.3511]: The paradigm for enabling the interworking between two or more cloud service providers.

NOTE – Inter-cloud computing is also referred as inter-cloud.

3.1.7 **peer cloud service** [ITU-T Y.3502]: A cloud service of one cloud service provider which is used as part of a cloud service of one or more other cloud service providers.

3.1.8 **peer cloud service provider** [ITU-T Y.3502]: A cloud service provider who provides one or more cloud services for use by one or more other cloud service providers as part of their cloud services.

3.1.9 **primary cloud service provider** [ITU-T Y.3511]: In inter-cloud computing, a cloud service provider which is making use of cloud services of peer cloud service providers (i.e., secondary cloud service providers) as part of its own cloud services.

3.1.10 **role** [ITU-T Y.3502]: A set of activities that serves a common purpose.

3.1.11 **secondary cloud service provider** [ITU-T Y.3511]: In inter-cloud computing, a cloud service provider which provides cloud services to a primary cloud service provider.

NOTE – The primary cloud service provider can use the services of secondary cloud service providers as part of its services offered to cloud service customers.

3.1.12 **sub-role** [ITU-T Y.3502]: A subset of the activities of a given role.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API Application Programming Interface
BSS Business Support System
CSC Cloud Service Customer
CSP Cloud Service Provider
CSU Cloud Service User
KPI Key Performance Indicator
OSS Operations Support System
QoS Quality of Service
SLA Service Level Agreement

5 Conventions

None.

6 Overview

6.1 Inter-cloud functional architecture with different patterns

Inter-cloud computing describes the interworking of cloud service providers (CSPs) in order to deliver cloud services to cloud service customers (CSCs) and cloud service users (CSUs) [ITU-T Y.3511]. One important target of inter-cloud computing for CSPs is to take benefit of the inter-cloud relationships established between peer CSPs (through inter-cloud patterns) in order to satisfy cloud service requirements of CSCs. The CSP who provides services for CSCs plays the role of primary CSP. The primary CSP is responsible for the cloud service level agreement (SLA) and interacts with peer CSP(s) within an inter-cloud relationship.

An inter-cloud relationship is bidirectional. As illustrated on Figure 6-1, CSP A plays a role of primary CSP when using the services of CSP B for providing services to its own customers, CSC A1 and CSC A2 (highlighted by black coloured arrows). CSP A plays the role of secondary CSP when providing services to CSP B, who plays the role of primary CSP and provides services to its own customers, CSC B1 and CSC B2 (highlighted by grey coloured arrows).

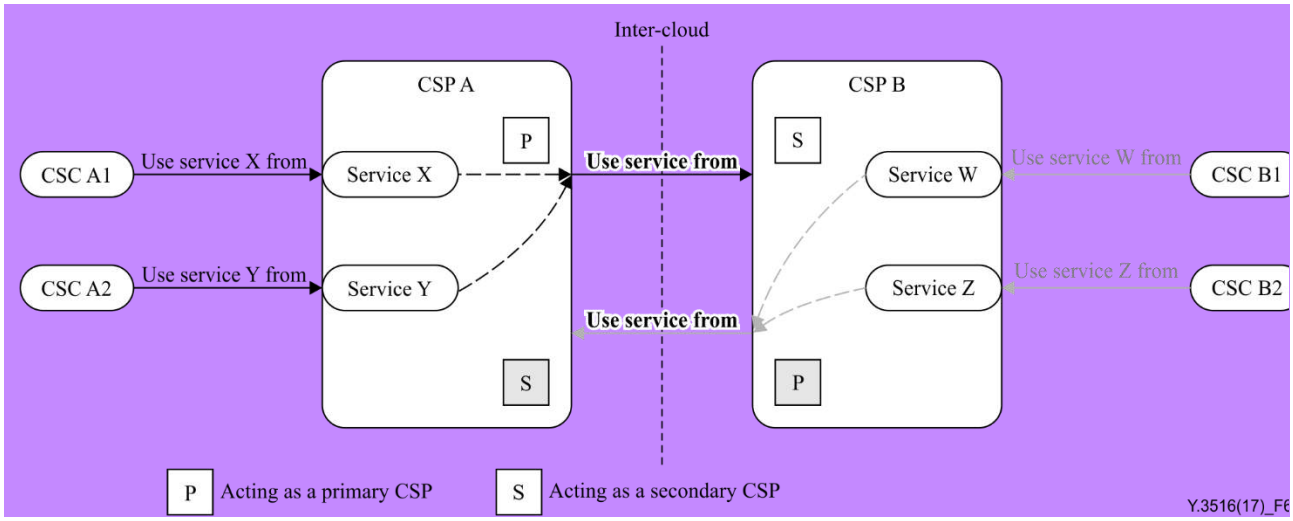


Figure 6-1 – Illustration of bidirectional relationship in inter-cloud computing

The inter-cloud computing concept is based on the relationship (pattern) among multiple CSPs as follows: peering, federation, and inter-cloud intermediary [ITU-T Y.3511]. These patterns are different in terms of business models and relationships between CSPs. However, these patterns are convergent from the viewpoint of inter-cloud computing functions and architecture.

The inter-cloud peering pattern contains only two CSPs and is the fundamental pattern, which may exist on its own or can be used in the other two patterns. The inter-cloud federation pattern involves a group of peer CSPs who mutually combine their service capabilities in order to provide the set of cloud services required by CSCs. The involved peer CSPs forming the inter-cloud federation establish and share common agreement which may range from service related policies, service level agreements (SLAs). The inter-cloud intermediary pattern refers to one and provides intermediation, aggregation and arbitrage of services provided by these peer CSPs.

The roles of the three patterns are also the same, the CSC, the primary CSP, and the secondary CSP. Among the multiple peer CSPs, the one that directly provides cloud services to its CSCs is called the primary CSP, while the one which indirectly provides its cloud service is called the secondary CSP. The secondary CSP treats the primary CSP as a CSC. Cloud services provided by the secondary CSP to the primary CSP are used by the primary CSP to offer services to its own customers (cf. the "perform peering, federation, intermediation, aggregation, arbitrage" activity defined in clause 8.3.2.16 of [ITU-T Y.3502]). For resource handling, the primary CSP negotiates to use the resources of secondary CSPs as an inter-cloud service.

NOTE – This Recommendation uses the term *inter-cloud service* instead of *abstracted resources* employed in [ITU-T Y.3511].

From the architecture point of view, the functions and functional components, as well as reference points for inter-cloud are the same, no matter which inter-cloud patterns are used.

6.2 Relationship with cloud computing reference architecture

The high-level interaction between CSPs for an inter-cloud relationship is described in the cloud computing reference architecture [ITU-T Y.3502]. Two functional components are defined to support inter-cloud computing [ITU-T Y.3502]: peer service integration (shown in Figure 6-2) and peer service management (shown in Figure 6-3 and Figure 6-4). As shown in Figure 6-2, a peer service integration functional component is used by a primary CSP to integrate services from peer CSP(s) (available through service access functional component in access layer) with its own services.

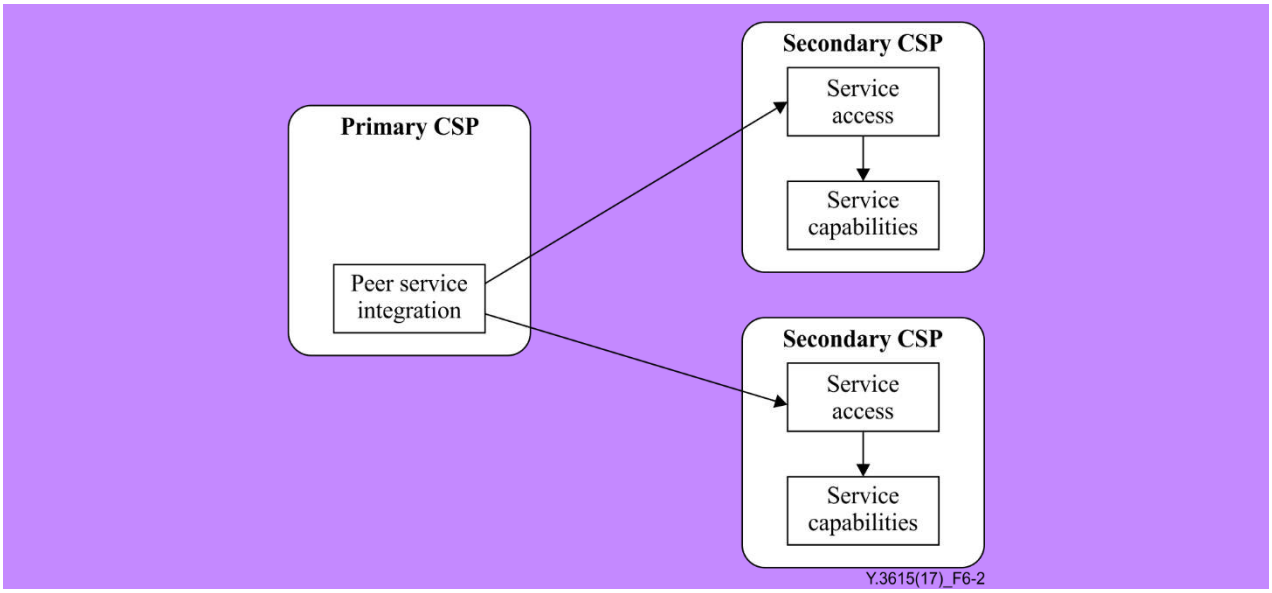


Figure 6-2 – Primary CSP using cloud services provided by secondary CSPs

Figure 6-3 and Figure 6-4 indicate primary CSP use peer service management functional component to make access to the secondary CSPs' operational support systems and business support systems (BSSs) through business access functional component and business capabilities, administration access functional component and business capabilities respectively.

This Recommendation describes additional extensions to [ITU-T Y.3502] for the support of inter-cloud, in particular extensions to functions and the definition of reference points necessary to support interactions between relevant functional components.

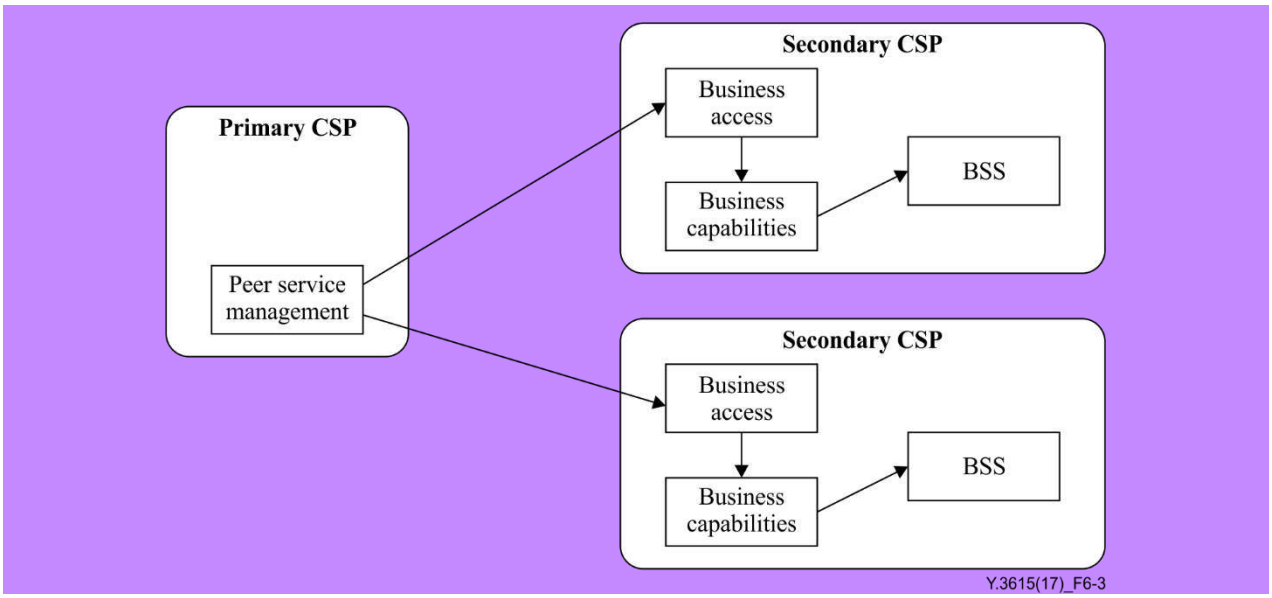


Figure 6-3 – Primary CSP using business capabilities provided by secondary CSPs

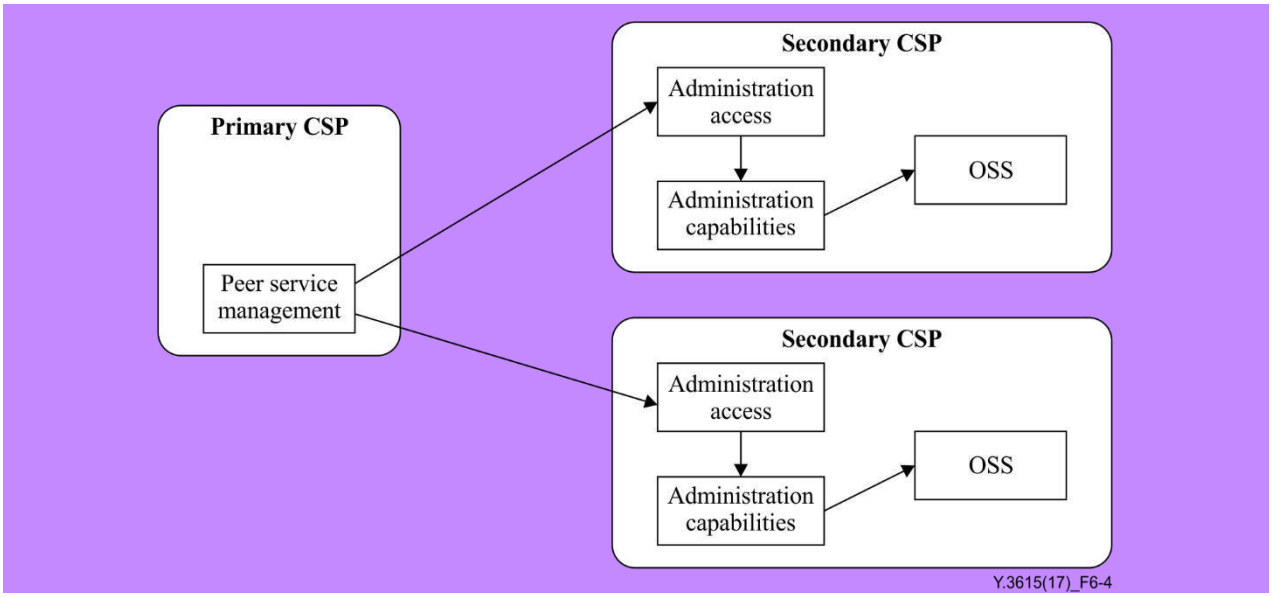


Figure 6-4 – Primary CSP using administration capabilities provided by secondary CSPs

The inter-cloud functional components in the functional architecture represent sets of functions that are required to perform inter-cloud computing activities for various roles and sub-roles. There are two types of relationship between peer CSPs:

- the use of cloud services of secondary CSPs by a primary CSP;
- the use of business and administration capabilities of secondary CSPs by a primary CSP.

The secondary CSP provides inter-cloud services to the primary CSP. From the secondary CSP point of view, the primary CSP plays the role of CSC. As a result, there is no difference in terms of service access and service capabilities for inter-cloud, compared to the case of cloud services provided by a CSP to a CSC.

The primary CSP utilizes a peer service integration functional component to connect to a secondary CSP. The primary CSP manages inter-cloud services by using a peer service management functional component along with the integration, BSSs, operations support system (OSS) and security systems functional components of a secondary CSP.

No functional extensions are needed for the user layer, access layer, service layer, resource layer and development function. As highlighted by the dark grey colour in Figure 6-5, this Recommendation identifies inter-cloud specific extensions to functional components [ITU-T Y.3502] that are part of integration, security systems, OSS and BSSs. Functional components in other parts of the architecture, i.e. user layer, access layer service layer, resource layer and multi-layer development functions, are reused without modification in the inter-cloud functional architecture.

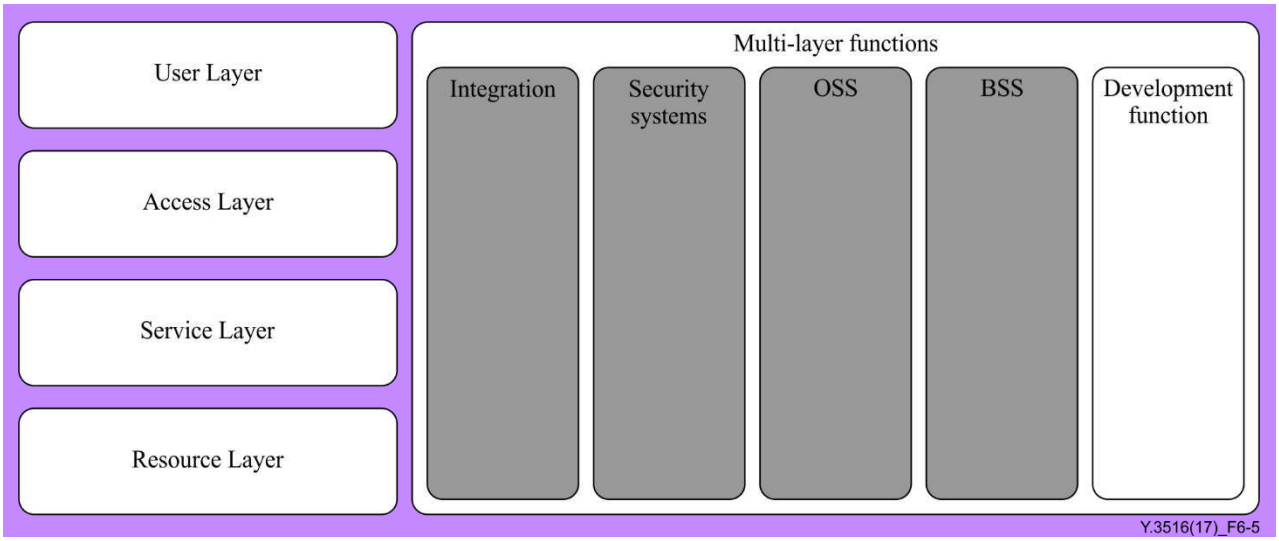


Figure 6-5 – Functional components extended with inter-cloud computing functions

7 Functions of inter-cloud computing

As shown in Figure 6-5, the inter-cloud functions only cover extensions to BSSs, OSS, integration and security systems. The inter-cloud functions are as follows:

– BSS functions, including service subscription management and billing.

– OSS functions, including service catalogue, service provisioning, monitoring and reporting, service policy management, service level management, incident and problem management and peer service management.

– Integration functions, including peer CSP management, inter-cloud service negotiation, inter-cloud service discovery, inter-cloud service selection, inter-cloud service reservation, inter-cloud service release and inter-cloud capabilities adaptation.

– Security systems functions, including authentication and identity management, authorization and security policy management and encryption management.

7.1 Business support systems

7.1.1 Service subscription management

The service subscription management function handles the subscription of the CSP to services provided by peer CSPs as well as subscription of peer CSPs to its own services.

This function includes the following.

– Service subscription management. This allows for managing, e.g., creating, modifying, updating, deleting and querying inter-cloud service subscription between peer CSPs.

7.1.2 Billing

The billing function generates service charging and invoice for inter-cloud services.

This function includes the following.

– Service charging. This allows for rating the usage of an inter-cloud service based on metering data of the particular inter-cloud service.

– Service invoice generation. This allows generating inter-cloud service invoice and delivering the invoices to peer CSPs.

7.2 Operational support systems

7.2.1 Service catalogue

The service catalogue function includes service catalogue synchronization and life-cycle management with peer CSPs.

This function includes the following.

– Service catalogue synchronization. This allows for periodically or on-demand exchange of service catalogue information for inter-cloud services.

– Service catalogue lifecycle management. This allows managing, e.g., creating, modifying, deleting and querying content of the service catalogue of the peer CSP for inter-cloud services. Service catalogue life-cycle management includes publishing catalogue content information allowing peer CSPs to consult and select inter-cloud services.

7.2.2 Service provisioning

The provisioning function allows for the provisioning of inter-cloud services provided by peer CSPs.

This function includes the following.

– Service deployment. This allows creating inter-cloud service instances based on the inter-cloud service template defined in the service catalogue, and delivery of inter-cloud service instances deployment requests to related peer CSPs.

– Service configuration and lifecycle management. This allows accessing and configuring deployed inter-cloud service instances as well as managing the lifecycle of deployed inter-cloud service instances.

NOTE – Service lifecycle management includes inter-cloud service creation, scaling, update and termination. For more details about end-to-end cloud service lifecycle management, refer to [ITU-T Y.3522].

7.2.3 Monitoring and reporting

The monitoring and reporting functions monitor inter-cloud services and provide monitoring reports to peer CSPs.

This function includes the following.

– Service monitoring. This allows for providing inter-cloud service metrics to peer CSPs periodically or on a request basis.

NOTE – Inter-cloud service metrics are tracked for the purpose of meeting the inter-cloud service availability contributing to SLAs.

– Monitoring information exchanging and reporting. This allows for exchanging, recording and reporting of inter-cloud services monitoring information for peer CSPs.

7.2.4 Service policy management

The service policy management function includes lifecycle management and provisioning policy negotiation.

This function includes the following.

– Service policy lifecycle management. This allows for defining, modifying, storing and retrieving of inter-cloud service policies.

NOTE – Inter-cloud service policy refers to an inter-cloud SLA, disaster recovery mechanism, auto-scale, inter-cloud service switchover and switchback.

– Service provisioning policy negotiation. This allows for inter-cloud service provisioning policy comparison, transformation and confirmation between peer CSPs.

7.2.5 Service automation

The service automation function delivers inter-cloud services automatically, including the management and execution of service templates and the orchestration of services.

This function includes the following.

– Service provisioning automation. This allows automation of workflows to realize inter-cloud service deployment between peer CSPs, without manual operations.

NOTE 1 – Typical use cases of service provision automation include: automatic recovery, scale-in and scale-out, switchover and switchback of cloud services with peer CSPs.

– Service configuration automation. This allows automation of workflows to realize automated inter-cloud service configuration, without manual operations.

NOTE 2 – Service provisioning and configuration automation allows for policy-based automated workflows for inter-cloud services.

7.2.6 Service level management

The service level management function manages the service levels of a particular inter-cloud service to meet the requirements of the SLA.

This function includes the following.

– SLA negotiation. This allows for negotiating inter-cloud service level information, e.g., capacity, performance, between peer CSPs.

– Service level tracking. This allows for measuring and recording of key performance indicators (KPIs) of inter-cloud service between peer CSPs according to the monitoring results.

– Service performance management. This allows for adjusting of particular inter-cloud service performance based on service performance tracking results to meet the requirements of the SLA.

– Service capacity management. This allows for identifying of current or potential capacity bottlenecks by comparing the allocated inter-cloud service capacity with KPIs, and planning inter-cloud service capacity to meet the requirements of the SLA.

7.2.7 Incident and problem management

The incident and problem management function detects and reports inter-cloud incidents and problems.

This function includes the following.

– Incident and problem detection. This allows for capturing of inter-cloud incidents or problems between peer CSPs.

– Incident and problem reporting. This allows for providing and exchanging of inter-cloud incident or problem reports to peer CSPs.

7.2.8 Peer service management

The peer service management function allows for connecting of OSS and BSSs of a peer CSP, by adapting an inter-cloud management application programming interface (API).

This function includes:

– Inter-cloud connection management. This allows for managing of connectivity with peer CSPs involved in an inter-cloud relationship.

– Access of the BSSs of a peer CSP. This allows for accessing to the inter-cloud BSSs of peer CSP with appropriate identity and credentials to provide business capabilities. The identity and credentials are provided by inter-cloud security (see clause 7.4). The functions of inter-cloud BSSs can be found in clause 7.1.

– Access to the OSS of a peer CSP. This allows for accessing to the inter-cloud OSS of a peer CSP with appropriate identity and credentials to provide administration capabilities. The identity and credentials are provided by inter-cloud security (see clause 7.4). The functions of an inter-cloud OSS can be found in clause 7.2.

– Inter-cloud management API adaptation. This allows for adapting of an inter-cloud BSS- and OSS-related API from a peer CSP.

7.3 Peer service integration

7.3.1 Peer CSP management

The peer CSP management function supports discovery of peer CSPs, negotiation with peer CSPs, primary CSP role delegation, primary CSP switchover and switchback.

This function includes the following.

– Peer CSP discovery. This allows for exchanging of available inter-cloud service and resource information between peer CSPs with peering, federation and intermediary patterns.

– Negotiation with peer CSPs. This allows for performing of API negotiation, SLA negotiation and policy negotiation between peer CSPs.

NOTE 1 – API negotiation mainly deals with the API format, protocol, and content.

NOTE 2 – SLA negotiation deals with the different inter-cloud service quality between peer CSPs.

NOTE 3 – Policy negotiation with peer CSPs deals with policies that apply to inter-cloud services. Policies can include business, technical, security, privacy and certification policies that apply to inter-cloud services and their usage by peer CSPs.

– Primary CSP role delegation. This allows for identifying of peer CSPs that are capable of inheriting the primary CSP role with peering, federation and intermediary inter-cloud patterns. This allows negotiating with the peer CSPs identified as to whether they can accept the inheritance and also allows for delegating of one of the peer CSPs identified to take the role of primary CSP.

– Primary CSP switchover and switchback. This allows for switchover of CSC access to a peer CSP (acting as primary CSP) without service interruption for that CSC. This allows the CSC to use services in a similar manner to the way they did before the access was switched over. This also allows for switching back on CSC access to the primary CSP when this CSP has recovered from the reasons that led to the switchover (e.g., a fault or load distribution).

NOTE 4 – Switchover conditions include load distribution between CSPs, in which the primary CSP role is maintained as it is; and fault cases, in which the primary CSP role is delegated to the peer CSP (see clause 9.6 of [ITU-T Y.3511]).

NOTE 5 – The mechanism of switchover and switchback of a primary CSP can be a policy-based process.

7.3.2 Inter-cloud service negotiation

The inter-cloud service negotiation function negotiates inter-cloud service information, quality of service (QoS), and performance estimation and selection policy between peer CSPs.

This function includes the following.

– Inter-cloud service information negotiation. This allows for negotiation of inter-cloud service information between peer CSPs. Inter-cloud inter-working can only start when inter-cloud service information negotiation is finalized and the inter-cloud service is available.

NOTE – The inter-cloud service information includes: inter-cloud service provider, inter-cloud service identifier, inter-cloud service type, inter-cloud service status (available, reserved, allocated, released), inter-cloud service priority (high, medium, normal, low).

– Inter-cloud service performance negotiation. This allows a primary CSP to negotiate with peer CSPs in order to guarantee inter-cloud service performance that satisfies inter-cloud service SLAs.

– Inter-cloud service performance estimation and selection policy negotiation. This allows for negotiating of inter-cloud service performance estimation and selection policies associated with peer CSPs.

7.3.3 Inter-cloud service discovery

The inter-cloud service discovery function discovers available particular inter-cloud services between peer CSPs.

This function includes the following.

– Inter-cloud service discovery. This allows for discovering of available particular inter-cloud services provided by peer CSPs that meet the requirements of an inter-cloud service SLA.

7.3.4 Inter-cloud service selection

The inter-cloud service selection function allows a primary CSP to match and identify a specified inter-cloud service.

This function includes the following.

– Inter-cloud service matching. This allows a primary CSP to find out about available inter-cloud services by matching inter-cloud service SLAs and inter-cloud service monitoring information.

– Inter-cloud service identification. This allows for selecting of appropriate inter-cloud services based on the matching result. The identification of the inter-cloud service selected, as the acknowledgement of the inter-cloud selection, is used to reserve an inter-cloud service by a primary CSP.

7.3.5 Inter-cloud service reservation

The inter-cloud service reservation function allows a primary CSP to create, update and release reserved inter-cloud service and its attached resource.

This function includes the following.

– Inter-cloud reserved service creation. This allows a primary CSP to reserve an inter-cloud service and its attached resources from other peer CSPs. The acknowledgement is sent between peer CSPs as confirmation of the creation.

– Inter-cloud reserved service updated. This allows a primary CSP to update the inter-cloud reserved service and its attached resources from other peer CSPs. The acknowledgement is sent between peer CSPs as confirmation of the update.

– Inter-cloud reserved service released. This allows a primary CSP to release an inter-cloud reserved service and its attached resources from other peer CSPs. The acknowledgement is sent between peer CSPs as confirmation of the release.

7.3.6 Inter-cloud service release

The inter-cloud service release function allows for releasing of a reserved and allocated inter-cloud service and return of its attached resources to peer CSPs.

This function includes the following.

– Inter-cloud reserved service release. This allows for releasing of an issued inter-cloud service reservation and return of its attached resources to peer CSPs.

– Inter-cloud allocated service release. This allows for de-allocating and terminating of the allocated inter-cloud service and return of its attached resources to peer CSPs.

7.3.7 Inter-cloud capabilities adaptation

The inter-cloud capabilities adaptation function allows for adapting inter-cloud service API from peer CSPs.

This function includes the following.

– Inter-cloud service API adaptation. This allows for adapting of an inter-cloud service API from peer CSPs. The format of an inter-cloud service API provided by peer CSPs is transformed into a primary CSP's own API by utilizing inter-cloud capabilities adaptation.

7.4 Security systems

7.4.1 Authentication and identity management

The authentication and identity management function provides authentication of and identities for peer CSPs.

This function includes the following.

– Federated identity management. This allows for using of federated identity management to permit peer CSPs to employ the same identity and credentials to access inter-cloud services.

7.4.2 Authorization and security policy management

The authorization and security policy management function controls and applies authorization for peer CSPs to access a specific inter-cloud service.

This function includes the following.

– Authorization management. This allows for implementing of permissions and authorization for particular peer CSPs and related inter-cloud services.

– Federated authorization and security policy management. This allows for providing of federated authorization and security policy management between peer CSPs.

– Trust management. This allows for encapsulating and verifying of the policies for trusted inter-cloud.

NOTE – For more information about trusted inter-cloud please refer to [ITU-T Y.3514].

7.4.3 Encryption management

The encryption management function provides data encryption, API encryption, as well as network connectivity encryption.

This function includes the following.

– Data encryption. This allows for encrypting of data exchanged through inter-cloud services.

– API encryption. This allows for encrypting of inter-cloud service and management APIs for peer CSPs.

– Network connectivity encryption. This allows for utilizing of security keys to secure the network connectivity between CSPs.

8 Functional components of inter-cloud

Figure 8-1 illustrates the mapping of inter-cloud functions and functional components.

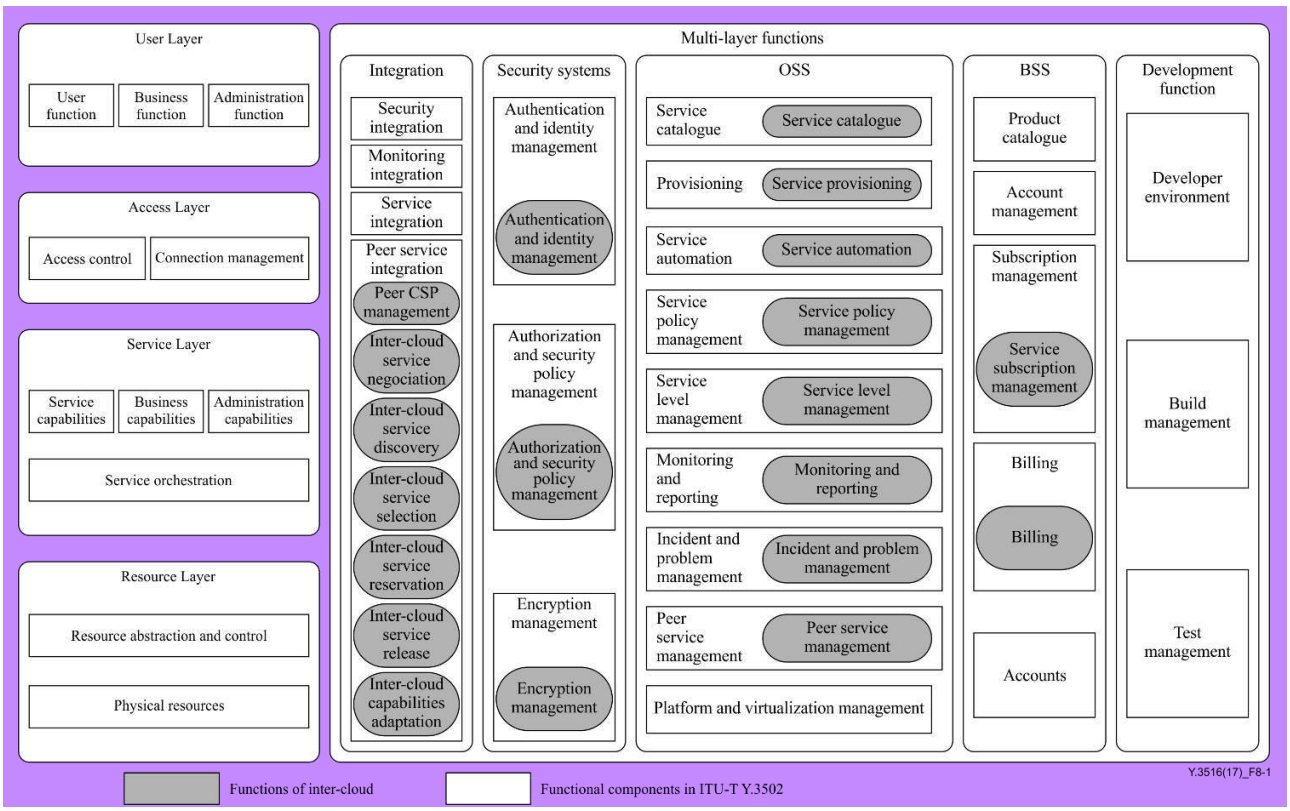


Figure 8-1 – Mapping of inter-cloud functions and functional components

The inter-cloud functions identified in clause 7 are mapped to functional components in [ITU-T Y.3502]. No new functional components are defined. However, functions of some functional components are extended for inter-cloud as follows.

– Business support systems
  - Service subscription management functional component is extended with service subscription management function for inter-cloud as described in clause 7.1.1.
  - Billing functional component is extended with billing function for inter-cloud as described in clause 7.1.2.

– Operational support systems
  - Service catalogue functional component is extended with service catalogue function for inter-cloud as described in clause 7.2.1.
  - Provisioning functional component is extended with service provisioning function for inter-cloud as described in clause 7.2.2.
  - Monitoring and reporting functional component is extended with monitoring and reporting function for inter-cloud as described in clause 7.2.3.
  - Service policy management functional component is extended with service policy management function for inter-cloud as described in clause 7.2.4.
  - Service automation functional component is extended with service automation function for inter-cloud as described in clause 7.2.5.
  - Service level management functional component is extended with service level management function for inter-cloud as described in clause 7.2.6.
  - Incident and problem management functional component is extended with incident and problem management function for inter-cloud as described in clause 7.2.7.
  - Peer service management functional components is extended with peer service management function for inter-cloud as described in clause 7.2.8.

– Peer service integration
  - Peer service integration functional component is extended with peer CSP management function as described in clause 7.3.1.
  - Peer service integration functional component is extended with inter-cloud service negotiation as described in clause 7.3.2.
  - Peer service integration functional component is extended with inter-cloud service discovery function as described in clause 7.3.3.
  - Peer service integration functional component is extended with inter-cloud service selection function as described in clause 7.3.4.
  - Peer service integration functional component is extended with inter-cloud service reservation function as described in clause 7.3.5.
  - Peer service integration functional component is extended with inter-cloud service release function as described in clause 7.3.6.
  - Peer service integration functional component is extended with inter-cloud capabilities adaptation function as described in clause 7.3.7.

– Security systems
  - Authentication and identity management functional component is extended with authentication and identity management function for inter-cloud as described in clause7.4.1.
  - Authorization and security policy management functional component is extended with authorization and security policy management function for inter-cloud as described in clause 7.4.2.

- Encryption management functional component is extended with encryption management function for inter-cloud as described in clause 7.4.3.

9 Security considerations

Security aspects for consideration within the cloud computing environment are addressed by security challenges for the CSPs, as described in [ITU-T X.1601]. In particular, [ITU-T X.1601] analyses security threats and challenges, and describes security capabilities that could mitigate these threats and meet the security challenges. In addition, clause 7 of this Recommendation identifies the inter-cloud security related functions.

Appendix I

Mapping of inter-cloud computing functional requirements and functions

(This appendix does not form an integral part of this Recommendation.)

This appendix aims to describe the mapping of inter-cloud computing functional requirements specified in [ITU-T Y.3511] and inter-cloud functions in clause 7 of this Recommendation.

Table I.1 – Mapping of inter-cloud computing functional requirements and inter-cloud functions

Functional requirements specified in [ITU-T Y.3511]		Inter-cloud functions in this Recommendation
9.1 SLA and policy negotiation	The SLA and policy negotiation capability is required to be aware of the SLA information related to the QoS and performance aspects of the CSPs involved in the inter-cloud using standard formats.	– 7.3.1 Peer CSP management – 7.2.4 Service policy management – 7.2.6 Service level management – 7.2.8 Peer service management – 7.3.7 Inter-cloud capabilities adaptation
9.2 resource monitoring	Allow describing and expressing of the resource information (e.g., resource type, configuration and status) in a standard manner in order to be able to monitor these resources across multiple CSPs.	– 7.2.8 Peer service management – 7.3.2 Inter-cloud service negotiation – 7.3.7 Inter-cloud capabilities adaptation
9.2 resource monitoring	Allow updating of the resource information across multiple CSPs in synchronization with the events (e.g., reserve or release of resources) involving the CSPs.	– 7.2.8 Peer service management – 7.2.3 Monitoring and reporting – 7.3.7 Inter-cloud capabilities adaptation
9.2 resource monitoring	Allow periodically, or on a request basis, collecting of information about the usage and performance status of the resources of multiple CSPs.	– 7.2.3 Monitoring and reporting – 7.2.8 Peer service management – 7.3.2 Inter-cloud service negotiation – 7.3.7 Inter-cloud capabilities adaptation
9.2 resource monitoring	Allow periodically, or on a request basis, collecting of information about the resource availability (e.g., dead or alive status of machines) of multiple CSPs.	– 7.2.3 Monitoring and reporting – 7.2.8 Peer service management – 7.3.7 Inter-cloud capabilities adaptation
9.2 resource monitoring	Allow exchange of monitoring information in commonly defined ways across multiple CSPs.	– 7.2.3 Monitoring and reporting – 7.2.8 Peer service management – 7.3.7 Inter-cloud capabilities adaptation
9.3 resource performance estimation and selection	The resource performance estimation and selection capability deals with the selection of resources from the candidate resources that have already been reserved in peer CSPs. This capability estimates the achievable performance of available reserved resources and assists the CSP in the selection of resources to be effectively used.	– 7.2.8 Peer service management – 7.3.4 Inter-cloud service selection – 7.3.7 Inter-cloud capabilities adaptation
9.4 resource discovery and reservation	Allow finding of available resources in the peer CSPs based on different priorities. Allow reservation of available resources in the peer CSPs on the basis of different priorities	– 7.3.2 Inter-cloud service negotiation – 7.3.7 Inter-cloud capabilities adaptation
9.4 resource discovery and reservation	Enable discovery of resources available in the peer CSPs.	– 7.3.3 Inter-cloud service discovery – 7.3.7 Inter-cloud capabilities adaptation

Table I.1 – Mapping of inter-cloud computing functional requirements and inter-cloud functions

Functional requirements specified in [ITU-T Y.3511]		Inter-cloud functions in this Recommendation
9.4 resource discovery and reservation	Allow the reservation of discovered resources in the peer CSPs.	– 7.3.5 Inter-cloud service reservation – 7.3.7 Inter-cloud capabilities adaptation
9.4 resource discovery and reservation	Allow provisional reservation of discovered resources, i.e., to keep the resources to be used (as candidates), for later acknowledgement (for some of them) or release (for others).	– 7.3.5 Inter-cloud service reservation – 7.3.7 Inter-cloud capabilities adaptation
9.4 resource discovery and reservation	Allow finding of available resources in the peer CSPs based on different priorities.	– 7.3.3 Inter-cloud service discovery – 7.3.4 Inter-cloud service selection – 7.3.7 Inter-cloud capabilities adaptation
9.4 resource discovery and reservation	Allow reservation of available resources in the peer CSPs on the basis of different priorities	– 7.3.5 Inter-cloud service reservation – 7.3.4 Inter-cloud service selection – 7.3.7 Inter-cloud capabilities adaptation
9.5 resource set-up and activation	The resource set-up and activation capability deals with the set up and activation of reserved resources in the peer CSPs. This includes connecting to the peer CSPs via networks, remotely activating (i.e., invoking) software and transferring or copying data to enable the use of resources in the peer CSPs.	– 7.2.2 Service provisioning – 7.2.8 Peer service management – 7.3.7 Inter-cloud capabilities adaptation – 7.4.1 Authentication and identity management – 7.4.2 Authorization and security policy management – 7.4.3 Encryption management
9.5 resource set-up and activation	Allow the establishment of reserved resources in a peer CSP.	– 7.2.2 Service provisioning – 7.3.7 Inter-cloud capabilities adaptation
9.5 resource set-up and activation	Allow accessing to the configuration and policy settings of reserved resources in the peer CSPs.	– 7.2.2 Service provisioning – 7.2.8 Peer service management – 7.3.7 Inter-cloud capabilities adaptation
9.6 cloud services switchover and switchback	Allow switching over of CSC end-user access to a peer CSP (acting as primary CSP) without manual operation from the CSC, in order to allow the CSC end user to use services in a similar manner to the way they did before the access was switched over. Allow switching back of CSC end-user access to the primary CSP when this CSP has recovered from the reasons that led to the switchover (e.g., a disaster or load distribution between peer CSPs is no longer needed).	– 7.3.1 Peer CSP management – 7.2.7 Incident and problem management – 7.2.5 Service automation – 7.3.7 Inter-cloud capabilities adaptation – 7.4.1 Authentication and identity management – 7.4.2 Authorization and security policy management – 7.4.3 Encryption management
9.7 resource release	Allow updating of the peer CSP resource configuration information.	– 7.2.3 Monitoring and reporting – 7.2.8 Peer service management – 7.3.7 Inter-cloud capabilities adaptation
9.7 resource release	Allow releasing by the CSP of resources reserved, activated or set up in the peer CSPs.	– 7.3.6 Inter-cloud service release – 7.3.7 Inter-cloud capabilities adaptation

Table I.1 – Mapping of inter-cloud computing functional requirements and inter-cloud functions

Functional requirements specified in [ITU-T Y.3511]		Inter-cloud functions in this Recommendation
9.8 CSC information exchange	Be able to manage CSC profiles and associated information. Be able to exchange CSC profiles and associated information among multiple CSPs according to a pre-determined protocol and format, with the condition that the CSC is informed of and agrees to the exchange.	– 7.2.8 Peer service management – 7.3.7 Inter-cloud capabilities adaptation – 7.4.1 Authentication and identity management – 7.4.2 Authorization and security policy management – 7.4.3 Encryption management
9.9 primary CSP role delegation	Allow a CSP to discover peer CSPs that are capable of inheriting the primary CSP role, and enable the CSP to negotiate with these peer CSPs as to whether they can accept the inheritance.	– 7.3.1 Peer CSP management – 7.3.7 Inter-cloud capabilities adaptation
9.9 primary CSP role delegation	Allow a CSP to transfer its management information associated with the primary CSP role in a reliable manner (e.g., periodically) to the peer CSPs that have accepted the permission transfer with that CSP.	– 7.2.8 Peer service management – 7.3.7 Inter-cloud capabilities adaptation – 7.4.1 Authentication and identity management – 7.4.2 Authorization and security policy management – 7.4.3 Encryption management
9.9 primary CSP role delegation	Allow the controllability of the information associated with the primary CSP role to be transferred to the secondary CSPs with minimum interruptions. Allow a CSP to cancel the permission transfer arrangements.	– 7.1.1 Service subscription management – 7.1.2 Billing – 7.3.1 Peer CSP management – 7.2.5 Service automation – 7.3.7 Inter-cloud capabilities adaptation
9.10 inter-cloud service handling	Support service intermediation, i.e., conditioning or enhancing the cloud service of a peer CSP. Support service aggregation, i.e., providing the composition of a set of services provided by the CSPs. Support service arbitrage, i.e., selecting one service offering from a group offered by the peer CSPs.	– 7.2.8 Peer service management – 7.2.1 Service catalogue – 7.2.5 Service automation – 7.3.7 Inter-cloud capabilities adaptation

Appendix II

Reference points of inter-cloud computing

(This appendix does not form an integral part of this Recommendation.)

As described in this Recommendation, inter-cloud functional architecture reuse the functional components of [ITU-T Y.3502] and extends BSS, OSS, integration and security system functional components with inter-cloud functions. Given no detailed interactions and reference points have been defined in [ITU-T Y.3502] between functional components, this appendix provides examples of inter-cloud related reference points for informative purposes.

The reference points of inter-cloud computing architecture are shown in Figure II.1.

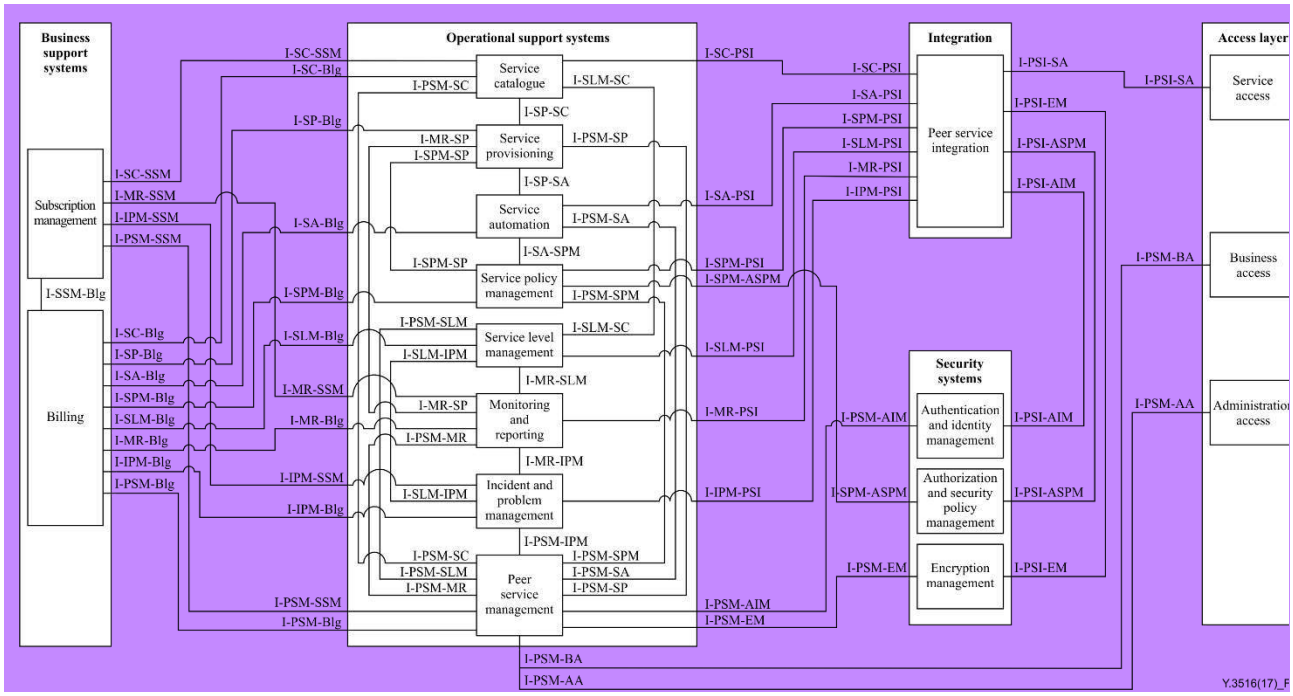


Figure II.1 – Reference points of inter-cloud computing architecture

II.1 Reference point: I-SSM-Blg

The subscription management functional component interacts with billing functional component through I-SSM-Blg to provide inter-cloud service subscription information for billing.

II.2 Reference point: I-SSM-IPM

The subscription management functional component interacts with incident and problem management functional component through I-SSM-IPM to synchronize inter-cloud incident- and problem-detecting and reporting information.

II.3 Reference point: I-SSM-MR

The subscription management functional component interacts with monitoring and reporting functional component through I-SSM-MR to get the monitoring information of inter-cloud services of different inter-cloud service subscriptions.

II.4 Reference point: I-SSM-SC

The subscription management functional component interacts with service catalogue functional component through I-SSM-SC to synchronize inter-cloud service catalogue information.

II.5 Reference point: I-SSM-PSM

The subscription management functional component interacts with peer service management functional component through I-SSM-PSM to access the BSSs of a peer CSP for subscription.

II.6 Reference point: I-Blg-IPM

The billing functional component interacts with incident and problem management functional component through I-Blg-IPM to get inter-cloud incident and problem information for billing.

II.7 Reference point: I-Blg-MR

The billing functional component interacts with monitoring and reporting functional component through I-Blg-MR to get inter-cloud service monitoring information for billing.

II.8 Reference point: I-Blg-SC

The billing functional component interacts with service catalogue functional component through I-Blg-SC to get inter-cloud service catalogue information for billing.

II.9 Reference point: I-Blg-SP

The billing functional component interacts with service provisioning functional component through I -Blg-SP to get inter-cloud service provisioning information for billing.

II.10 Reference point: I-Blg-SA

The billing functional component interacts with service automation functional component through I-Blg-SA to get inter-cloud service automation information for billing.

II.11 Reference point: I-Blg-SPM

The billing functional component interacts with service policy management functional component through I-Blg-SPM to get inter-cloud service policy information for billing.

II.12 Reference point: I-Blg-SLM

The billing functional component interacts with service level management functional component through I-Blg-SLM to get inter-cloud service level information for billing.

II.13 Reference point: I-Blg-PSM

The billing functional component interacts with service level management functional component through I-Blg-PSM to exchange with peer CSP's billing.

II.14 Reference point: I-SP-SC

The service catalogue functional component interacts with service provisioning functional component through I-SP-SC to provision inter-cloud service by using inter-cloud service templates.

II.15 Reference point: I-SLM-SC

The service catalogue functional component interacts with service level management functional component through I-SLM-SC to exchange service level information.

II.16 Reference point: I-PSM-SC

The service catalogue functional component interacts with peer service management functional component through I-PSM-SC to access the inter-cloud service catalogue of a peer CSP.

II.17 Reference point: I-SC-PSI

The service catalogue functional component interacts with peer service integration functional component through I-SC-PSI to provide inter-cloud service integration information.

II.18 Reference point: I-SPM-SP

The service provisioning functional component interacts with service policy management functional component through I-SPM-SP to get inter-cloud service provisioning policy information.

II.19 Reference point: I-SP-SA

The provisioning functional component interacts with service automation functional component through I-SP-SA to provision inter-cloud service automatically.

II.20 Reference point: I-PSM-SP

The provisioning functional component interacts with peer service management functional component through I-PSM-SP to access the OSS of a peer CSP in order to provision inter-cloud service among peer CSPs.

II.21 Reference point: I-MR-SP

The provisioning functional component interacts with monitoring and reporting functional component through I-MR-SP to exchange inter-cloud monitoring and provision information.

II.22 Reference point: I-PSM-SA

The service automation functional component interacts with peer service management functional component through I-PSM-SA to access peer CSP's OSS in order to delivers inter-cloud service automatically.

II.23 Reference point: I-SA-SPM

The service automation functional component interacts with service policy management functional component through I-SA-SPM to get inter-cloud service provisioning policies and configuration policies.

II.24 Reference point: I-SA-PSI

The service automation functional component interacts with peer service integration functional component through I-SA-PSI to provide automation processing of primary CSP switchover and switchback.

II.25 Reference point: I-PSM-SPM

The service policy management functional component interacts with peer service management functional component through I-PSM-SPM to access the OSS of a peer CSP to manage inter-cloud service policy and negotiated provisioning policy.

II.26 Reference point: I-SPM-PSI

The service policy management functional component interacts with peer service integration functional component through I-SPM-PSI to negotiate inter-cloud service policy with peer CSPs.

II.27 Reference point: I-SPM-ASPM

The service policy management functional component interacts with authorization and security policy management functional component through I-SPM-ASPM to exchange inter-cloud security policy information.

II.28 Reference point: I-SLM-IPM

The service level management functional component interacts with incident and problem management functional component through I-SLM-IPM to get inter-cloud incident and problem information for inter-cloud service level tracking, performance and capacity management.

II.29 Reference point: I-PSM-SLM

The service level management functional component interacts with peer service management functional component through I-PSM-SLM to access the OSS of a peer CSP to manage the service levels of a particular inter-cloud service to meet the requirements of the inter-cloud SLA.

II.30 Reference point: I-MR-SLM

The service level management functional component interacts with monitoring and reporting functional component through I-MR-SLM to get inter-cloud monitoring information.

II.31 Reference point: I-SLM-PSI

The service level management functional component interacts with peer service integration functional component though I-SLM-PSI to negotiate inter-cloud service SLA with peer CSPs.

II.32 Reference point: I-MR-IPM

The monitoring and reporting functional component interacts with incident and problem management functional component through I-MR-IPM to exchange inter-cloud monitoring information for inter-cloud incident and problem management.

II.33 Reference point: I-PSM-MR

The monitoring and reporting functional component interacts with peer service management functional component through I-PSM-MR to access the OSS of a peer CSP for monitoring and reporting.

II.34 Reference point: I-MR-PSI

The monitoring and reporting functional component interacts with peer service integration functional component through I-MR-PSI to get inter-cloud services negotiation, discovery, selection, reservation and release information for monitoring.

II.35 Reference point: I-PSM-IPM

The incident and problem management functional component interacts with peer service management functional component through I-PSM-IPM to access the OSS of a peer CSP for inter-cloud incidents and problems management.

II.36 Reference point: I-IPM-PSI

The incident and problem management functional component interacts with peer service integration functional component through I-IPM-PSI to get inter-cloud integration information for incident and problem management.

II.37 Reference point: I-PSM-AIM

The peer service management functional component interacts with authentication and identity management functional component through I-PSM-AIM for peer CSP and inter-cloud service authenticate and identities.

II.38 Reference point: I-PSM-EM

The peer service management functional component interacts with encryption management functional component through I-PSM-EM to get data encryption and API encryption for peer CSPs.

II.39 Reference point: I-PSM-BA

The peer service management functional component interacts with the business access functional component of a peer CSP through I-PSM-BA to access the business capabilities of a peer CSP.

II.40 Reference point: I-PSM-AA

The peer service management functional component interacts with the administration access functional component of a peer CSP through I-PSM-AA to access the administration capabilities of a peer CSP.

II.41 Reference point: I-PSI-AIM

The peer service integration functional component interacts with authentication and identity management functional component through I-PSI-AIM to provide authentication and identities for inter-cloud service integration.

II.42 Reference point: I-PSI-ASPM

The peer service integration functional component interacts with authorization and security policy management functional component through I-PSI-ASPM to apply authorization for peer CSPs to access inter-cloud services.

II.43 Reference point: I-PSI-EM

The peer service integration functional component interacts with encryption management functional component through I-PSI-EM to get API encryption function for peer CSPs.

II.44 Reference point: I-PSI-SA

The peer service integration functional component interacts with peer CSP's service access functional component through I-PSI-SA to access the services of a peer CSP.

Bibliography

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary*.

[b-ITU-T Y.3501] Recommendation ITU-T Y.3501 (2016), *Cloud computing framework and high-level requirements.*

Cloud computing – Overview of inter-cloud trust management

Recommendation ITU-T Y.3517

(12/2018)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Summary

Recommendation ITU-T Y.3517 provides an overview of inter-cloud trust management by specifying isolation and security management mechanisms, inter-cloud trust management model, reputation-based trust management in an inter-cloud environment, cloud service evaluation framework and the relationship with cloud computing reference architecture. It also provides requirements for inter-cloud trust management derived from the corresponding use cases.

Keywords

Inter-cloud, inter-cloud trust management model, isolation and security mechanism, management, reputation-based trust management, trust, trust management.

Table of Contents

1 Scope

This Recommendation describes inter-cloud trust management aspects including:

– isolation and security management mechanism;
– trust management model;
– reputation-based trust management;
– cloud service evaluation framework;
– relationship with cloud computing reference architecture;
– requirements for inter-cloud trust management and relative use cases.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing*.

[ITU-T Y.3501] Recommendation ITU-T Y.3501 (2016), *Cloud computing – Framework and high-level requirements*.

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014) | ISO/IEC 17789:2014, *Cloud computing – Reference architecture*.

[ITU-T Y.3511] Recommendation ITU-T Y.3511 (2014), *Framework of inter-cloud computing*.

[ITU-T Y.3514] Recommendation ITU-T Y.3514 (2017), *Cloud computing – Trusted inter-cloud computing framework and requirements*.

[ITU-T Y.3516] Recommendation ITU-T Y.3516 (2017), *Cloud computing – Functional architecture of inter-cloud computing*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 cloud computing [b-ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

3.1.2 cloud service [b-ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.3 cloud service agreement [b-ISO/IEC 19086-1]: Documented agreement between the cloud service provider and cloud service customer that governs the covered service(s).

NOTE – A cloud service agreement can consist of one or more parts recorded in one or more documents.

3.1.4 cloud service customer [b-ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

NOTE – A business relationship does not necessarily imply financial agreements.

3.1.5 cloud service level objective [b-ISO/IEC 19086-1]: Commitment a cloud service provider makes for a specific, quantitative characteristic of a cloud service, where the value follows the interval scale or ratio scale.

NOTE – An SLO commitment may be expressed as a range.

3.1.6 cloud service provider [b-ITU-T Y.3500]: Party which makes cloud services available.

3.1.7 cloud service qualitative objective [b-ISO/IEC 19086-1]: Commitment a cloud service provider makes for a specific, qualitative characteristic of a cloud service, where the value follows the nominal scale or ordinal scale.

NOTE 1 – A cloud service qualitative objective may be expressed as an enumerated list.

NOTE 2 – Qualitative characteristics typically require human interpretation.

NOTE 3 – The ordinal scale allows for existence/non-existence.

3.1.8 inter-cloud computing [ITU-T Y.3511]: The paradigm for enabling the interworking between two or more cloud service providers.

3.1.9 service level agreement (SLA) [b-ITU-T Y.3500]: Documented agreement between the service provider and customer that identifies services and service targets.

NOTE 1 – A service level agreement can also be established between the service provider and a supplier, an internal group or a customer acting as a supplier.

NOTE 2 – A service level agreement can be included in a contract or another type of documented agreement.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

BSS Business Support System

CSA Cloud Service Agreement

CSC Cloud Service Customer

CSP Cloud Service Provider

DoS Denial-of-Service

E2E End-to-End

IaaS Infrastructure as a Service

NaaS Network as a Service

OSS Operations Support System

SaaS Software as a Service

SDN Software Defined Network

SLA Service Level Agreement

SLO cloud Service Level Objective

SQO cloud Service Qualitative Objective

SSO Single Sign-On

TLS Transport Layer Security

VM Virtual Machine

5 Conventions

In this Recommendation:

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

6 Overview of inter-cloud trust management

The inter-cloud computing concept is based on the relationship (pattern) among multiple cloud service providers (CSPs). This pattern (peering, federation or intermediary) allows a CSP to interwork with one or more peer CSPs to assure intermediation and security of services provided by these CSPs. The trusted inter-cloud relationship among multiple CSPs relies on confidence between CSPs, or between a cloud service customer (CSC) and a CSP, as one of them has to delegate physical control over applications, services, resources and data to the others. Therefore, trust management is a key point between CSPs, or between a CSC and a CSP in inter-cloud.

The trust management of inter-cloud uses a two-dimensional (vertical and horizontal) model, where the vertical axis is based on the layers of the cloud computing reference architecture [ITU-T Y.3502], and the horizontal ones is based on the interconnection of CSPs based on the inter-cloud framework [ITU-T Y.3511].

The inter-cloud trust management framework relies on components for managing isolation and security mechanisms, which handle cross-layer trust and establish chain of trust, respectively [ITU-T Y.3514]. According to particular needs, inter-cloud trust management may either be CSC-related or CSP-related.

From a CSC-related perspective, major threats concern data security and privacy. Even assuming a trusted cloud service provider, a malicious administrator has sufficient permissions to affect unauthorised use and to modify customer information. Thus, CSP control over the infrastructure should be limited to avoid inspection or analysis of user data and virtual machine (VM) instances without explicit CSC consent. Moreover, security should be self-service, so that a CSC can exercise fine-grained control over protection of their cloud resources according to a given security service level agreement (SLA). This means the CSC should be able to actively monitor its allocated resources, while enabling a high level of customizability of the architecture and its services.

From a CSP-related perspective, major threats are malicious customers issuing attacks against the virtualization layer, to break isolation or perform denial-of-service (DoS). An attacker is a non-privileged malicious cloud tenant. Mitigation of such threats implies first isolation: tenants should not be authorized to monitor or modify VM state or data from other tenants. It also means a small trusted computing base: the number of vulnerabilities and failures in the platform is directly linked with the code size run at the highest privilege level and the set of primitives exported.

Many different classes of mechanisms and architectures have been proposed to address this issue, where trust management and isolation are intimately linked. Representative isolation architectures include modular hypervisors partly controlled by the CSC or secure enclaves based on hardware security mechanisms. Side-channel attacks also introduce major isolation issues for inter-cloud systems. Although many cryptographic solutions protect user confidentiality in the cloud, it is not possible to perform efficient and fast enough arbitrary computations on the data while they are encrypted.

In an inter-cloud environment, reputation is a key factor for selecting the CSP to transact with. There are different approaches to implement reputation-based trust management in inter-cloud environments, all of them are based on a uniform cloud SLA framework which could make CSP and CSC avoid confusion and have a common understanding about the cloud service quality commitment.

6.1 Isolation and security management mechanism

The isolation and security of trusted inter-cloud is based on distributed cloud management. It enables the CSP who provides cloud services to a CSC to have end-to-end (E2E) and unified control for trust of cloud services across multiple CSPs.

For implementation of managing isolation and security, mechanisms could be used as follows:

– **Annotation of workloads and data**: to increase security of trusted inter-cloud computing, it is necessary to define a terminology (language) to annotate (or tag) workloads and data with security requirements (such as permissible storage locations). These annotations will be processed by the system during scheduling and migration to ensure that workload constraints are maintained. Additionally, annotation of workloads allows the use of appropriate network data plane mechanisms (e.g., software defined network (SDN)) for strong security protection and traffic isolation to ensure that the above constraints are reached when workloads are practically placed, executed (data accessed and stored) and migrated. Such annotation of workloads and data might be based on standards for data categorization (see clause 6.4 of [ITU-T Y.3514]).

– **Modular hypervisors partly controlled by the CSC**: hypervisors usually have a large and complex administrative domain with privileges to inspect a client's VM state. Attacks against or misuse of the administrative domain can compromise client security and privacy. Moreover, these hypervisors provide clients inflexible control over their own VMs. Modular hypervisors simultaneously address problems with security/privacy and inflexible control. It introduces a novel privilege model that reduces the power of the administrative domain and gives the CSC more flexible control over their own VMs. It splits administrative privileges between a system-wide domain and per-client administrative domains. Each CSC can manage and perform privileged system tasks on its own VMs, thereby providing flexibility. The system-wide administrative domain cannot inspect the code, data or computation of client VMs, thereby ensuring security and privacy.

– **Secure enclave based on hardware security mechanisms**: secure enclave is an isolated process, executed on a platform that provides confidentiality and integrity of code and data as well as sealing and attestation. Isolated execution of a process restricts access to a subset of memory to that particular process or enclave. No other process on the same processor, operating system, hypervisor, or system management module, can access this memory. Sealing is the authenticated encryption of data with an encryption key based on the identity of the enclave and the platform it is running on. Attestation is the ability to prove to third parties that a secure enclave is running with a particular identity securely on the hardware.

– **Single sign-on (SSO)**: in an inter-cloud environment, the CSC should be able to access various resources and services offered by different CSPs once they are successfully authenticated in the inter-cloud. Since each CSP has its own authentication mechanism, a standard method that provides SSO authentication within inter-cloud environments should be deployed. In an inter-cloud environment, SSO can be achieved through the delegation of trust that allows an entity to act on another entity's behalf. This mechanism allows entities of inter-cloud to securely interact by establishing a chain of trust of proxy certificates. SSO can also be achieved through the use of a trusted third party who will certify credentials on behalf of all parties of inter-cloud.

NOTE – The functionalities for managing isolation and security mechanisms are provided in Appendix II.

6.2 Inter-cloud trust management model

The inter-cloud trust management is realized based on a two-dimensional (vertical and horizontal) model as follows:

– The vertical axis (cross-layer) is based on the layers of the cloud computing reference architecture [ITU-T Y.3502]. The inter-cloud trust management in this dimension is realized over functional components for managing isolation and security mechanisms. The components managing isolation ensure that different tenants and their workloads and data are isolated and inaccessible to one another in each layer. The components managing security, establish a chain of trust in the cross-layer dimension. In higher layers, it focusses on user-centric trust, such as user identity

management, authentication and authorization. In lower layers it focusses on resource control and security over the distributed inter-cloud infrastructure, such as virtualization and encryption management.

– The horizontal axis (cross-provider) is based on the interconnection of CSPs and relies on the inter-cloud framework [ITU-T Y.3511]. The inter-cloud trust management in this dimension is realized over functional components for managing security mechanisms. The trust management functionalities located in the multi-layer function ("Authorization and security policy management") establish a chain of trust between CSPs with peering, federation and intermediary patterns.

6.3 Reputation-based trust management in inter-cloud environment

In an inter-cloud environment, information such as a CSP's competence, honesty, availability, quality of service and reputation will influence the selection of the CSP to transact with. Therefore, there is a need to assess and maintain the reputation of CSPs.

Reputation is a measurement which could be derived from direct or indirect knowledge of earlier interactions of peers and is used to assess the level of trust to a peer. As an entity can trust another entity in the inter-cloud based on their reputation, we can use reputation to build trust.

One approach to implementing reputation-based trust management is shown in Figure 6-1. It is a distributed framework that enables interested parties to determine the reputation of inter-cloud entities. In this approach, each CSP has its own trust evaluation system which maintains and computes its trust values locally. Trust value is a reputation scoring for CSPs and could be referenced in selecting a CSP to transact with. It could be calculated in realtime based on direct observation and experience (i.e., first-hand reputation information) and indirect information by sharing observations and experience measures with other entities (i.e., second-hand reputation information).

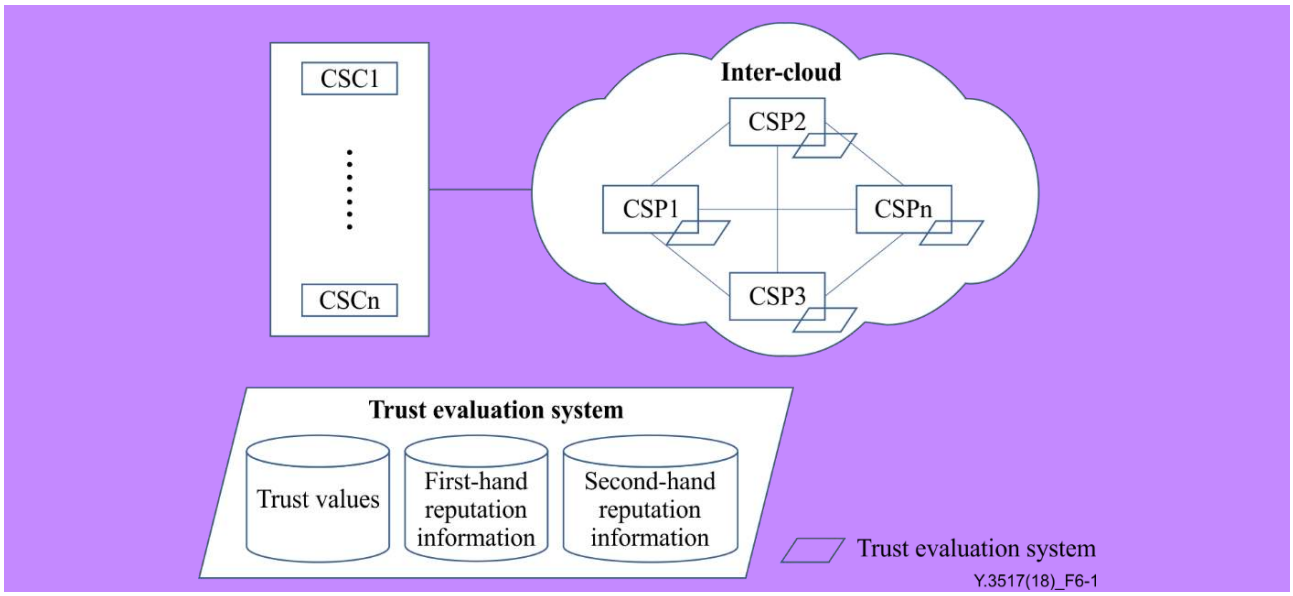


Figure 6-1 – One approach to implement reputation-based trust management

The trust evaluation system is responsible for collecting and maintaining reputation information such as a CSP's competence, honesty, availability, quality of service about every other CSP that it has peering agreements with, and this information could be represented by parameters such as ''mean time between failures'', ''mean time to restore service'', ''ready for service date'' and so on. First-hand reputation information should be updated when a CSP completes a transaction with other CSPs. At the same time, the trust evaluation system should publish its updated first-hand reputation information to a subset of their peers that they have a peering agreement with. Since the integrity of the second-hand reputation information has signally influence on the quality of a trust evaluation system, a mechanism should be implemented to protect against unfair ratings from others.

Another approach to implement reputation-based trust evaluation is shown in Figure 6-2. It is a centralized framework which has one or some independent trust evaluation systems operated by a third-party operator. With this approach, CSPs do not have their own trust evaluation system; they only provide their first-hand reputation information to the centralized trust evaluation system and query the trust values of CSPs from the centralized trust evaluation system when they need it. In this approach, the trust evaluation system calculates the trust value for CSPs only based on second-hand reputation information provided by CSPs in the inter-cloud. Therefore, an efficient mechanism for protecting against unfair ratings is more important in this approach.

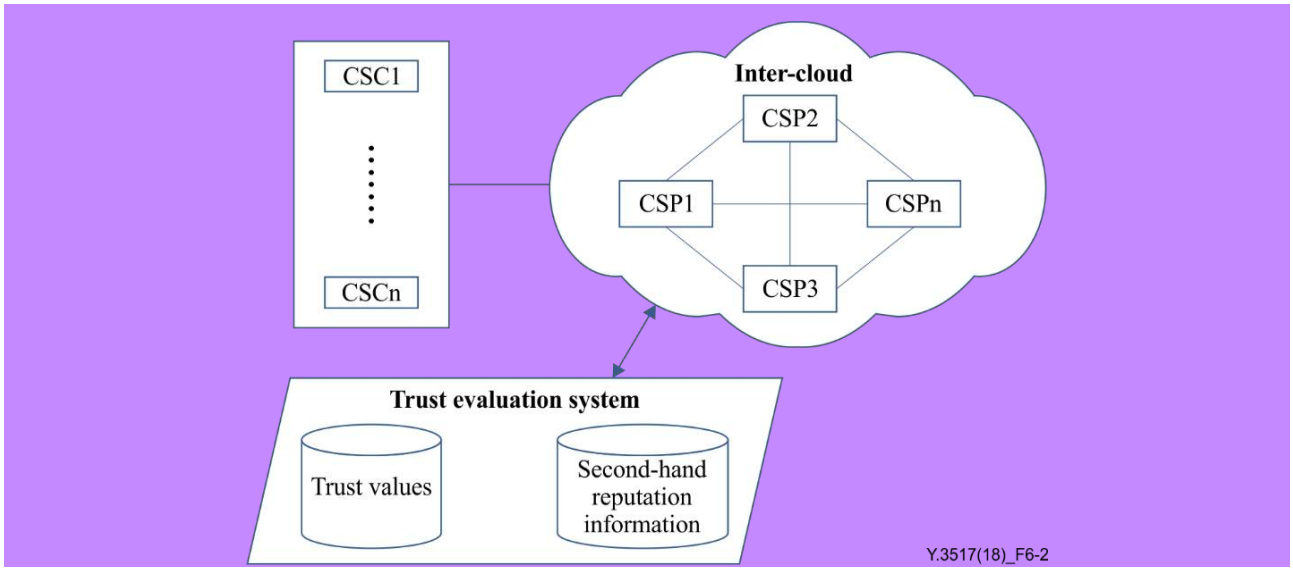


Figure 6-2 – Another approach to implement reputation-based trust management

6.4 Cloud service evaluation framework

The reputation of a CSP is highly correlated with the evaluation of cloud services it provides. A CSC could compare and evaluate cloud services through the cloud SLA provided by the CSP. A cloud SLA is a part of the cloud service agreement (CSA) that includes cloud service level objectives (SLOs) and cloud service qualitative objectives (SQOs) for the covered cloud service. An SLO is a commitment a CSP makes for a specific, quantitative characteristic of a cloud service, where the value follows the interval scale or ratio scale. An SQO is a commitment a cloud service provider makes for a specific, qualitative characteristic of a cloud service, where the value follows the nominal scale or ordinal scale. Both SLO and SQO could be measured by metrics. Metric is the standard of measurement that defines the conditions and the rules for performing the measurement and for understanding the results of a measurement.

With a uniform cloud SLA framework, a CSP and a CSC could avoid confusion and have a common understanding about the cloud service quality commitment. Therefore, it could be used as a cloud service evaluation framework by a CSC when comparing cloud services from different cloud service providers.

For more information about CSA, cloud SLA, SLO, SQO and cloud SLA metric models refer to [b-ISO/IEC 19086-1] and [b-ISO/IEC 19086-2].

6.5 Relationship with cloud computing reference architecture

The cloud computing reference architecture [ITU-T Y.3502] provides an architectural framework that is effective for describing the cloud computing roles, sub-roles, cloud computing activities, cross-cutting aspects, as well as the functional architecture and functional components of cloud computing. It also defines functional components for supporting inter-cloud computing, e.g., peer service integration and peer service management.

The inter-cloud computing functional architecture [ITU-T Y.3516] identifies inter-cloud specific extensions to functional components that are part of integration, security systems, operations support systems (OSSs) and business support systems (BSSs). For trusted inter-cloud, it defines a function called trust management. The trust management functionalities (see clause 6.2 of [ITU-T Y.3514]) are supported by the "authorization and security policy management" functional component within the multi-layer functions of the cloud computing reference architecture [ITU-T Y.3502]. Inter-cloud trust management can be realized using above functional components and functionalities. Inter-cloud trust management is also supported by functional components for managing isolation and security mechanisms, these functional components located in the "security systems" of the cloud computing reference architecture, as well.

This Recommendation is based on the functions defined in [ITU-T Y.3502], [ITU-T Y.3516] and [ITU-T Y.3514]. This Recommendation focuses on the trust management model and requirements in an inter-cloud environment based on the establishment of relationships (patterns) among multiple peer CSPs, including peering, federation and intermediary which are defined in [ITU-T Y.3511].

7 Requirements for inter-cloud trust management

This clause identifies requirements applicable to inter-cloud trust management.

7.1 Inter-cloud trust policies and credentials

It is recommended that a CSP provides specification of policies and credentials used for trust management.

It is recommended that a CSP implements a trust management system to evaluate whether the provided credentials satisfy the specified policy.

7.2 Inter-cloud reputation scoring

It is recommended that a CSP uses a trust scheme to evaluate whether other CSPs among inter-cloud relationships fulfil trust management requirements.

It is recommended that a CSP evaluate other CSPs among inter-cloud relationships to create and update reputation scoring of CSPs.

7.3 Inter-cloud reputation-based trust evaluation

It is recommended that a CSP has a trust evaluation system to manage other CSPs' reputations.

It is recommended that a CSP supports query and compares reputation of other CSPs from a third- party trust evaluation system.

7.4 SSO authentication

It is recommended that a CSP supports an SSO mechanism to enable a CSC’s access to various services offered by different CSPs once it is successfully authenticated by inter-cloud.

7.5 Periodical verification

It is recommended that a CSP supports a periodical verification mechanism to check if a CSC still has the privilege of accessing the CSP's service.

7.6 Control privilege for VM and data

It is recommended that a CSP avoids inspection or analysis of a CSC's data and VM instances without explicit CSC consent.

It is recommended that a CSP supports fine-grained CSC control over protection of its cloud resources according to a given security SLA.

It is required that a CSP avoids unauthorised use or modifications of a CSC's VM state, service data or CSC data by other CSCs.

8 Security considerations

Security aspects for consideration within the cloud computing environment, including inter-cloud computing, are described in [ITU-T X.1601] which analyses security threats and challenges, and describes security capabilities that could mitigate these threats and meet these security challenges.

Appendix I

Use case of inter-cloud trust management

(This appendix does not form an integral part of this Recommendation.)

I.1 Use case template

The use cases developed in this appendix should adopt the following unified format for better readability and convenient material organization.

Table I.1 – Use case template

Title	The title of the use case
Description	Scenario description of the use case
Roles	Roles involved in the use case
Figure (optional)	Figure to explain the use case, optional not mandatory
Pre-conditions (optional)	The necessary pre-conditions that should be achieved before starting the use case
Post-conditions (optional)	The post-conditions that will be carried out after the termination of current use case
Derived requirements	Requirements derived from the use cases, whose detailed description is presented in the dedicated chapter

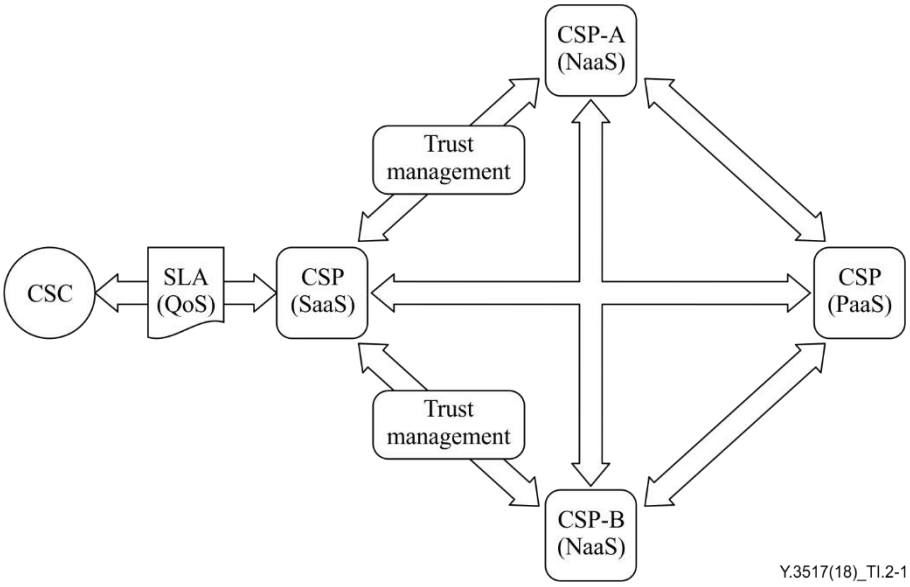
I.2 Use case of trusted network function virtualization

This use case illustrates trust management aspect in inter-cloud. The federation pattern of inter-cloud used to illustrate the use case is an example only.

Table I.2 – Trusted network function virtualization

Title	Trusted network function virtualization
Description	A CSC requests ''premium aoftware'' as a service (software as a service (SaaS)), respecting network quality of service (QoS). The CSP (SaaS) forms inter-cloud federation pattern among CSP(PaaS) and CSPs (network as a service (NaaS)). The CSP(SaaS) becomes contact point for CSC. The CSP-A(NaaS) and CSP-B(NaaS) uses network function virtualization (NFV) and SDN technologies to serve NaaS service. The CSP(SaaS) uses a trust management system to keep track of CSP(NaaS) service. In case CSP-A(NaaS) performed out of schemes used to compute trust, the SaaS service is automatically established between the CSP(SaaS) and CSP-B(NaaS). Additionally, the CSP(SaaS) updates information on reputation of CSPs(NaaS).
Roles	CSC, CSP(SaaS), CSP(PaaS), CSP(NaaS).

Table I.2 – Trusted network function virtualization

Figure (optional)	
Pre-conditions (optional)	– The CSPs(SaaS) form federation pattern of inter-cloud.
Post-conditions (optional)	– The CSPs(SaaS) implement trust management system. – The CSP(SaaS) uses reputation scores of CSPs.
Derived requirements	– Inter-cloud trust policies and credentials (refer to clause 7.1). – Inter-cloud reputation scoring (refer to clause 7.2).

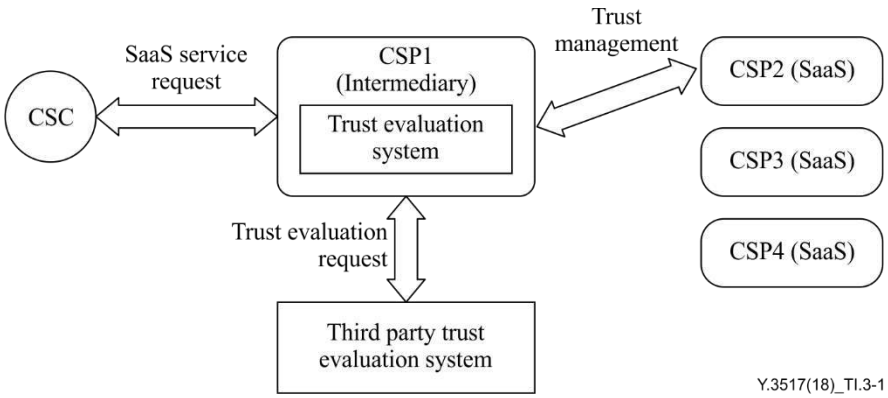
I.3 Use case of selecting CSP by reputation-based trust evaluation

This use case illustrates reputation-based trust evaluation in inter-cloud. The intermediary pattern of inter-cloud used to illustrate the use case is an example only.

Table I.3 – Selecting CSP by reputation-based trust evaluation

Title	Selecting CSP by reputation-based trust evaluation
Description	– The CSC requests a SaaS service from CSP1; – CSP1 cannot provide the service by itself, it plans to fulfil the service with inter-cloud intermediary pattern in which CSP1 acts as the intermediary; – All of CSP2(SaaS), CSP3(SaaS) and CSP4(SaaS) can provide the services CSP1 needs; – CSP1 will select a CSP as the secondary CSP base on the reputation of them. In this step: 1) If CSP1 has an internal trust evaluation system, it will query and compare the reputation of CSP2, CSP3 and CSP4 in this system and choose the best one to establish a trust relationship with; 2) If CSP1 does not have an internal trust evaluation system or there are no records about CSP2, CSP3 and CSP4 in the internal system, CSP1 should find a third-party trust evaluation system to query and compare the reputation data about these CSPs; – CSP2(SaaS) is the best choice and CSP1 establishes a trust relationship with it.
Roles	CSC, CSP, CSP(SaaS).

Table I.3 – Selecting CSP by reputation-based trust evaluation

Figure (optional)	
Pre-conditions (optional)	– All of CSP2(SaaS), CSP3(SaaS) and CSP4(SaaS) can provide the services CSP1 needs. – CSP1 has an internal trust evaluation system. – There is a third-party trust evaluation system.
Post-conditions (optional)	– CSP1 establishes a trust relationship with CSP2(SaaS) and provides service to the CSC with an inter-cloud intermediary pattern.
Derived requirements	– Inter-cloud reputation-based trust evaluation (refer to clause 7.3).

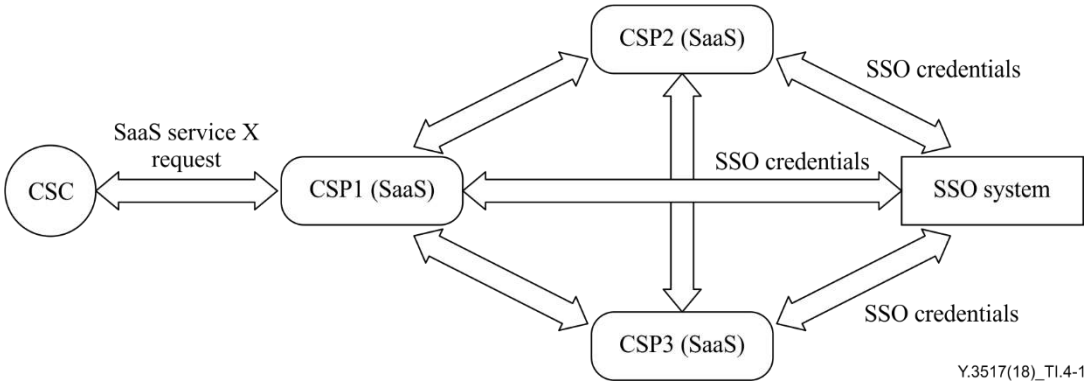
I.4 Use case of SSO authentication within inter-cloud environment

This use case illustrates SSO authentication in inter-cloud. The federation pattern of inter-cloud used to illustrate the use case is an example only.

Table I.4 – SSO authentication within inter-cloud environment

Title	SSO authentication within inter-cloud environment
Description	– The CSC requests SaaS service X from CSP1(SaaS); – The CSPs(SaaS) form inter-cloud federation pattern among them. The service X is integrated from services provided by CSP1(SaaS), CSP2(SaaS) and CSP3(SaaS); – Each CSP has its own identity management system, and the CSC is not willing to be authenticated more than one time when accessing SaaS service X; – There is a trusted third-party SSO system which provides a certification service to certify credentials on behalf of all parties in the federation. With this SSO mechanism, the CSC is able to access various SaaS services offered by different CSPs once it is successfully authenticated by any member of the federation; – Each CSP supports a periodical verification mechanism to check if the CSC still has the privilege to access the CSP's service.
Roles	CSC, CSPs(SaaS).

Table I.4 – SSO authentication within inter-cloud environment

Figure (optional)	
Pre-conditions (optional)	– The CSPs(SaaS) form a federation pattern of inter-cloud. – The CSPs(SaaS) use a third-party SSO system for implementing SSO authentication functionality within their federation.
Post-conditions (optional)	– The CSC is able to access various services offered by different CSPs once it is successfully authenticated by any member of the CSPs(SaaS) federation.
Derived requirements	– SSO authentication (refer to clause 7.4). – Periodical verification (refer to clause 7.5).

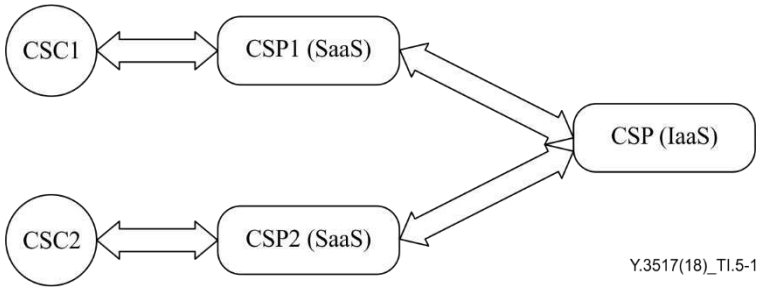
I.5 Use case of control privilege of inter-cloud

This use case illustrates security and control concerns in inter-cloud. The peering pattern of inter-cloud used to illustrate the use case is an example only.

Table I.5 – Control privilege of inter-cloud

Title	Control privilege of inter-cloud
Description	– The CSC requests SaaS service from CSPs(SaaS); – Both CSP1(SaaS) and CSP2(SaaS) use infrastructure including computing and storage resources from CSP (infrastructure as a service (IaaS)) to provide their cloud services. Therefore, they all have service instances and data in CSP(IaaS); – For the sake of CSPs(SaaS) data security and privacy, CSP(IaaS) control over the infrastructure should be limited to avoid inspection or analysis of CSPs(SaaS) data and VM instances without explicit CSPs(SaaS) consent; – CSPs(SaaS) should be able to exercise fine-grained control over protection of their cloud resources according to a given security SLA. This means that CSPs(SaaS) should be able to actively monitor their allocated resources; – CSPs(SaaS) should not be authorized to monitor or modify VM state, service data and CSC data from other CSCs.
Roles	CSCs, CSPs(SaaS), CSP(IaaS).

Table I.5 – Control privilege of inter-cloud

Figure (optional)	
Pre-conditions (optional)	– The CSPs(SaaS) and CSP(IaaS) form peering pattern of inter-cloud.
Post-conditions (optional)	
Derived requirements	– Control privilege for VM and data (refer to clause 7.6).

Appendix II

Functionalities for managing isolation and security mechanism

(This appendix does not form an integral part of this Recommendation.)

This appendix provides functionalities for managing isolation and security mechanisms.

II.1 Functionalities for managing isolation and security mechanism

The functionalities for managing isolation and security mechanisms are supported by the 'authentication and identity management'', ''authorization and security policy management'', ''encryption management'' and ''platform and virtualization management'' functional components within the multi-layer functions of the cloud computing reference architecture [ITU-T Y.3502]. The positioning of these functionalities for managing isolation and security mechanisms across the CSPs, which provide inter-cloud services, is presented in Figure II.1.

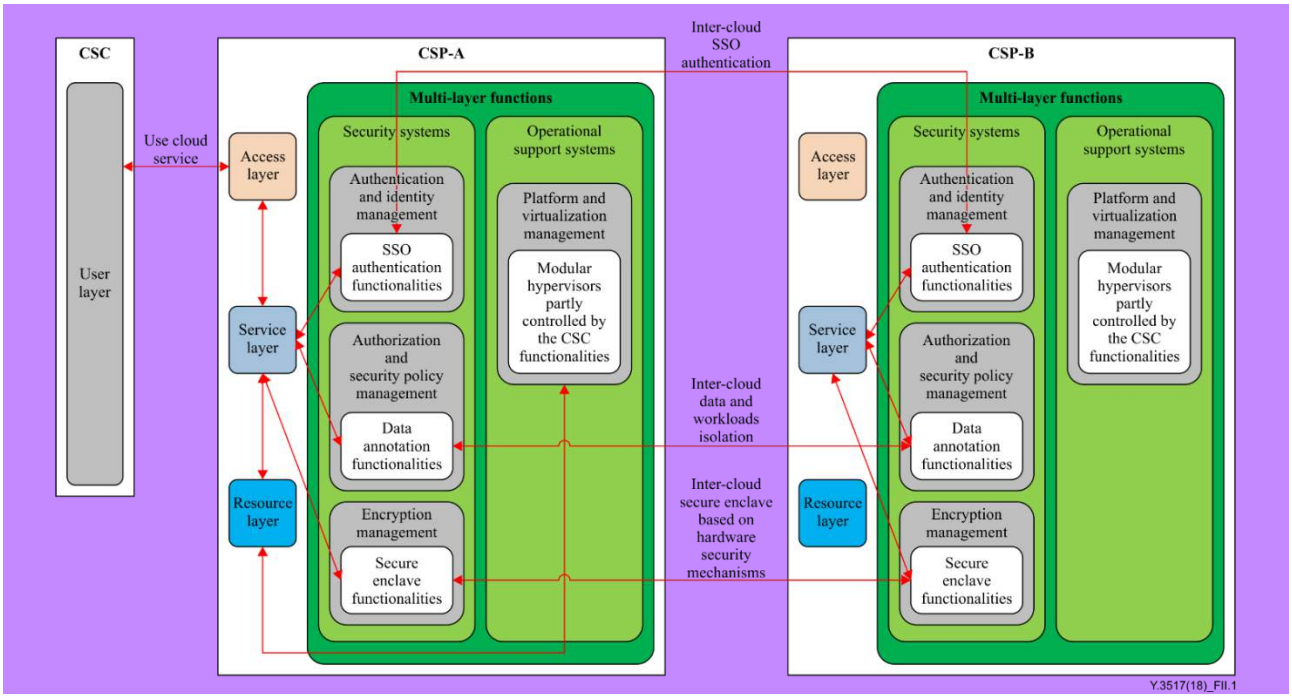


Figure II.1 – The positioning of functionalities for managing isolation and security mechanisms in inter-cloud

The data annotation functionalities are built upon elements as follows:

– **Data annotation definer:** manages the terminology (language) to annotate (or tag) workloads and data;

– **Data annotation manager:** responsible for annotating the workloads and data according to the isolation and security requirements;

– **Data annotation handler:** responsible for parsing and executing the isolation and security requirements based on the annotations of workloads and data.

The modular hypervisors partly controlled by the CSC functionalities are built upon elements as follows:

– **User domain manager:** responsible for building and managing the per-user administrative domain and user domains for each user;

– **System domain manager**: responsible for building and managing the system-wide administrative domain.

The secure enclave based on hardware security mechanisms functionalities are built upon elements as follows:

– **Secure enclave library:** responsible for implementing encrypted networking using transport layer security (TLS) (e.g., using a standard TLS library), encrypted and sealed storage, attestation, and inter-process communication. These are features that are exposed to the application code. Cloud service developers use these secure primitives to write their secure cloud service.

– **Discrete security chips coupled with processor features:** responsible for providing the necessary underlying capabilities to implement secure enclave.

The SSO authentication functionalities are built upon elements as follows:

– **User request handler:** responsible for accepting the identity information provided by the cloud service user and forwarding this information to the identity management system;

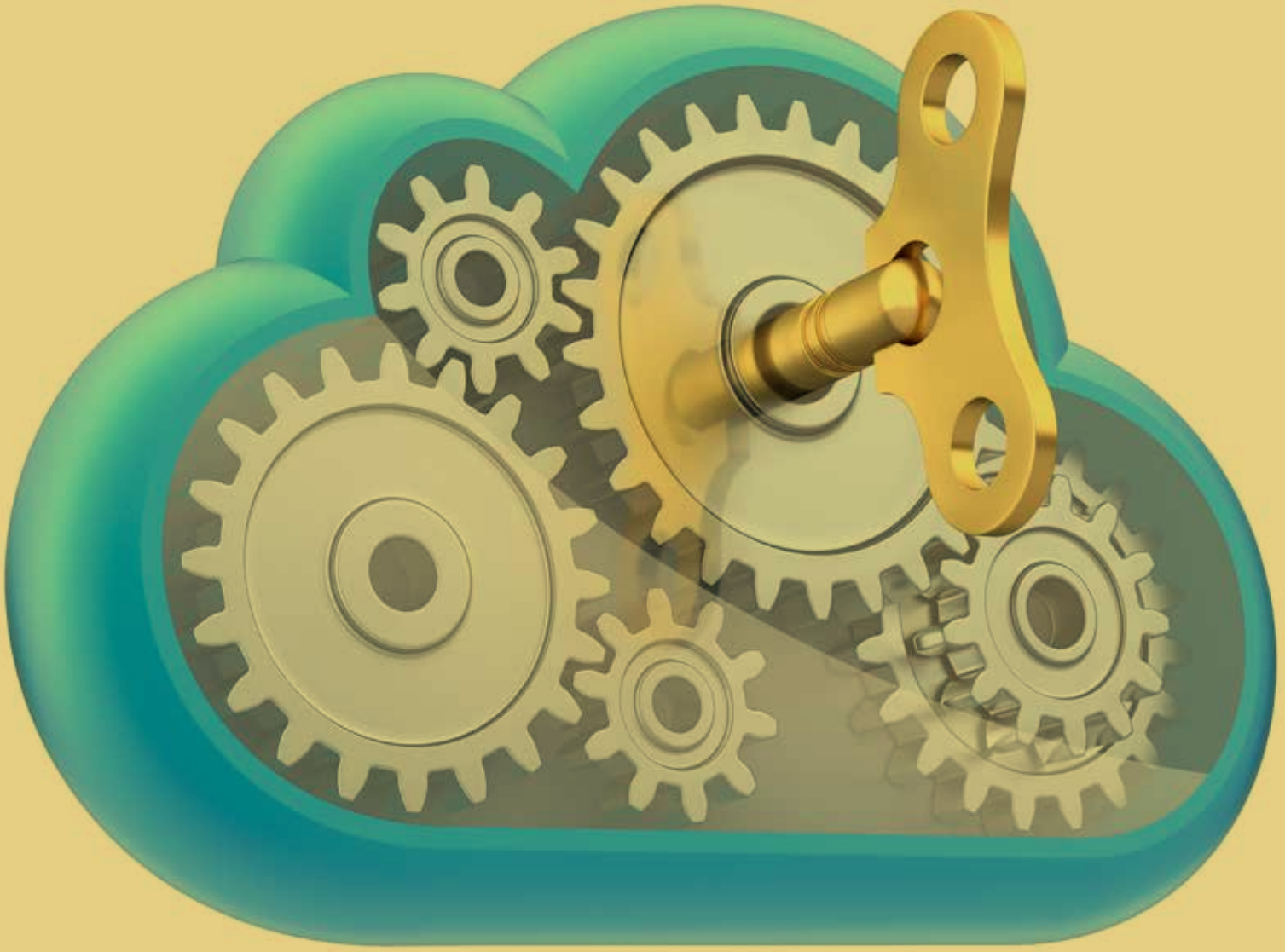
– **Identity management system:** responsible for authenticating CSC requests and sharing the result of this authentication to inter-cloud members. It is also responsible for managing the identity information of its associated inter-cloud members.

Bibliography

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014), *Information technology – Cloud computing – Overview and vocabulary*.

[b-ISO/IEC 19086-1] ISO/IEC 19086-1:2016, *Information technology – Cloud computing – Service level agreement (SLA) framework – Part 1: Overview and concepts*.

[b-ISO/IEC 19086-2] ISO/IEC 19086-2:2018, *Information technology – Cloud computing – Service level agreement (SLA) framework – Part 2: Metric model*.



The framework and overview of cloud computing interoperability testing

Recommendation ITU-T Q.4040

(02/2016)

SERIES Q: SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

Summary

Recommendation ITU-T Q.4040 describes the framework and provides an overview of cloud computing interoperability testing. According to the identified target areas of testing, this framework Recommendation includes an overview of cloud computing interoperability testing with common confirmed items, infrastructure capabilities type, platform capabilities type and application capabilities type interoperability testing. This Recommendation describes the overview target areas of testing for interoperability testing of cloud computing.

Keywords

Cloud computing, interoperability.

Table of Contents

1 Scope

This Recommendation describes the framework and provides an overview of cloud computing interoperability testing. According to the identified target areas of testing, this framework Recommendation includes an overview of cloud computing interoperability testing with common confirmed items, infrastructure capabilities type, platform capabilities type and application capabilities type interoperability testing.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.101] Recommendation ITU-T Y.101 (2000), *Global Information Infrastructure terminology: Terms and definitions*.

[ITU-T Y.1401] Recommendation ITU-T Y.1401 (2008), *Principles of interworking*.

[ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud Computing – Overview and vocabulary*.

[ITU-T Y.3501] Recommendation ITU-T Y.3501 (2016), *Cloud computing framework and high-level requirements*.

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014) | ISO/IEC 17789:2014, *Information technology – Cloud computing – Reference architecture*.

[ITU-T Y.3510] Recommendation ITU-T Y.3510 (2016), *Cloud computing infrastructure requirements*.

[ITU-T Y.3511] Recommendation ITU-T Y.3511 (2014), *Framework of inter-cloud computing*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 interoperability [ITU-T Y.101]: The ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged.

3.1.2 interworking [ITU-T Y.1401]: The term ''interworking'' is used to express interactions between networks, between end systems, or between parts thereof, with the aim of providing a functional entity capable of supporting an end-to-end communication.

3.1.3 cloud service provider (CSP) [ITU-T Y.3500]: Party which makes cloud services available.

3.1.4 cloud service customer (CSC) [ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 cloud interoperability: The capability to interact between CSCs and CSPs or between different CPSs, including the ability of CSCs to interact with cloud services and exchange information, the ability for one cloud service to work with other cloud services, and the ability for CSCs to interact with the cloud service management facilities of the CSPs.

3.2.2 cloud interoperability testing: Verifying functions and interaction that realize the cloud interoperability.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

BSS	Business Support Systems
CCRA	Cloud Computing Reference Architecture
CSC	Cloud Service Customer
CSP	Cloud Service Provider
IaaS	Infrastructure as a Service
ICT	Information and Communication Technology
IT	Information Technology
OSS	Operational Support Systems
PaaS	Platform as a Service
QoS	Quality of Service
SaaS	Software as a Service
SLA	Service-Level-Agreement
VM	Virtual Machine

5 Overview of cloud computing interoperability testing

Interoperability in the context of cloud computing includes the ability of a cloud service customer to interact with a cloud service and exchange information according to a prescribed method and obtain predictable results. Typically, interoperability implies that the cloud service operates according to an agreed specification, one that is possibly standardized. The cloud service customer should be able to use widely available ICT facilities in-house when interacting with the cloud services, avoiding the need to use proprietary or highly specialized software. The interoperability of cloud services can be categorized by the management and functional interfaces of the cloud services. Many existing IT standards contribute to the interoperability between cloud consumer applications and cloud services, and between cloud services themselves. There are standardization efforts that are specifically initiated to address the interoperability issues in the cloud system. Interoperability also includes the ability for one cloud service to work with other cloud services, either through an inter-cloud provider relationship, or where a cloud service customer uses different multiple cloud services in some form of composition to achieve its business goals.

Interoperability stretches beyond the cloud services themselves and also includes the interaction of the cloud service customer with the cloud service management facilities of the cloud service provider. Ideally, the cloud service customer should have a consistent and interoperable interface to the cloud service management functionality and be able to interact with two or more cloud service providers without needing to deal with each provider in a specialized way.

The main purpose of interoperability testing is to evaluate the interaction between cloud service customer and cloud service provider to obtain predictable results, collaboration among different cloud services, and consistency and interoperability of management interface across different services.

A cloud capabilities type is a classification of the functionality provided by a cloud service to the cloud service customer, based on the resources used. There are three different cloud capabilities types [ITU-T Y.3500]: infrastructure capabilities type, platform capabilities type, and application capabilities type, which are different because they follow the principle of separation of concerns, i.e., they have minimal functionality overlap between each other. The interoperability testing in different cloud capabilities type is different; there are three major interoperability testing scenarios as follows:

- infrastructure capabilities type interoperability testing
- platform capabilities type interoperability testing
- application capabilities type interoperability testing.

As shown in Figure 1, there are three different target areas of cloud computing interoperability testing as follows:

- "CSC – CSP", dealing with interaction between CSC and CSP
- "CSP – CSP", dealing with collaboration among different CSPs
- "CSP – management", dealing with CSP management functions.

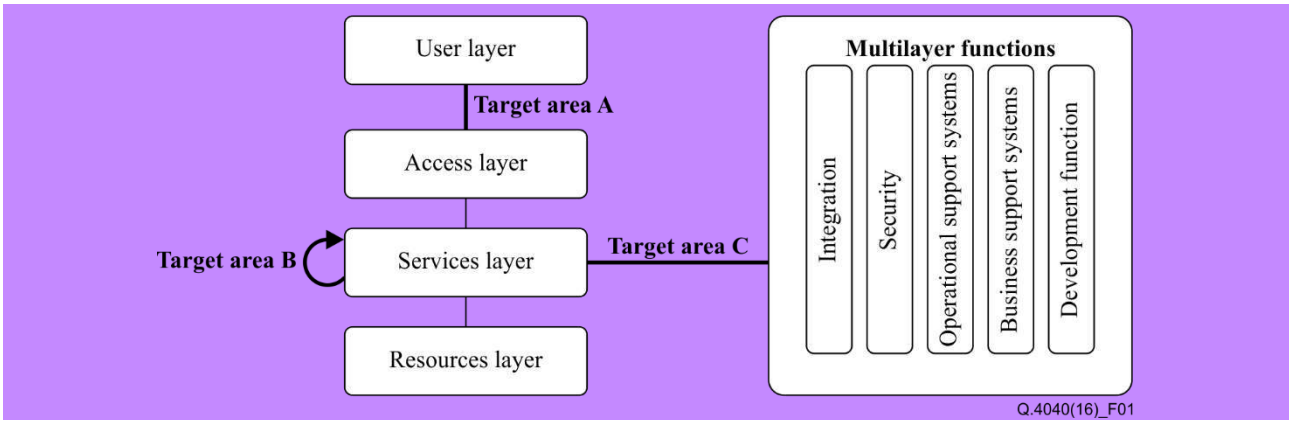


Figure 1 – Target areas of cloud computing interoperability testing

Also, the cloud architecture in terms of the common set of cloud computing functional components are described in [ITU-T Y.3502]. Figure 2 presents a high level overview of the CCRA functional components organized by means of the layering framework.

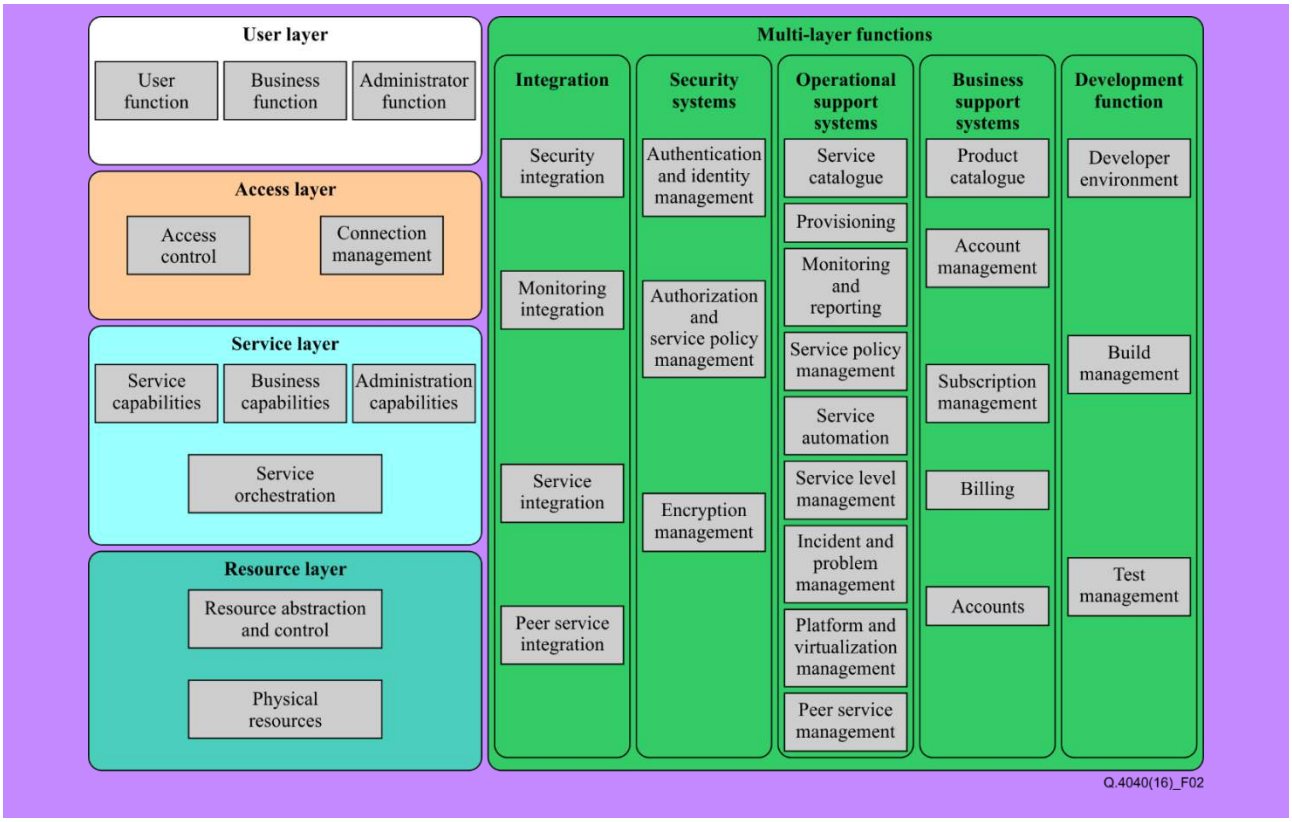


Figure 2 – Functional components of the CCRA

This Recommendation covers the typical functional components, not all components, and interworking among them in clauses 7, 8 and 9.

5.1 Common aspects to be considered in cloud computing interoperability testing

The aspects which should be considered for the testing of cloud computing interoperability need to be prescribed according to the requirements described in [ITU-T Y.3501]. The following items, picked up from the general requirements for cloud computing [ITU-T Y.3501], indicate common aspects to be considered in cloud computing interoperability testing:

- Service life-cycle management

It is required that cloud computing supports automated service provisioning, modification and termination during the service life-cycle.

- Regulatory aspects

It is required that all applicable laws and regulations be respected, including those related to privacy protection.

- Security

It is required that the cloud computing environment be appropriately secured to protect the interests of all persons and organizations involved in the cloud computing ecosystem.

- Accounting and charging

It is recommended that cloud computing supports various accounting and charging models and policies.

- Efficient service deployment

It is recommended that cloud computing enables efficient use of resources for service deployment.

- Interoperability

It is recommended that cloud computing systems comply with appropriate specifications and/or standards for allowing these systems to work together.

- Portability

It is recommended that cloud computing supports the portability of software assets and data of cloud service customers (CSCs) with minimum disruption.

- Service access

Cloud computing is recommended to provide CSCs with access to cloud services from a variety of user devices. It is recommended that CSCs be provided with a consistent experience when accessing cloud services from different devices.

- Service availability, service reliability and quality assurance

It is recommended that the cloud service provider (CSP) provides end-to-end quality of service assurance, high levels of reliability and continued availability.

5.2 Infrastructure capabilities type interoperability testing

Cloud infrastructure includes compute, storage, network and other hardware resources, as well as software assets. Abstraction and control of physical resources are essential means to achieve on-demand and elastic characteristics of cloud infrastructure. This way, physical resources can be abstracted into virtual machines (VMs), virtual storage and virtual networks. The abstracted resources are controlled to meet cloud service customers' (CSC) needs. [ITU-T Y.3510]

The goal for cloud infrastructure capabilities type interoperability is to devise and implement testing methods and conduct a basic set of functional tests for infrastructure capabilities type (IaaS) Interoperability in a hybrid cloud environment using both private and public clouds.

Ideally, cloud subscribers would like to be able to select any cloud provider based on the basis of service cost, performance and capabilities. In order to make this feasible for the cloud consumer, the various hypervisor platforms and infrastructure components involved will need to be interoperable and enable portability, leveraging defined industry standards.

Reliability and reproducibility of a change such as a VM migration involved in IaaS are based on pre-defined standards, specifications, frameworks, scenarios, and processes. This need exists in their organizations too for reasons such as being able to demonstrate the ability to move between internal private clouds, being able to move between cloud providers if necessary, and if for no other reason, to demonstrate that the service is not locked in to that environment with no relocation options once it has been established there.

5.3 Platform capabilities type interoperability testing

Platform capabilities type (PaaS) interoperability encourages seamless operation of cloud applications across providers, rapid integration with consumer orchestration engines, and automatable configuration and operation of both the PaaS container and the execution of the application itself. This provides the combined benefits of rapid application deployment and linear scalability without the overhead of directly managing the underlying infrastructure for the application, all while avoiding PaaS lock-in.

The business drivers for PaaS Interoperability are as follows:

- Rapid application deployment: Enable subscribers to quickly deploy new business applications. Reduce the overhead of ongoing application deployments.
- Application scalability: Ability to quickly scale applications up and back based on the real-time demand for those applications.
- Application migration: Ability to move applications from one discrete PaaS to another PaaS available from the same or different cloud provider with minimal effort.
- Business continuity: Migrate or replicate applications among PaaS services to address outages, security breaches, or other disruptions. This is intended to encompass both disaster recovery and disaster avoidance.

Interoperability perspectives follow:

- Interconnectability: The parallel process in which two coexisting environments communicate and interact.
- Portability: The serial process of moving a system from one cloud environment to another.

5.4 Application capabilities type interoperability testing

In portability and interoperability of application capabilities (SaaS) environments, business process functionality offered through SaaS solutions can be initially connected, transferred, or interconnected. SaaS interoperability allows organizations to create mash-ups from multiple SaaS and non-SaaS applications. This is an issue that primarily concerns data exchange, which includes metadata, and interface compatibility.

6 Cloud computing interoperability testing between CSC and CSP

CSC is a party in a business relationship for the purpose of using cloud services. The interoperability between CSC and CSP supports the CSC to interact with CSP according to a prescribed method and obtain predictable results. Enabled by interworking between CSC and CSP, CSC can use the capabilities provided by CSP, such as using the processing, network and storage capability. For example, CSC can use virtual machine provide by the CSP.

CSC can also perform business administration tasks such as subscribing to cloud service and administering use of cloud service through the interaction with CSP.

Based on the reference architecture described in [ITU-T Y.3502], the interworking involved in CSC-CSP relationship and corresponding test objective can be identified as follows:

- Interworking between CSC and CSP's service integration component.

  Test objective is to verify that CSP can provide connections to CSP's services for CSC.

- Interworking between CSC and CSP's authentication and identities management component

  Test objective is to verify that CSP can provide capabilities relating to user identities and the credentials required to authenticate users are provided when CSC access cloud services and related administration and business capabilities.

- Interworking between CSC and CSP's authorization and security policy management component

  Test objective is to verify that CSP can provide capabilities for the control and application of authorization for CSC to access specific capabilities or data.

- Interworking between CSC and CSP's product catalogue component

  Test objective is to verify that the CSP can provide capabilities for browsing available service list, and capabilities for management of the content of catalogue.

- Interworking between CSC and CSP's account management CSC

  Test objective is to verify that the CSP can provide capabilities for managing cloud service relationships, including management of contracts, subscription to cloud service, entitlements, service pricing and policies that apply to the treatment of CSC data.

- Interworking between CSC and CSP's subscription management component

  Test objective is to verify that the CSP can handle subscriptions from CSC to particular cloud services, aiming to record new or changed subscription information from the customer and ensure the delivery of the subscribed service(s) to the customer.

- Interworking between CSC and CSP's monitoring and report component

  Test objective is to verify that CSP can provide capabilities monitoring the cloud computing activities of other functional components throughout the CSP's system and providing reports on the behaviour of the cloud service provider's system.

- Interworking between CSC and CSP's service access

  Test objective is to verify that CSP can provide service access capabilities that provide access offered by CSP, perform authentication of the CSC and establish authorization to use particular capabilities of the cloud service. If authorized, the service access capabilities invoke the cloud service implementation which performs the request.

- Interworking between CSC and CSP's service capabilities

  Test objective is to verify that CSP can provide service capabilities which consist of the necessary software required to implement the service offered to CSC.

- Interworking between CSC and CSP's resource abstraction and control

  Test objective is to verify that CSP can provide access to the physical computing resources through software abstraction and to offer qualities such as rapid elasticity, resource pooling and on-demand self-service.

- Interworking between CSC and CSP's physical resources

  Test objective is to verify that the operational support systems can manage all the elements of the physical resources (e.g., computing resources, storage resources, and network resources).

For interoperability testing between CSC and CSP, the interoperability testing target should cover the interworking between CSC and CSP described above. A set of functional test cases need to be developed based on the corresponding test objectives, and perform functional test to determine if CSC interoperate with CSP. Figure 3 shows the relationships among functional components and functions for the "use cloud service" activity between CSC and CSP according to clause A.1.1 of [ITU-T Y.3502].

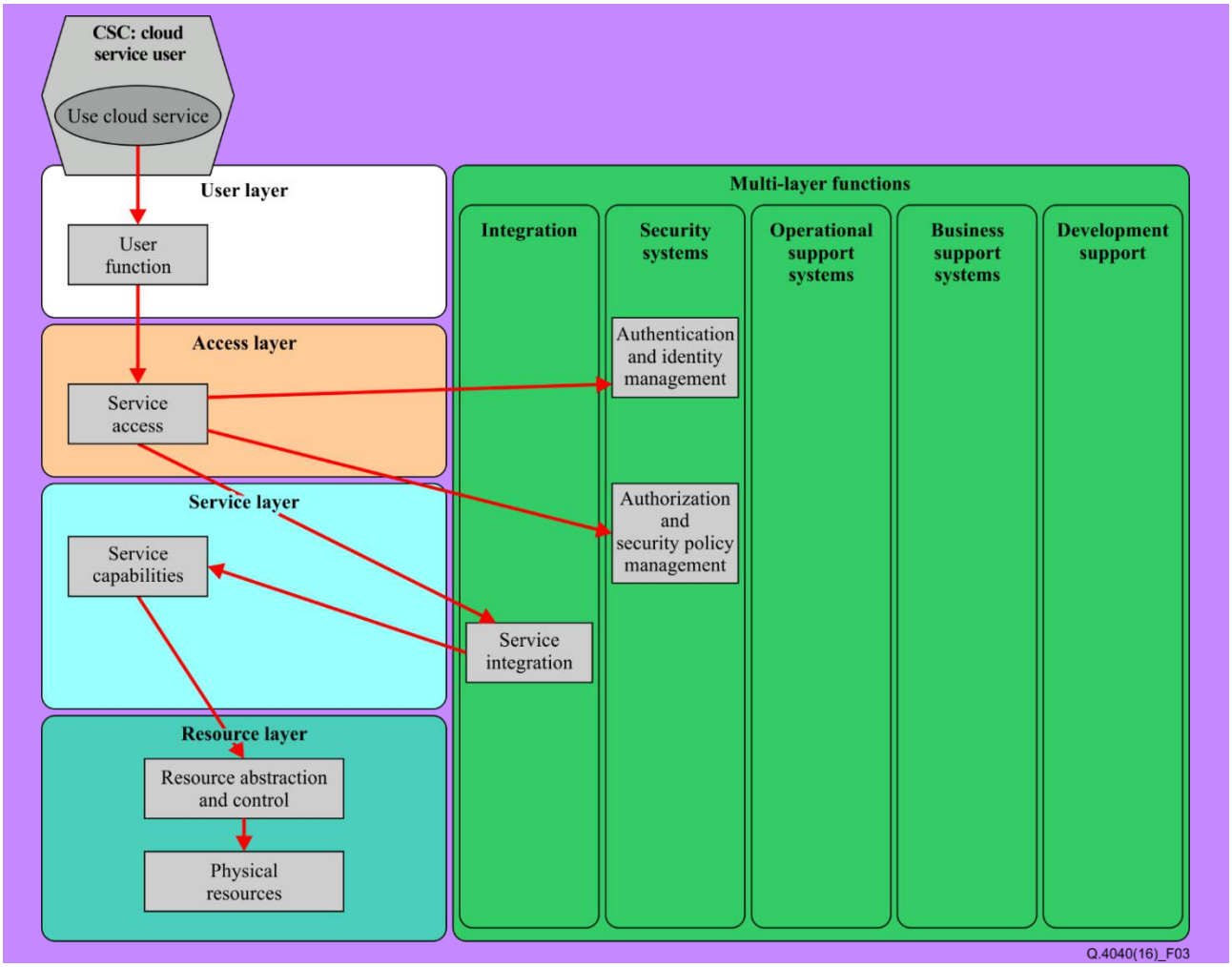


Figure 3 – Relationships among functional components and functions for the "use cloud service" activity between CSC and CSP

7 Cloud computing interoperability testing between CSP and CSP

Ideally, multiple interoperable CSPs could interact in different patterns of inter-cloud: peering, federation, and intermediary patterns, as defined in [ITU-T Y.3511]. In inter-cloud peering pattern, two CSPs interwork directly with each other, and one CSP can use the services provided by the peer CSP. In inter-cloud federation pattern, a group of peer CSPs mutually combine their service capabilities in order to provide the set of cloud services required by CSCs. In inter-cloud intermediary pattern, CSP interworks with one or more peer CSPs and provides intermediation, aggregation and arbitrage of services provided by these CSPs.

The functions which should be tested for inter cloud computing interoperability need to be prescribed according to the functional requirements described in [ITU-T Y.3511]. The following bullet items indicate aspects to be considered in the cloud computing interoperability testing of the CSP-CSP interworking.

- SLA and policy negotiation should be confirmed as follows:
  - the SLA and policy information that is aware of the SLA information related to the QoS and performance aspects of the CSPs involved is exchanged among multiple CSPs using standard formats;
  - the SLA and policy information comparing, negotiating and settling down service provisioning policies is exchanged among multiple CSPs using standard formats.

- Resource monitoring should be confirmed as follows:
  - resource information is exchanged in a standard manner among multiple CSPs;
  - updated resource information is exchanged among multiple CSPs in synchronization with the events involving the CSPs;
  - collecting information about the usage and performance status of the resources is exchanged among multiple CSPs periodically or on a request basis;
  - collecting information about the resource availability is exchanged among multiple CSPs periodically or on a request basis;
  - monitoring information in commonly defined ways is exchanged among multiple CSPs.
- Resource performance estimation and selection should be confirmed as follows:
  - the achievable resource performance that is available reserved resources in the secondary CSPs is exchanged between secondary CSPs.
- Resource discovery and reservation should be confirmed as follows:
  - CSP can discover available resources of the peer CSPs;
  - discovered resources in the peer CSPs are reserved;
  - discovered resources in the peer CSPs are reserved provisionally;
  - available resources in the peer CSPs are found based on different priorities;
  - available resources in the peer CSPs are reserved on the basis of different priorities.
- Resource set-up and activation should be confirmed as follows:
  - reserved resources in a peer CSP are established;
  - the configuration and policy settings of reserved resources in the peer CSPs are accessed.
- Cloud services switchover and switchback should be confirmed as follows:
  - the CSC's end-user is switched over access to a peer CSP without manual operation from the CSC, in order to allow the CSC's end user to use services in a similar manner to the way he/she did before the access was switchover;
  - the CSC's end-user access is switched back to the primary CSP when this CSP has recovered from the switchover
- Resource release should be confirmed as follows:
  - resources reserved, activated and/or set up in the peer CSPs are released by the CSP;
  - the peer CSP's resource configuration information are updated;
  - received cloud application data are erased and/or transferred back during the resource reservation.
- CSC information exchange should be confirmed as follows:
  - CSC information is activated only with the prior agreement of the CSC;
  - CSC profiles and associated information can be managed;
  - CSC profiles and associated information can be exchanged among multiple CSPs according to a pre-determined protocol and format, with the condition that the CSC is informed of and agrees to the exchange.
- Primary CSP role delegation should be confirmed as follows:
  - a CSP is activated only with the prior agreement of the CSC;
  - a CSP is able to discover peer CSPs that are capable of inheriting the primary CSP role, and to negotiate with these peer CSPs as to whether they can accept the inheritance;
  - a CSP is able to transfer its management information associated with the primary CSP role in a reliable manner to the peer CSPs that have accepted the permission transfer with that CSP;

  - the controllability of the information associated with the primary CSP role can be transferred to the secondary CSPs with minimum interruptions;
  - a CSP is able to cancel the permission transfer arrangements.
- Inter-cloud service handling should be confirmed as follows:
  - service intermediation is supported;
  - service aggregation is supported;
  - service arbitrage is supported.

A CSP can make use of one or more cloud services which are provided by other CSP. In every patterns of inter-cloud, there are two roles of CSP – primary CSP and secondary CSP. The provider making use of the services is termed a primary CSP while a provider whose services are being used is termed a secondary CSP. There are two types of relationship between a primary CSP and a secondary CSP:

- the use of secondary CSP's cloud services by a primary CSP;
- the use of secondary CSP's business and administration capabilities by the primary CSP's cloud service operations manager and CSP's cloud service manager to establish and control the use of the secondary CSP's cloud services.

Based on the reference architecture, the interworking involved in CSP-CSP relationship and corresponding test objectives can be identified as follows:

- interworking between primary CSP and CSC

  test objective is to verify that CSC can use cloud service, administer use of cloud service and perform business administration to the cloud services, in peering, federation or intermediary pattern;
- interworking between primary CSP's peer service integration component and secondary CSP

  test objective is to verify that primary CSP can connect to services of secondary CSP with appropriate security and with appropriate accounting for the usage;
- interworking between primary CSP's peer service management component and secondary CSP

  test objective is to verify that the primary CSP's operational support systems and business support systems can be connected to the administration capabilities and business capabilities of secondary CSP;
- interworking between CSPs to form and maintain inter-cloud pattern

  test objective is to verify that multiple CSP can interact to form and maintain the peering, federation or intermediary pattern.

8 Cloud computing interoperability testing between CSP and its management system

The interface of management system is used to interact with cloud services to provide supporting capabilities, such as monitoring and provisioning of cloud service. As described in [ITU-T Y.3502], management functional components are implemented in multi-layer functions in reference architecture. Interoperability testing is done to verify the following test objective:

- Operational support test

  Test objective is to verify that CSP can perform OSS related operation that required managing and controlling the cloud services offered to CSC, including runtime administration, monitoring, provisioning and maintenance.
- Business support test

  Test objective is to verify that CSP can provide a set of business-related management capabilities dealing with customers and supporting processes, including product catalogue, billing and financial management.

- Security test

  Test objective is to verify that security related controls can be applied to mitigate the threats in cloud computing environment, including authentication, authorization, auditing, validation, and encryption.

- Integration test

  Test objective is to verify that functional components can be connected to achieve the required functionality.

- Development support test

  Test objective is to verify that CSP can provide development support capabilities involving the creation, testing and life-cycle management of services and service components and support the cloud computing activities of the cloud service developer.

Appendix I

Cloud interoperability testing scenarios

(This appendix does not form an integral part of this Recommendation.)

ITU-T, ETSI and NIST have been considering wide technical areas related to cloud computing and also developing several use case documents which are generally recognised by cloud computing industry. Since the use case documents are like a framework document for cloud usage and involve wide technical areas, the documents shown below are useful reference documents in order to develop cloud interoperability testing specifications.

1) ITU-T Y.3500 series

[ITU-T Y.3501] – Cloud computing framework and high-level requirements

Appendix I – Use cases of cloud computing

[ITU-T Y.3511] – Framework of inter-cloud computing for network and infrastructure

Appendix I – Use cases from the inter-cloud perspective

Appendix II – Use cases from telecom and non-telecom providers' views

Appendix III – Abstract service offering models for inter-cloud computing

2) ETSI Cloud Standards Coordination Final Report (November 2013)

Section 3 – Use cases analysis (especially cloud bursting)

3) NIST cloud computing program technical efforts

NIST cloud computing test scenario use cases – Version 1

4) ODCA usage model for IaaS, PaaS, SaaS

ODCA has published many usage models:

ODCA SAAS_Interop_UM_Rev1.0 Software as service (SaaS) interoperability

ODCA PAAS_Interop_UM_Rev1.0 Platform as a service (PaaS) interoperability

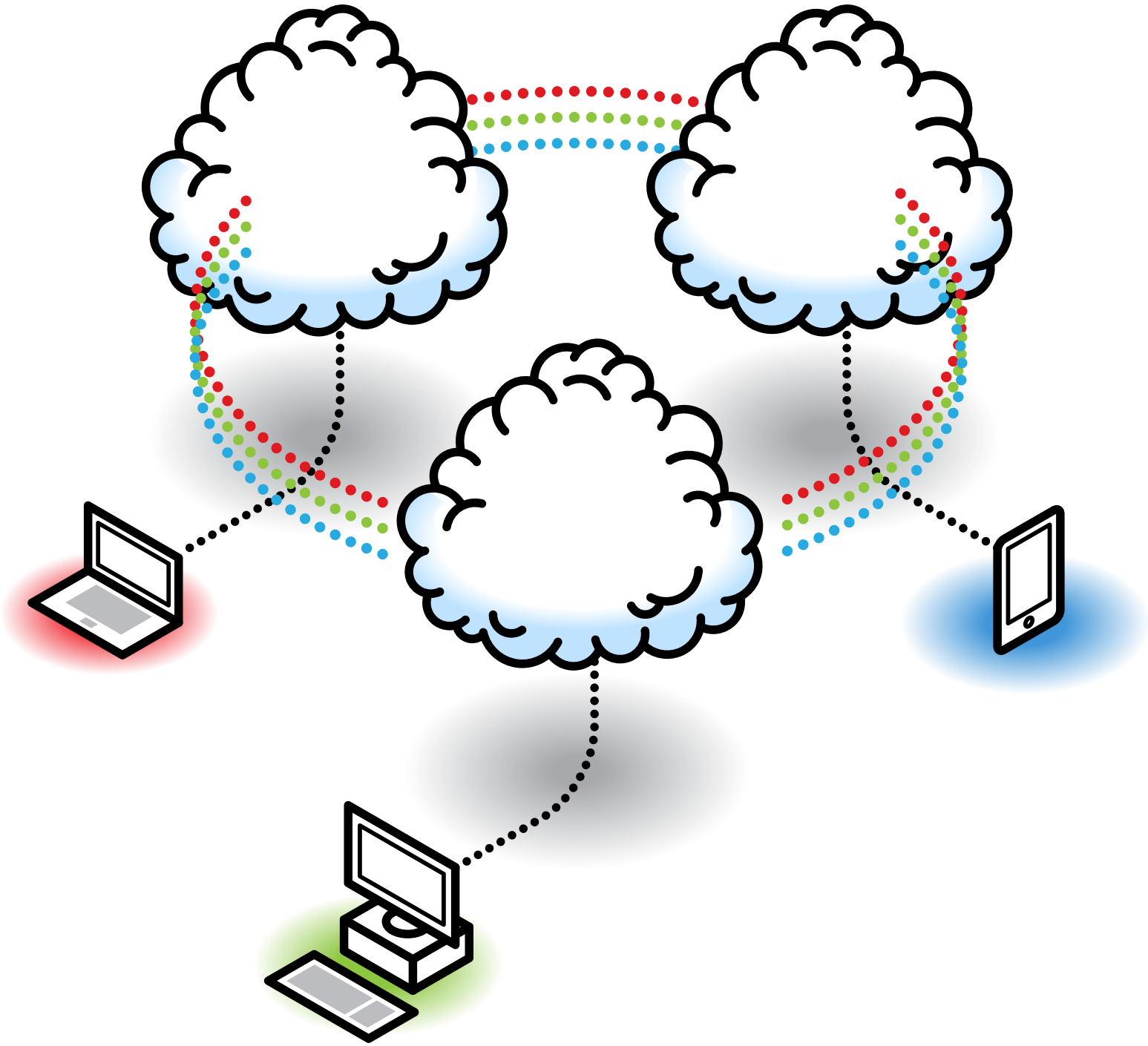
ODCA VM_Interoperability_in_a Hybrid_Cloud_Enviroment_rev1.2 Virtual machine (VM) Interoperability in a hybrid cloud environment

ODCA VM_Interop_PoC_White_Paper Implementing the Open Data Center Alliance Virtual Machine Interoperability Usage Model

NOTE – The detail contents are described in [b-ITU-T Q-Sup.65].

Bibliography

[b-ITU-T Q-Sup. 65] ITU-T Q-series Recommendations – Supplement 65 (2014), *Cloud computing interoperability activities*.



Cloud computing infrastructure capabilities interoperability testing – part 1: Interoperability testing between the CSC and CSP

Recommendation ITU-T Q.4040.1

(01/2018)

SERIES Q: SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

Summary

Recommendation ITU-T Q.4041.1 specifies the cloud computing infrastructure capabilities type interoperability testing between the CSC and CSP, including interoperability testing of computing services, storage services, network services and related management functions, based on the functional requirements specified in Recommendation ITU-T Y.3513. The test cases of cloud computing infrastructure capabilities type interoperability testing between the CSC and CSP have also been introduced.

Keywords

Cloud computing, infrastructure capabilities, interoperability testing.

Table of Contents

1 Scope

This Recommendation specifies the cloud computing infrastructure capabilities type interoperability testing between the CSC and CSP, including interoperability testing of computing services, storage services, network services and related management functions, based on the functional requirements specified in [ITU-T Y.3513].

The scope of this Recommendation consists of:

– Overview of cloud computing infrastructure capabilities type interoperability testing between the CSC and CSP;

– computing service interoperability testing between the CSC and CSP;

– storage service interoperability testing between the CSC and CSP;

– network service interoperability testing between the CSC and CSP.

NOTE – This Recommendation is the first part of cloud computing infrastructure capabilities type interoperability testing, which focuses on validating the infrastructure capabilities type functions provided by the CSP to the CSC. The second part focuses on validating the interaction between CSPs in the inter-cloud environment.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Q.4040] Recommendation ITU-T Q.4040 (2016), *The framework and overview of cloud computing interoperability testing.*

[ITU-T Y.101] Recommendation ITU-T Y.101 (2000), *Global Information Infrastructure terminology: Terms and definitions.*

[ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology –Cloud computing – Overview and vocabulary.*

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014) | ISO/IEC 17789:2014, *Information technology – Cloud computing – Reference architecture.*

[ITU-T Y.3513] Recommendation ITU-T Y.3513 (2014), *Cloud computing – Functional requirements of Infrastructure as a Service.*

[ISO/IEC 19941] ISO/IEC 19941 (2017), *Information technology – Cloud computing – Interoperability and portability.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 **activity** [ITU-T Y.3502]: A specified pursuit or set of tasks.

3.1.2 **cloud interoperability** [ITU-T Q.4040]: The capability to interact between CSCs and CSPs or between different CPSs, including the ability of CSCs to interact with cloud services and exchange information, the ability for one cloud service to work with other cloud services, and the ability for CSCs to interact with the cloud service management facilities of the CSPs.

3.1.3 cloud interoperability testing [ITU-T Q.4040]: Verifying functions and interaction that realize the cloud interoperability.

3.1.4 cloud service [ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.5 cloud service customer [ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

3.1.6 cloud service provider [ITU-T Y.3500]: Party which makes cloud services available.

3.1.7 cloud service user [ITU-T Y.3500]: Natural person, or entity acting on their behalf, associated with a cloud service customer that uses cloud services.

NOTE – Examples of such entities include devices and applications.

3.1.8 interoperability [ITU-T Y.101]: The ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged**.**

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CPU	Central Processing Unit
CSC	Cloud Service Customer
CSP	Cloud Service Provider
DHCP	Dynamic Host Configuration Protocol
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
IOPS	Input/Output operations Per Second
I/O	Input/Output
IP	Internet Protocol
LUN	Logical Unit Number
NAT	Network Address Translation
NIC	Network Interface Card
OVF	Open Virtualization Format
QCOW2	QEMU Copy On Write version 2
QEMU	Quick Emulator
QoS	Quality of Service
SLA	Service Level Agreement
SSH	Secure Shell
VLAN	Virtual Local Area Network
VM	Virtual Machine
VMDK	Virtual Machine Disk
VNC	Virtual Network Computing

5 Conventions

In this Recommendation, the keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

6 Overview of cloud computing infrastructure capabilities type interoperability testing between the CSC and CSP

Cloud interoperability is the ability of a CSC's system to interact with a cloud service, or the ability of one cloud service to interact with another cloud service, by exchanging information according to a prescribed method to obtain predictable results [ISO/IEC 19941]. The goal for cloud infrastructure capabilities type interoperability testing is to devise and implement testing methods and conduct a basic set of functional tests for infrastructure capabilities type interoperability in a hybrid cloud environment using both private and public clouds [ITU-T Q.4040].

The cloud computing infrastructure capabilities type interoperability testing can be divided into two parts; the first part focuses on validating the infrastructure capabilities type functions provided by the CSP to the CSC, and the second part focuses on validating the interaction between CSPs in the inter-cloud environment. The scope of this Recommendation is to validate the interaction between the CSC and CSP with infrastructure capabilities.

Infrastructure as a Service (IaaS) provides computing service functions, storage service functions and network service functions to the CSC [ITU-T Y.3513]. All the functional requirements specified in [ITU-T Y.3513] should be validated. It is recommended to consider the following for cloud computing infrastructure capabilities type interoperability testing:

- Computing service interoperability testing between the CSC and CSP
  - It is recommended to verify that the CSP provides a computing service to the CSC, including virtual machine (VM) configuration, VM migration, VM snapshot, VM clone, VM time synchronization, VM reservation, VM image, VM template, VM scaling and VM backup.
  - It is recommended to verify that the CSP provides computing service related management functions to the CSC, including life cycle management of the VM and physical machine, and VM and physical machine configuration inquiring.
- Storage service interoperability testing between the CSC and CSP
  - It is recommended to verify that the CSP provides a storage service to the CSC, including storage migration, storage snapshot, storage backup, storage resource reservation and I/O performance.
  - It is recommended to verify that the CSP provides storage service related management functions to the CSC, including storage life cycle management, storage utilization status inquiring.
- Network service interoperability testing between the CSC and CSP
  - It is recommended to verify that the CSP provides network service to the CSC, including network policy migration, network QoS, network address translation (NAT), network isolation, IP address allocation, IP address reservation, load balance, firewall and multipath routing.
  - It is recommended to verify that the CSP provides network service related management function to the CSC, including network information inquiring.

This Recommendation describes cloud computing infrastructure capabilities type interoperability testing from the functional perspective without distinguish five facets (transport, syntactic, semantic data, behavioural and policy) which were defines by [ISO/IEC 19941]. However, all the considerations described in [ISO/IEC 19941] are taking into account for better understanding of the cloud computing infrastructure capabilities type interoperability testing.

7 Computing service interoperability testing between the CSC and CSP

Computing service interoperability testing between the CSC and CSP valuates the interaction between the CSC and CSP for computing service and related management functions, which include VM configuration, VM migration, VM snapshot, VM clone, VM time synchronization, VM reservation, VM image, VM template, VM scaling, VM backup, life cycle management of the VM and physical machine, and VM and physical machine configuration inquiring. For a description of related functional requirements refer to [ITU-T Y.3513].

7.1 Interoperability testing of VM configuration between the CSC and CSP

The test object of VM configuration is to verify that the CSC configures the VM with processors, hard disks, memory and NIC parameters. The test case of VM configuration can be found in Appendix II.1.1.

7.2 Interoperability testing of VM migration between the CSC and CSP

The test object of VM migration is to verify that the CSC migrates the VM from a particular host to another host. The test case of VM migration can be found in Appendix II.1.2.

7.3 Interoperability testing of VM snapshot between the CSC and CSP

The test object of VM snapshot is to verify that the CSC captures the state (VM memory, settings, and virtual disks) of the VM by taking snapshots of it and rolling back to the previous VM state when needed. The test case of VM snapshot can be found in Appendix II.1.3.

7.4 Interoperability testing of VM clone between the CSC and CSP

The test object of VM clone is to verify that the CSC clones a particular VM and the cloned VM has identical configuration and CSP/CSC data as the original one. The test case of VM clone can be found in Appendix II.1.4.

7.5 Interoperability testing of VM time synchronization between the CSC and CSP

The test object of VM time synchronization is to verify that the CSC sets VM time synchronization manually or automatically. The test case of VM time synchronization can be found in Appendix II.1.5.

7.6 Interoperability testing of VM reservation between the CSC and CSP

The test object of VM reservation is to verify that the CSC reserves available computing resources (CPU, memory) for particular VM before it is initiated. The test case of VM reservation can be found in Appendix II.1.6.

7.7 Interoperability testing of VM image between the CSC and CSP

The test object of VM image is to verify that the CSC creates a new VM by VM image, which consists of infrastructure configuration and CSP data, CSC data or both. The test case of VM image can be found in Appendix II.1.7.

7.8 Interoperability testing of VM template between the CSC and CSP

The test object of VM template is to verify that the CSC creates VMs by VM template, including the open virtualization format (OVF). The test case of VM template can be found in Appendix II.1.8.

7.9 Interoperability testing of VM scaling between the CSC and CSP

The test object of VM scaling is to verify that the CSC changes the scale of VMs dynamically based on the scaling policies and monitored events of the VM; this includes configuration change (e.g., CPU, memory, network bandwidth increased or decreased) and components change (new VM added or removed). The test case of VM scaling can be found in Appendix II.1.9.

7.10 Interoperability testing of VM backup between the CSC and CSP

The test object of VM backup is to verify that the CSC obtains the configuration and data of a particular VM by making a backup and restoring the VM. The test case of VM backup can be found in Appendix II.1.10.

7.11 Interoperability testing of VM life cycle management between the CSC and CSP

The test object of VM life cycle management is to verify that the CSC manages the VM with various operations including start, shutdown, restart, suspend and resume VM. The test case of VM life cycle management can be found in Appendix II.1.11.

7.12 Interoperability testing of physical machine life cycle management between the CSC and CSP

The test object of physical machine life cycle management is to verify that the CSC manages the physical machine with various operations including start, shutdown, hibernate and wake-up. The test case of physical machine life cycle management can be found in Appendix II.1.12.

7.13 Interoperability testing of VM configuration inquiring between the CSC and CSP

The test object of VM configuration inquiring is to verify that the CSC inquires VM configuration with the CPU number, memory allocated, NIC number and IP address allocated. The test case of VM configuration inquiring can be found in Appendix II.1.13.

7.14 Interoperability testing of physical machine configuration inquiring between the CSC and CSP

The test object of physical machine configuration inquiring is to verify that the CSC inquires physical machine configuration with the number of CPU cores, memory size, disk size and NIC number. The test case of physical machine configuration inquiring can be found in Appendix II.1.14.

8 Storage service interoperability testing between the CSC and CSP

Storage service interoperability testing between the CSC and CSP valuates the interaction between the CSC and CSP for storage service and related management functions; these include storage migration, storage snapshot, storage backup, storage resource reservation, I/O performance, storage life cycle management and storage utilization status inquiring. For a description of related functional requirements refer to [ITU-T Y.3513].

8.1 Interoperability testing of storage migration between the CSC and CSP

The test object of storage migration is to verify that the CSC migrates data of the VM to different storage media without any loss. The test case of storage migration can be found in Appendix II.2.1.

8.2 Interoperability testing of storage snapshot between the CSC and CSP

The test object of storage snapshot is to verify that the CSC preserves and recovers the state and data of storage. The test case of storage snapshot can be found in Appendix II.2.2.

8.3 Interoperability testing of storage backup between the CSC and CSP

The test object of storage backup is to verify that the CSC backs up and restores data when faulty or data loss occurs. The test case of storage backup can be found in Appendix II.2.3.

8.4 Interoperability testing of storage resource reservation between the CSC and CSP

The test object of storage resource reservation is to verify that the CSC reserves available storage resources (e.g., storage space and LUN) for the VM. The test case of storage resource reservation can be found in Appendix II.2.4.

8.5 Interoperability testing of I/O performance between the CSC and CSP

The test object of I/O performance is to verify that the CSC constrains the I/O traffic of a particular VM with a specified level. The test case of I/O performance can be found in Appendix II.2.5.

8.6 Interoperability testing of storage life cycle management between the CSC and CSP

The test object of storage life cycle management is to verify that the CSC manages storage with various operations including create, attach, detach, query and delete storage. The test case of storage life cycle management can be found in Appendix II.2.6.

8.7 Interoperability testing of storage utilization status inquiring between the CSC and CSP

The test object of storage utilization status inquiring is to verify that the CSC inquires storage utilization status information including used space and unused space of storage. The test case of storage utilization status inquiring can be found in Appendix II.2.7.

9 Network service interoperability testing between the CSC and CSP

Network service interoperability testing between the CSC and CSP valuates the interaction between the CSC and CSP for network service and related management functions, which include network policy migration, network QoS, network address translation, network isolation, IP address allocation, IP address reservation, load balance, firewall, multipath routing and network information inquiring. For a description of related functional requirements refer to [ITU-T Y.3513].

9.1 Interoperability testing of network policy migration between the CSC and CSP

The test object of network policy migration is to verify that the CSC migrates the VM while the network policy (generally includes access control list, bandwidth limitation and priority policy) is consistent before and after VM migration. The test case of network policy migration can be found in Appendix II.3.1.

9.2 Interoperability testing of network QoS between the CSC and CSP

The test object of network QoS is to verify that the CSC configures network QoS for the VM, including bandwidth limitation, bandwidth reservation, traffic shaping, traffic classification and congestion avoidance. The test case of network QoS can be found in Appendix II.3.2.

9.3 Interoperability testing of network address translation between the CSC and CSP

The test object of network address translation is to verify that the CSC configures the mapping between an internal IP address and external IP address of a specific VM. The test case of network address translation can be found in Appendix II.3.3.

9.4 Interoperability testing of network isolation between the CSC and CSP

The test object of network isolation is to verify that the CSC's tenant network is isolated even though the network address is overlapped with another tenants' network. The test case of network isolation can be found in Appendix II.3.4.

9.5 Interoperability testing of IP address allocation between the CSC and CSP

The test object of IP address allocation is to verify that the CSC allocates an IP address to the VM statically or dynamically. The test case of IP address allocation can be found in Appendix II.3.5.

9.6 Interoperability testing of IP address reservation between the CSC and CSP

The test object of IP address reservation is to verify that the CSC reserves an IP address or a range of IP-addresses for specific VM(s). The test case of IP address reservation can be found in Appendix II.3.6.

9.7 Interoperability testing of load balance between the CSC and CSP

The test object of load balance is to verify that the CSC deploys a load balance mechanism for multiple VMs in order to achieve scalability and fault tolerance of an application. The test case of load balance can be found in Appendix II.3.7.

9.8 Interoperability testing of firewall between the CSC and CSP

The test object of firewall is to verify that the CSC monitors and controls incoming and outgoing VM traffic based on predetermined security rules. The test case of firewall can be found in Appendix II.3.8.

9.9 Interoperability testing of multipath routing between the CSC and CSP

The test object of multipath routing is to verify that the CSC accesses cloud services through multiple network paths. The test case of multipath routing can be found in Appendix II.3.9.

9.10 Interoperability testing of network information inquiring between the CSC and CSP

The test object of network information inquiring is to verify that the CSC inquires network information from the CSP with network device(s) specification, network traffic performance (in terms of throughput, jitter, loss, delay) and network topology. The test case of network address inquiring can be found in Appendix II.3.10.

Appendix I

Test case template

(This appendix does not form an integral part of this Recommendation.)

Table I.1 provides a test case template to describe cloud computing infrastructure capability type interoperability testing between the CSC and CSP. The test case template is designed with reference to relevant technical specifications. As shown in the table, an interoperability test case consists of test purpose, reference, test sequence and test verdict.

– Test purpose is a statement that specifies which test case to verify.

– Reference of the test case provides list of references to the base specification clause(s), use case(s), requirement(s), etc. which are either used in the test or define the functionality being tested.

– The test sequences provide the steps required to perform the test. There are two types of test step. A stimulus corresponds to an event that triggers a specific action on the object under test. There is no need to provide result for a stimulus step. A check consists of observing that the object under test behaves as described. A result must be provided for every check step. If the object under test behaves as described in the description of the check step, the result should be recorded as OK, otherwise the result should be recorded as fail.

– For every test case, test verdict should be provided to indicate whether the test is passed.

Table I.1 – Test case template

Interoperability test description				
Test purpose		A concise summary of the test reflecting its purpose and allowing readers to easily distinguish this test from any other test in the document.		
Reference		List of references to the base specification clause(s), use case(s), requirement(s), etc., which are either used in the test or define the functionality being tested.		
Test sequences	Step	Type	Description	Result
	1	Stimulus	A stimulus corresponds to an event that triggers a specific action on the object under test. There is no need to provide 'Result' for a stimulus step.	There is no need to provide 'Result' for a stimulus step.
	2	Check	A check consists of observing that the object under test behaves as described. A result must be provided for every check step. If the object under test behaves as described in the description of the check step, the result should be recorded as OK, otherwise the result should be recorded as fail.	A result must be provided for every check step.
Test verdict	It is deemed as successfully terminated if all/or one check(s) is (are) successful, otherwise it is deemed as failed.			

Appendix II

Test cases for cloud computing infrastructure capabilities interoperability testing between the CSC and CSP

(This appendix does not form an integral part of this Recommendation.)

II.1 Test cases for computing service interoperability testing between the CSC and CSP

II.1.1 Test case: VM configuration

Table II.1 – Test case: VM configuration

VM configuration test description				
Test purpose		To verify that the CSC configures the VM with processors, hard disks, memory and NIC parameters.		
Reference		[ITU-T Y.3513] clause 7.1.2		
Test sequence	Step	Type	Description	Result
	1	Stimulus	The CSC configures the processor parameters of the VM, in the permissible range of physical resources conditions.	
	2	Check	Processor parameters configuration is in effect. The processor of the VM is consistent with the parameters specified in step 1.	
	3	Stimulus	The CSC configures the hard disk parameters of the VM, in the permissible range of physical resources conditions.	
	4	Check	Hard disk parameters configuration is in effect. The hard disks of the VM are consistent with the parameters specified in step 3.	
	5	Stimulus	The CSC configures the NIC parameters of the VM, in the permissible range of physical resources conditions.	
	6	Check	NIC parameters configuration is in effect. The NIC of the VM is consistent with parameters specified in step 5.	
Test verdict	It is deemed as successfully terminated if all the checks are successful, otherwise it is deemed as failed.			

II.1.2 Test case: VM migration

Table II.2 shows the test case for VM migration.

Table II.2 – Test case: VM migration

VM migration test description				
Test purpose	To verify that the CSC migrates the VM from a particular host to another host.			
Reference	[ITU-T Y.3513] clause 7.1.3			
	Step	Type	Description	Result
	1	Stimulus	The CSC migrates the VM in power off state to another host.	
	2	Stimulus	The CSC starts the VM.	
	3	Check	The VM is running on the target host without any changes.	
	4	Stimulus	The CSC migrates the running VM to another host.	
	5	Check	The VM is running on the target host without any changes; the service carried by the VM is still on during the migration.	
Test verdict	It is deemed as successfully terminated if at least one check is successful, otherwise it is deemed as failed.			

II.1.3 Test case: VM snapshot

Table II.3 shows the test case for VM snapshot.

Table II.3 – Test case: VM snapshot

VM snapshot test description				
Test purpose	To verify that the CSC captures the state (VM memory, settings and virtual disks) of the VM by taking snapshots and rolling back to the previous VM state when needed.			
Reference	[ITU-T Y.3513] clause 7.1.5			
Test sequence	Step	Type	Description	Result
	1	Stimulus	The CSC uses an application running on a VM.	
	2	Stimulus	The CSC takes a snapshot (with memory state) of the VM, called snapshot A.	
	3	Stimulus	The CSC makes some changes to the application and closes it, and reconfigures the VM.	
	4	Stimulus	The CSC takes another snapshot (with memory state) of the VM, called snapshot B.	
	5	Stimulus	The CSC restores snapshot A.	
	6	Check	The VM's virtual disk, configurations and memory state are consistent with the state when snapshot A was taken. The application is running on the VM without any changes.	
	7	Stimulus	The CSC deletes snapshot A and restores snapshot B.	
	8	Check	The VM's virtual disk, configurations and memory state are consistent with the state when snapshot B was taken. The application is not running on the VM.	
Test verdict	It is deemed as successfully terminated if all the checks are successful, otherwise it is deemed as failed.			

II.1.4 Test case: VM clone

Table II.4 shows the test case for VM clone.

Table II.4 – Test case: VM clone

VM clone test description				
Test purpose		To verify that the CSC clones a particular VM and the cloned VM has identical configuration and CSP/CSC data as the original one.		
Reference		[ITU-T Y.3513] clause 7.1.6		
Test sequence	Step	Type	Description	Result
	1	Stimulus	The CSC clones VM A, called VM A-1.	
	2	Stimulus	The CSC starts VM A.	
	3	Stimulus	The CSC starts VM A-1.	
	4	Check	VM A and VM A-1 can run independently without affecting each other.	
	5	Check	Configuration and CSP/CSC data of VM A-1 is consistent with VM A.	
Test verdict	It is deemed as successfully terminated if all the checks are successful, otherwise it is deemed as failed.			

II.1.5 Test case: VM time synchronization

Table II.5 shows the test case for VM time synchronization.

Table II.5 – Test case: VM time synchronization

VM time synchronization test description				
Test purpose		To verify that the CSC sets VM time synchronization manually or automatically.		
Reference		[ITU-T Y.3513] clause 7.1.8		
Test sequence	Step	Type	Description	Result
	1	Stimulus	The CSC synchronizes the VM A system time to a specified time manually.	
	2	Check	The system time of VM A is consistent with the specified time in step 1.	
	3	Stimulus	The CSC configures the synchronization of VM A's time along with that of the host automatically.	
	4	Stimulus	The CSC logs in VM A and adjusts the system time to a different time.	
	5	Check	The system time of VM A is synchronized with the host that the VM is running on.	
Test verdict	It is deemed as successfully terminated if all the checks are successful, otherwise it is deemed as failed.			

II.1.6 Test case: VM reservation

Table II.6 shows the test case for VM reservation.

Table II.6 – Test case: VM reservation

VM reservation test description				
Test purpose		To verify that the CSC reserves available computing resources (CPU, memory) for a particular VM before it is initiated.		
Reference		[ITU-T Y.3513] clause 7.1.9		
Test sequence	Step	Type	Description	Result
	1	Stimulus	The CSC configures VM reservation, which includes the configuration of guaranteed minimum allocation of CPU and memory for a specified VM, called VM A.	
	2	Stimulus	The CSC runs an application to perform heavy consumption of CPU and memory on other VMs hosted in the same host except for VM A. Consumption of CPU and memory is close to the amount of the host computing resource.	
	3	Stimulus	The CSC performs heavy consumption of CPU and memory on VM A.	
	4	Check	CPU and memory resources reserved for VM A are not occupied by other VMs.	
Test verdict	It is deemed as successfully terminated if all the checks are successful, otherwise it is deemed as failed.			

II.1.7 Test case: VM image

Table II.7 shows the test case for VM image.

Table II.7 – Test case: VM image

VM image test description				
Test purpose		To verify that the CSC creates a new VM by VM image, which consists of infrastructure configuration and CSP data, CSC data or both.		
Reference		[ITU-T Y.3513] clause 7.1.10		
Test sequence	Step	Type	Description	Result
	1	Stimulus	The CSC creates an image, called image A. Image A is converted from existing VM1.	
	2	Stimulus	The CSC creates a VM based on image A.	
	3	Check	New VM (VM2) can be created based on image A. The configuration, CSP data and CSC data of new VMs are consistent with VM1.	
	4	Stimulus	The CSC exports image A as exported image in different supporting format, such as QCOW2, VMDK, etc.	
	5	Stimulus	The CSC imports the exported image as image B.	
	6	Stimulus	The CSC creates a VM based on image B.	
	7	Check	A new VM can be created based on image B. The configuration, CSP data and CSC data of new VMs created based on the VM image are consistent with the VM image.	
	8	Stimulus	The CSC updates image B by modifying the name of the image.	
	9	Check	The name of the image changes to a specified name.	
	10	Stimulus	The CSC deletes image B.	
	11	Check	The VMs created which are based on image B still exist.	
Test verdict	It is deemed as successfully terminated if all the checks are successful, otherwise it is deemed as failed.			

II.1.8 Test case: VM template

Table II.8 shows the test case for VM template.

Table II.8 – Test case: VM template

VM template test description				
Test purpose		To verify that the CSC creates VMs by VM template, including open virtualization format (OVF).		
Reference		[ITU-T Y.3513] clause 7.1.11		
Test sequence	Step	Type	Description	Result
	1	Stimulus	The CSC creates a VM template by exporting a VM as VM template in OVF format.	
	2	Check	The exported VM template conforms to the format of OVF.	
	3	Stimulus	The CSC imports the VM template to create a new VM.	
	4	Check	The configuration and data of the new VM created in step 3 are consistent with the VM template.	
	5	Stimulus	The CSC updates the VM template by modifying the VM template's name.	
	6	Check	The name of VM template changes to a specified name.	
	7	Stimulus	The CSC deletes the VM template.	
	8	Check	The VM created which is based on the VM template still exists.	
Test verdict	It is deemed as successfully terminated if all the checks are successful, otherwise it is deemed as failed.			

II.1.9 Test case: VM scaling

Table II.9 shows the test case for VM scaling.

Table II.9 – Test case: VM scaling

VM scaling test description				
Test purpose		To verify that the CSC changes the scale of VMs dynamically based on the scaling policies and monitored events of the VM; this includes configuration change (e.g., CPU, memory, network bandwidth increased or decreased) and components change (new VM added or removed).		
Reference		[ITU-T Y.3513] clause 7.1.4		
Test sequence	Step	Type	Description	Result
	1	Stimulus	The CSC configures VM A; checks the VM status, such as CPU, memory resources allocation and its components.	
	2	Stimulus	The CSC configures the configuration change based scaling policy that when memory consumed is more than 90%, it allocates twice the memory for VM A automatically.	
	3	Stimulus	The CSC runs an application on VM A to perform more than 90% consumption of memory on VM A to trigger auto-scaling.	
	4	Check	VM A is allocated with twice as much memory as before.	
	5	Stimulus	The CSC configures the components change based scaling policy that when the CPU has consumed more than 90%, add a new VM with the same resource configuration as VM A automatically.	

Table II.9 – Test case: VM scaling

VM scaling test description				
	6	Stimulus	The CSC runs an application on VM A to perform more than 90% consumption of CPU on VM A to trigger auto-scaling.	
	7	Check	A new VM with the same resource configuration as VM A is added.	
	8	Stimulus	The CSC configures the configuration change based scaling policy that when memory consumed is less than 10%, reduce memory allocation by half for VM A automatically.	
	9	Check	The CSC performs low(less than 10%) consumption of memory on VM A to trigger auto-scaling.	
	10	Stimulus	Memory allocation for VM A is reduced by half.	
	11	Check	The CSC configures the components change based scaling policy that when the CPU consumed less than 10%, remove a VM automatically.	
	12	Stimulus	The CSC performs low(less than 10%) consumption of CPU on VM A to trigger auto-scaling.	
	13	Check	VM A is terminated.	
	14	Stimulus	The CSC configures events monitoring based components change for VM A that when VM A is suspended, add a new VM with the same resource configuration as VM A automatically.	
	15	Stimulus	The CSC suspends VM A.	
	16	Check	A new VM with the same resource configuration as VM A is added.	
Test verdict	It is deemed as successfully terminated if all the checks are successful, otherwise it is deemed as failed.			

II.1.10 Test case: VM backup

Table II.10 shows the test case for VM backup.

Table II.10 – Test case: VM backup

VM backup test description				
Test purpose	To verify that the CSC obtains the configuration and data of a particular VM by making a backup and restoring the VM.			
Reference	[ITU-T Y.3513] clause 7.1.7			
Test sequence	Step	Type	Description	Result
	1	Stimulus	The CSC makes a backup of VM A, called backup A.	
	2	Stimulus	The CSC changes the configuration and data of VM A.	
	3	Stimulus	The CSC restores VM A with backup A.	
	4	Check	Configuration and data of VM A is consistent with the state when backup A was taken.	
Test verdict	It is deemed as successfully terminated if all the checks are successful, otherwise it is deemed as failed.			

II.1.11 Test case: VM life cycle management

Table II.11 shows the test case for VM life cycle management.

Table II.11 – Test case: VM life cycle management

VM life cycle management test description				
Test purpose		To verify that the CSC manages the VM with various operations including start, shutdown, restart, suspend and resume VM.		
Reference		[ITU-T Y.3513] clause 7.1.2		
Test sequence	Step	Type	Description	Result
	1	Stimulus	The CSC shuts down a VM which has its power on.	
	2	Check	The state of the VM is power off.	
	3	Stimulus	The CSC starts the VM.	
	4	Check	The state of the VM is power on.	
	5	Stimulus	The CSC restarts the VM.	
	6	Check	The state of the VM is power on.	
	7	Stimulus	The CSC suspends the VM, tries to log in VM's operating system through SSH, VNC or other tools provided by the CSP.	
	8	Check	The state of the VM is suspended and VM's activity is paused. The CSC cannot log in the VM's operating system through SSH, VNC or other tools.	
	9	Stimulus	The CSC resumes the VM, then checks the power states of the VM, tries to log in VM's operating system through SSH, VNC or other tools provided by the CSP.	
	10	Check	The state of the VM is power on and the VM's activity is consistent with the moment before suspend operation.	
Test verdict	It is deemed as successfully terminated if all the checks are successful, otherwise it is deemed as failed.			

II.1.12 Test case: physical machine life cycle management

Table II.12 shows the test case for physical machine life cycle management.

Table II.12 – Test case: physical machine life cycle management

Physical machine life cycle management test description				
Test purpose		To verify that the CSC manages a physical machine with various operations including start, shutdown, hibernate and wakeup.		
Reference		[ITU-T Y.3513] clause 7.1.1		
Test sequence	Step	Type	Description	Result
	1	Stimulus	The CSC shuts down a physical machine which has its power on.	
	2	Check	The state of the physical machine is power off.	
	3	Stimulus	The CSC starts the physical machine.	
	4	Check	The state of the physical machine is power on.	
	5	Stimulus	The CSC hibernates a physical machine which is in power on state.	
	6	Check	The state of the physical machine is hibernate.	

Table II.12 – Test case: physical machine life cycle management

Physical machine life cycle management test description				
	7	Stimulus	The CSC wakes up the physical machine which is in hibernate state.	
	8	Check	The state of the physical machine is power on.	
Test verdict	It is deemed as successfully terminated if all the checks are successful, otherwise it is deemed as failed.			

II.1.13 Test case: VM configuration inquiring

Table II.13 shows the test case for VM configuration inquiring.

Table II.13 – Test case: VM configuration inquiring

VM configuration inquiring test description				
Test purpose	To verify that the CSC inquires VM configuration with CPU number, memory allocated, NIC number, IP address allocated.			
Reference	[ITU-T Y.3513] clause 7.1.2			
Test sequence	Step	Type	Description	Result
	1	Stimulus	The CSC queries the CPU number of the VM.	
	2	Check	The CSC receives the information of a particular VM's CPU number that is consistent with the number of the CPU allocated for the VM.	
	3	Stimulus	The CSC queries memory size of the VM from the CSP.	
	4	Check	The CSC receives the information of a particular VM's memory size that is consistent with the size of memory allocated for the VM.	
	5	Stimulus	The CSC queries the NIC number of the VM from the CSP.	
	6	Check	The CSC receives the information of a particular VM's NIC number that is consistent with the number of the NIC allocated for the VM.	
	7	Stimulus	The CSC queries the IP address of the VM from the CSP.	
	8	Check	The CSC receives the information of a particular VM's IP address that is consistent with the IP address allocated for the VM.	
Test verdict	It is deemed as successfully terminated if all the checks are successful, otherwise it is deemed as failed.			

II.1.14 Test case: physical machine configuration inquiring

Table II.14 shows the test case for physical machine status inquiring.

Table II.14 – Test case: physical machine status inquiring

Physical machine configuration inquiring test description	
Test purpose	To verify that the CSC inquires physical machine configuration with the number of CPU cores, memory size, disk size and NIC number.
Reference	[ITU-T Y.3513] clause 7.1.1

Table II.14 – Test case: physical machine status inquiring

Physical machine configuration inquiring test description				
Test sequence	Step	Type	Description	Result
	1	Stimulus	The CSC queries the CPU's cores number of the physical machine from the CSP.	
	2	Check	The CSC receives the information of a particular physical machine's CPU cores number that is consistent with the CPU cores number of the physical machine.	
	3	Stimulus	The CSC queries memory size of the physical machine from the CSP.	
	4	Check	The CSC receives the information of a particular physical machine's memory size that is consistent with the memory size of the physical machine.	
	5	Stimulus	The CSC queries the disk size of the physical machine from the CSP.	
	6	Check	The CSC receives the information of a particular physical machine's disk size that is consistent with the disk size of the physical machine.	
	7	Stimulus	The CSC queries The NIC number of the physical machine from the CSP.	
	8	Check	The CSC receives the information of a particular physical machine's NIC number that is consistent with the NIC number of the physical machine.	
Test verdict	It is deemed as successfully terminated if all the checks are successful, otherwise it is deemed as failed.			

II.2 Test cases for storage service interoperability testing between the CSC and CSP

II.2.1 Test case: storage migration

Table II.15 shows the test case for storage migration.

Table II.15 – Test case: storage migration

Storage migration test description				
Test purpose	To verify that the CSC migrates data of the VM to different storage media without any loss.			
Reference	[ITU-T Y.3513] clause 7.2.1			
Test sequence	Step	Type	Description	Result
	1	Stimulus	The CSC migrates the VM's data from local storage to shared storage.	
	2	Check	The VM uses the shared storage after migration is done without affecting the service running on the VM.	
	3	Stimulus	The CSC migrates the VM's data from shared storage to local storage.	
	4	Check	The VM uses the local storage after migration is done without affect the service running on the VM.	
Test verdict	It is deemed as successfully terminated if all the checks are successful, otherwise it is deemed as failed.			

II.2.2 Test case: storage snapshot

Table II.16 shows the test case for storage snapshot.

Table II.16 – Test case: Storage snapshot

Storage snapshot test description				
Test purpose		To verify that the CSC preserves and recovers the state and data of storage.		
Reference		[ITU-T Y.3513] clause 7.2.2		
Test sequence	Step	Type	Description	Result
	1	Stimulus	The CSC takes a storage snapshot of storage A, called snapshot A.	
	2	Stimulus	The CSC changes the data of storage A.	
	3	Stimulus	The CSC takes another storage snapshot of storage A, called snapshot B.	
	4	Stimulus	The CSC restores snapshot A.	
	5	Check	Storage A's state and data are consistent with the states when snapshot A was taken.	
	6	Stimulus	The CSC deletes snapshot A.	
	7	Check	Snapshot A can be deleted without affecting snapshot B.	
	8	Stimulus	The CSC restores snapshot B.	
	9	Check	Storage A's state and data are consistent with the states when snapshot B was taken.	
Test verdict	It is deemed as successfully terminated if all the checks are successful, otherwise it is deemed as failed.			

II.2.3 Test case: storage backup

Table II.17 shows the test case for storage backup.

Table II.17 – Test case: storage backup

Storage backup test description				
Test purpose		To verify that the CSC backs up and restores data when faulty or data loss occurs.		
Reference		[ITU-T Y.3513] clause 7.2.3		
Test sequence	Step	Type	Description	Result
	1	Stimulus	The CSC takes a storage backup of storage A, called backup storage A.	
	2	Stimulus	The CSC changes the data in the storage A.	
	3	Stimulus	The CSC restores storage A with storage backup A.	
	4	Check	Configuration and data of backup storage A is consistent with storage A.	
Test verdict	It is deemed as successfully terminated if all the checks are successful, otherwise it is deemed as failed.			

II.2.4 Test case: storage resource reservation

Table II.18 shows the test case for storage resource reservation.

Table II.18 – Test case: storage resource reservation

Storage resource reservation test description				
Test purpose		To verify that the CSC reserves available storage resource (e.g., storage space and LUN) for the VM.		
Reference		[ITU-T Y.3513] clause 7.2.5		
Test sequence	Step	Type	Description	Result
	1	Stimulus	The CSC configures storage reservation for VM A, which has guaranteed minimum allocation of storage space.	
	2	Stimulus	The CSC runs an application to perform heavy consumption of storage usage on VMs hosting in the same host except for VM A. The total consumption of storage is close to the amount of the storage available for the host.	
	3	Stimulus	The CSC performs heavy consumption of storage usage on VM A.	
	4	Check	VM A can get the storage resource.	
Test verdict	It is deemed as successfully terminated if all the checks are successful, otherwise it is deemed as failed.			

II.2.5 Test case: I/O performance

Table II.19 shows the test case for I/O performance.

Table II.19 – Test case: I/O performance

I/O performance test description				
Test purpose		To verify that the CSC constrains I/O traffic of a particular VM with a specified level.		
Reference		[ITU-T Y.3513] clause 7.2.4		
Test sequence	Step	Type	Description	Result
	1	Stimulus	The CSC runs an application to perform heavy reading and writing of storage on VM A. It records the actual IOPS obtained by VM A.	
	2	Stimulus	The CSC configures I/O performance limitation for VM A. The IOPS limit configured is significantly lower than the IOPS obtained in step 1.	
	3	Stimulus	The CSC runs an application to perform heavy reading and writing on VM A.	
	4	Check	The actual IOPS obtained by VM A does not exceed the limitation.	
Test verdict	It is deemed as successfully terminated if all the checks are successful, otherwise it is deemed as failed.			

II.2.6 Test case: storage life cycle management

Table II.20 shows the test case for storage life cycle management.

Table II.20 – Test case: Storage life cycle management

Storage life cycle management test description				
Test purpose		To verify that the CSC manages storage with various operations including create, attach, detach, query and delete storage.		
Reference		[ITU-T Y.3513] clause 7.2		
Test sequence	Step	Type	Description	Result
	1	Stimulus	The CSC creates storage space called storage A with different types, such as block level, file-system level and object-based storage according to a service level agreement (SLA).	
	2	Check	The created storage A is accessible to the CSC.	
	3	Stimulus	The CSC attaches storage A to VM A.	
	4	Check	The VM can use storage A.	
	5	Stimulus	The CSC detaches storage A from VM A.	
	6	Check	VM A cannot use storage A anymore but storage A could be used for other VMs.	
	7	Stimulus	Deletes storage A.	
	8	Check	Storage A cannot be used.	
Test verdict	It is deemed as successfully terminated if all the checks are successful, otherwise it is deemed as failed.			

II.2.7 Test case: storage utilization status inquiring

Table II.21 shows the test case for storage utilization status inquiring.

Table II.21 – Test case: Storage utilization status inquiring

Storage utilization status inquiring test description				
Test purpose		To verify that the CSC inquires storage utilization status information including used space and unused space of storage.		
Reference		[ITU-T Y.3513] clause 7.2		
Test sequence	Step	Type	Description	Result
	1	Stimulus	The CSC queries utilization status of storage, including used space and unused space of storage.	
	2	Check	The CSC receives the information of a particular storage's used space and unused space that is consistent with the actual utilization status of the storage.	
Test verdict	It is deemed as successfully terminated if all the checks are successful, otherwise it is deemed as failed.			

II.3 Test cases for network service interoperability testing between the CSC and CSP

II.3.1 Test case: network policy migration

Table II.22 shows the test case for network policy migration.

Table II.22 – Test case: network policy migration

Network policy migration test description				
Test purpose		To verify that the CSC migrates the VM while the network policy (generally includes access control list, bandwidth limitation and priority policy) is consistent before and after VM migration.		
Reference		[ITU-T Y.3513] clause 7.3.1		
Test sequence	Step	Type	Description	Result
	1	Stimulus	The CSC configures the network policy for VM A, including configuring the access control list, bandwidth limitation and priority policy for VM A.	
	2	Stimulus	The CSC migrates VM A to another host.	
	3	Check	The access control list configuration of VM A is consistent with the original configuration before migration.	
	4	Check	The bandwidth limitation configuration of VM A is consistent with the original configuration before migration.	
	5	Check	The priority policy configuration of VM A is consistent with original the configuration before migration.	
Test verdict	It is deemed as successfully terminated if all the checks are successful, otherwise it is deemed as failed.			

II.3.2 Test case: network QoS

Table II.23 shows the test case for network QoS.

Table II.23 – Test case: network QoS

Network QoS test description				
Test purpose		To verify that the CSC configures network QoS for the VM, including bandwidth limitation, bandwidth reservation, traffic shaping, traffic classification and congestion avoidance.		
Reference		[ITU-T Y.3513] clause 7.3.2		
Test sequence	Step	Type	Description	Result
	1	Stimulus	The CSC configures the bandwidth limitation for the interworking between two VMs.	
	2	Check	Network throughput between the two VMs does not exceed the bandwidth specified in step 1.	
	3	Stimulus	The CSC configures bandwidth reservation for the interworking between two VMs.	
	4	Check	Network throughput between the two VMs is not less than the reserved bandwidth specified in step 3.	
	5	Stimulus	The CSC configures traffic shaping for the specified interface of VM A.	
	6	Check	The traffic of a specified interface of VM A is sent at a more stable rate with lower jitter than before.	
	7	Stimulus	The CSC configures traffic classification for the specified interface of VM A.	
	8	Check	The traffic of a specified interface of VM A is automatically categorized into a number of traffic classes.	
Test verdict	It is deemed as successfully terminated if all the checks are successful, otherwise it is deemed as failed.			

II.3.3 Test case: network address translation

Table II.24 shows the test case for network address translation.

Table II.24 – Test case: network address translation

Network address translation test description				
Test purpose		To verify that the CSC configures the mapping between an internal IP address and external IP address of a specific VM.		
Reference		[ITU-T Y.3513] clause 7.3.3		
Test sequence	Step	Type	Description	Result
	1	Stimulus	The CSC configures NAT to map the VM's private network address to the public network address.	
	2	Check	The private IP address of the VM is translated to specify a public address while accessing the Internet.	
	3	Stimulus	The CSC configures NAT to map the public network address to the VM's private network address.	
	4	Check	The public IP address of the VM is translated to the private network address.	
Test verdict	It is deemed as successfully terminated if all the checks are successful, otherwise it is deemed as failed.			

II.3.4 Test case: network isolation

Table II.25 shows the test case for network isolation.

Table II.25 – Test case: Network isolation

Network isolation test description				
Test purpose		To verify that the CSC's tenant network is isolated even though the network address is overlapped with another tenants' network.		
Reference		[ITU-T Y.3513] clause 7.3.4		
Test sequence	Step	Type	Description	Result
	1	Stimulus	The CSC logs in as tenant A and creates a VM called VM A.	
	2	Stimulus	The CSC creates a VM called VM C assigned with the network address of the same subnet as VM A.	
	3	Stimulus	The CSC logs in as tenant B and creates a VM called VM B assigned with the network address of the same subnet as VM A.	
	4	Check	VM A can communicate with VM C.	
	5	Check	VMA and VM B cannot communicate with each other.	
Test verdict	It is deemed as successfully terminated if all the checks are successful, otherwise it is deemed as failed.			

II.3.5 Test case: IP address allocation

Table II.26 shows the test case for IP address allocation.

Table II.26 – Test case: IP address allocation

IP address allocation test description				
Test purpose		To verify that the CSC allocates an IP address to the VM statically or dynamically.		
Reference		[ITU-T Y.3513] clause 7.3.3		
Test sequence	Step	Type	Description	Result
	1	Stimulus	The CSC allocates specified IP addresses for the VM statically.	
	2	Check	The VM gets the IP as requested by the CSC.	
	3	Stimulus	The CSC allocates IP addresses for the VM through dynamic allocation (DHCP) with a specified IP addresses pool.	
	4	Check	VMs get the IP within the range of the IP pool specified by the CSC.	
Test verdict	It is deemed as successfully terminated if at least one check is successful, otherwise it is deemed as failed.			

II.3.6 Test case: IP address reservation

Table II.27 shows the test case for IP address reservation.

Table II.27 – Test case: IP address reservation

IP address reservation test description				
Test purpose		To verify that the CSC reserves an IP address or a range of IP addresses for specific VM(s).		
Reference		[ITU-T Y.3513] clause 7.3.3		
Test sequence	Step	Type	Description	Result
	1	Stimulus	The CSC reserved a particular IP address for VM A.	
	2	Check	The reserved IP address will not be assigned to VMs other than VM A.	
	3	Stimulus	The CSC reserved a range of IP addresses for VM B.	
	4	Check	The reserved IP addresses will not be assigned to VMs other than VM B.	
Test verdict	It is deemed as successfully terminated if at least one check is successful, otherwise it is deemed as failed.			

II.3.7 Test case: load balance

Table II.28 shows the test case for load balance.

Table II.28 – Test case: load balance

Load balance test description				
Test purpose		To verify that the CSC deploys a load balance mechanism for multiple VMs in order to achieve scalability and fault tolerance of an application.		
Reference		[ITU-T Y.3513] clause 7.3.6		
Test sequence	Step	Type	Description	Result
	1	Stimulus	The CSC configures a round-robin based load balance for HTTP traffic among VMs.	
	2	Check	The HTTP request is forwarded to each server in turn based on a round-robin load balancing policy in step 1.	
	3	Stimulus	The CSC configures a least-connection scheduling based load balance for FTP traffic among VMs.	
	4	Check	The FTP workload is balanced by assigning a new connection request to the VM with the smallest number of connections based on a least-connection scheduling load balancing policy in step 3.	
Test verdict	It is deemed as successfully terminated if all the checks are successful, otherwise it is deemed as failed.			

II.3.8 Test case: firewall

Table II.29 shows the test case for firewall.

Table II.29 – Test case: Firewall

Firewall test description				
Test purpose		To verify that the CSC monitors and controls incoming and outgoing VM traffic based on predetermined security rules.		
Reference		[ITU-T Y.3513] clause 7.3.7		
Test sequence	Step	Type	Description	Result
	1	Stimulus	The CSC configures the VM's network policies to reject all incoming traffic.	
	2	Check	The VM's incoming traffic is dropped by the firewall.	
	3	Stimulus	The CSC configures the VM's network policy to reject all outgoing traffic.	
	4	Check	The VM's outgoing traffic is dropped by the firework.	
Test verdict	It is deemed as successfully terminated if all the checks are successful, otherwise it is deemed as failed.			

II.3.9 Test case: multipath routing

Table II.30 shows the test case for multipath routing.

Table II.30 – Test case: multipath routing

Multipath routing test description				
Test purpose		To verify that the CSC accesses a cloud service through multiple network paths.		
Reference		[ITU-T Y.3513] clause 7.3.6		
Test sequence	Step	Type	Description	Result
	1	Stimulus	The CSC enables a multipath routing function for a particular cloud service.	
	3	Stimulus	One network path is unavailable.	
	4	Check	The particular service is still accessed with the SLA guaranteed by another network path.	
Test verdict	It is deemed as successfully terminated if all the checks are successful, otherwise it is deemed as failed.			

II.3.10 Test case: network information inquiring

Table II.31 shows the test case for network information inquiring.

Table II.31 – Test case: network information inquiring

Network information inquiring test description				
Test purpose		To verify that the CSC inquires network information from the CSP with network device(s) specification, network traffic performance (in terms of throughput, jitter, loss, delay) and network topology.		
Reference		[ITU-T Y.3513] clause 7.3		
Test sequence	Step	Type	Description	Result
	1	Stimulus	The CSC queries the network device's information.	
	2	Check	The CSC receives the information of a particular network's device specification that is consistent with the actual status of the network.	
	3	Stimulus	CSC queries network traffic performance.	
	4	Check	The CSC receives the information of a particular network's traffic performance status that is consistent with the actual status of the network.	
	5	Stimulus	The CSC queries network topology.	
	6	Check	The CSC receives the information of a particular network's topology that is consistent with the actual status of the network.	
Test verdict	It is deemed as successfully terminated if all the checks are successful, otherwise it is deemed as failed.			

Appendix III

Alignment analysis with [ITU-T Y.3513]

(This appendix does not form an integral part of this Recommendation.)

[ITU-T Y.3513] introduces the concept of Infrastructure as a Service (IaaS) and describes its functional requirements. As one of the cloud computing service categories, IaaS provides infrastructure capabilities as services by cloud service providers. It is necessary to ensure that the test cases cover requirements in [ITU-T Y.3513]. Alignment analysis with requirements in [ITU-T Y.3513] is provided as Table III.1.

Table III.1 – Alignment analysis with functional requirements in [ITU-T Y.3513]

	Functional requirements in [ITU-T Y.3513]		Test objects in this Recommendation
1	7 Functional requirement	– It is recommended that the IaaS CSP provides to the CSC IaaS functions, such as a composition of processing, storage, and networking resources with service logic, specific service level agreements (SLAs) and charging model.	Too general, not involved.
2		– It is required that the IaaS CSP provides the CSC with operations handling mechanisms related to provisioned infrastructure resources, such as assign, modify, query and release.	Too general, not involved.
3		– It is recommended that the IaaS CSP provides status information about the infrastructure in response to queries from the CSC.	Too general, not involved.
4		– It is recommended that the IaaS CSP provides a template to the CSC, related to instantiation of infrastructure, which allows for provision processing, storage and networking resources that could be implemented based on the configuration.	Too general, not involved.
5		– It is recommended that the IaaS CSP provides the CSC with operations handling mechanisms related to infrastructure templates to allow modification of infrastructure, such as upload, update, disable, enable, query or release.	Too general, not involved.
6	7.1 Computing service functional requirements	– It is required that the IaaS CSP provides computing functions with specific SLAs and charging model to the CSC.	Too general, not involved.

Table III.1 – Alignment analysis with functional requirements in [ITU-T Y.3513]

	Functional requirements in [ITU-T Y.3513]		Test objects in this Recommendation
7	7.1.1 Physical machine	– It is recommended that the IaaS CSP provides specific hardware specifications of a physical machine to the CSC according to the SLA.	– 7.12 Interoperability testing of physical machine life cycle management between the CSC and CSP
8		– It is recommended that the IaaS CSP provides the CSC with operation handling mechanisms related to a physical machine, such as start, shutdown, hibernate and wakeup.	– 7.12 Interoperability testing of physical machine life cycle management between the CSC and CSP
9		– It is recommended that the IaaS CSP provides physical machine related information in response to queries from the CSC.	– 7.14 Interoperability testing of physical machine configuration inquiring between the CSC and CSP
10	7.1.2 Virtual machine	– It is recommended that the IaaS CSP provides a virtual machine based on the VM template.	– 7.8 Interoperability testing of VM template between the CSC and CSP
11		– The IaaS CSP can optionally provide a virtual machine based on the configurations specified by the CSC.	– 7.1 Interoperability testing of VM configuration between the CSC and CSP
12		– It is required that the IaaS CSP provides the CSC with operations handling mechanisms related to the VM, including, but not limited to, create, delete, start, shutdown, suspend, restore, hibernate and wakeup.	– 7.11 Interoperability testing of VM life cycle management between the CSC and CSP
13		– It is recommended that the IaaS CSP provides VM-related information in response to queries from the CSC.	– 7.13 Interoperability testing of VM configuration inquiring between the CSC and CSP
14	7.1.3 VM migration	– It is recommended that the IaaS CSP provides a virtual machine with migration functions. Based on migration policies, the virtual machine can be migrated from one host to another.	– 7.2 Interoperability testing of VM migration between the CSC and CSP
15	7.1.4 VM scaling	– It is recommended that the IaaS CSP provides a virtual machine with scaling functions based on the scaling policies and monitored events of the virtual machine.	– 7.9 Interoperability testing of VM scaling between the CSC and CSP
16	7.1.5 VM snapshot	– It is recommended that the IaaS CSP provides a virtual machine with snapshot functions. Schedule of snapshots taken from the virtual machine can be performed automatically or manually.	– 7.3 Interoperability testing of VM snapshot between the CSC and CSP

Table III.1 – Alignment analysis with functional requirements in [ITU-T Y.3513]

	Functional requirements in [ITU-T Y.3513]		Test objects in this Recommendation
17	7.1.6 VM clone	– It is recommended that the IaaS CSP provides a virtual machine with clone functions. The cloned VM has identical configuration and CSP/CSC data as the original one.	– 7.4 Interoperability testing of VM clone between the CSC and CSP
18	7.1.7 VM backup	– It is recommended that the IaaS CSP provides a virtual machine with backup functions. When the VM becomes faulty or its data is lost, the VM can be restored using its backup stored according to the CSC policy.	– 7.10 Interoperability testing of VM backup between the CSC and CSP
19	7.1.8 VM time synchronizati on	– It is recommended that the IaaS CSP provides time synchronization functions, which allow the CSC to control the VM time.	– 7.5 Interoperability testing of VM time synchronization between the CSC and CSP
20	7.1.9 VM reservation	– It is recommended that the IaaS CSP provides processing resources reservation (such as CPU, memory) functions. Resources reservation is used to reserve available resources from IaaS infrastructure before VM is initiated.	– 7.6 Interoperability testing of VM reservation between the CSC and CSP
21	7.1.10 VM image	– It is recommended that the IaaS CSP offers the ability for the CSC to provide and use virtual machine images. A VM image consists of infrastructure configuration and CSP data, CSC data or both.	– 7.7 Interoperability testing of VM image between the CSC and CSP
22		– It is recommended that the IaaS CSP supports a different machine image format.	– 7.7 Interoperability testing of VM image between the CSC and CSP
23		– It is required that the IaaS CSP provides operation handling mechanisms related to image，including, but not limited to, add, import, store, register, deregister, query, update, delete and export.	– 7.7 Interoperability testing of VM image between the CSC and CSP
24	7.1.11 VM template	– It is recommended that the IaaS CSP supports the open virtualization format (OVF) template, which is a packaging standard designed to address the portability and deployment of virtual appliances.	– 7.8 Interoperability testing of VM template between the CSC and CSP
25		– It is recommended that the IaaS CSP provides operations handling mechanisms related to machine templates, such as upload, update, disable, enable, query and delete to the CSC.	– 7.8 Interoperability testing of VM template between the CSC and CSP

Table III.1 – Alignment analysis with functional requirements in [ITU-T Y.3513]

	Functional requirements in [ITU-T Y.3513]		Test objects in this Recommendation
26	7.2 Storage service functional requirements	– It is recommended that the IaaS CSP provides storage functions, such as block level storage, file level storage and object-based storage, with specific SLAs and charging model to the CSC. The storage functions can be provided to the CSC directly or used by the virtual machine as attached storage.	– 8.6 Interoperability testing of storage life cycle management between the CSC and CSP
27		– It is recommended that the IaaS CSP provides the CSC with operations handling mechanisms related to storage, such as create, attach, detach, query and delete a volume of storage at either block level or file-system level, write, read and delete data for a given storage.	– 8.6 Interoperability testing of storage life cycle management between the CSC and CSP
28		– It is recommended that the IaaS CSP provides storage utilisation information in response to queries from the CSC.	– 8.7 Interoperability testing of storage utilization status inquiring between the CSC and CSP
29	7.2.1 Storage migration	– It is recommended that the IaaS CSP provides storage migration functions. Based on migration policies, data can be migrated between different logical unit numbers (LUNs), different storage devices, local storage to shared storage and vice versa.	– 8.1 Interoperability testing of storage migration between the CSC and CSP
30	7.2.2 Storage snapshot	– It is recommended that the IaaS CSP provides storage with snapshot functions. Snapshot can be realized at either block or file-system levels. The data can be restored using the snapshot.	– 8.2 Interoperability testing of storage snapshot between the CSC and CSP
31	7.2.3 Storage backup	– It is recommended that the IaaS CSP provides storage with backup functions. Backup can be realized at block level, file level or object-based storage.	– 8.3 Interoperability testing of storage backup between the CSC and CSP
32	7.2.4 I/O performance	– It is recommended that the IaaS CSP provides input/output (I/O) limitation for each VM.	– 8.5 Interoperability testing of I/O performance between the CSC and CSP
33	7.2.5 Storage resource reservation	– It is recommended that the IaaS CSP provides storage resource (e.g., storage space and LUN) reservation functions.	– 8.4 Interoperability testing of storage resource reservation between the CSC and CSP
34	7.3 Network service functional requirements	– It is recommended that the IaaS CSP provides network functions, such as IP address, VLAN, virtual switch, load balance, firewall, with specific SLAs or charging model. Network functions are applied to access and interconnect processing and storage resources.	– 9.7 Interoperability testing of load balance between the CSC and CSP – 9.8 Interoperability testing of firewall between the CSC and CSP
35		– It is recommended that the IaaS CSP provides network information in response to queries from the CSC.	– 9.10 Interoperability testing of network information inquiring between the CSC and CSP

Table III.1 – Alignment analysis with functional requirements in [ITU-T Y.3513]

	Functional requirements in [ITU-T Y.3513]		Test objects in this Recommendation
36	7.3.1 Network policy migration	– It is recommended that the IaaS CSP provides network policy migration along with virtual machine migration. In this case, the network policy of the migrated virtual machine is the same as before the migration.	– 9.1 Interoperability testing of network policy migration between the CSC and CSP
37	7.3.2 Network QoS	– It is recommended that the IaaS CSP provides operation handling mechanisms related to the network quality of service (QoS), such as bandwidth limit, bandwidth reservation, traffic shaping, traffic classification, congestion avoidance, at port level, device level and network level.	– 9.2 Interoperability testing of network QoS between the CSC and CSP
38	7.3.3 IP Address	– It is recommended that the IaaS CSP provides IP address reservation.	– 9.6 Interoperability testing of IP address reservation between the CSC and CSP
39		– It is required that the IaaS CSP allows the CSC to apply, bind, unbind, query, release an IP address to processing resources or storage resources.	– 9.5 Interoperability testing of IP address allocation between the CSC and CSP
40		– It is recommended that the IaaS CSP allows the CSC to allocate IP addresses to provisioned processing resources or storage resources with a dynamic or static method.	– 9.5 Interoperability testing of IP address allocation between the CSC and CSP
41		– The IaaS CSP can optionally provide network address translation (NAT).	– 9.3 Interoperability testing of network address translation between the CSC and CSP
42	7.3.4 Network isolation	– It is required that the IaaS CSP provides the CSC with isolated tenants' networks.	– 9.4 Interoperability testing of network isolation between the CSC and CSP
43		– It is recommended that the IaaS CSP provides the CSC with operations handling mechanisms related to isolated tenants' networks, such as create, query and release.	– 9.4 Interoperability testing of network isolation between the CSC and CSP
44	7.3.5 Virtual Networking	– It is recommended that the IaaS CSP manages virtual networking to provide network connectivity amongst various processing and storage resources.	– 9.4 Interoperability testing of network isolation between the CSC and CSP
45	7.3.6 Load balance	– It is recommended that the IaaS CSP optimizes infrastructure resources utilization by providing load balance related functions, such as throughput, response time, to avoid overload of any one of the infrastructure resources.	– 9.7 Interoperability testing of load balance between the CSC and CSP
46		– The IaaS CSP can optionally provide multipath routing to achieve an optimized traffic management (e.g., to improve network utilization, to guarantee QoS at network congestion or fault).	– 9.9 Interoperability testing of multipath routing between the CSC and CSP

Table III.1 – Alignment analysis with functional requirements in [ITU-T Y.3513]

	Functional requirements in [ITU-T Y.3513]		Test objects in this Recommendation
47	7.3.7 Firewall	– It is recommended that the IaaS CSP delivers a physical or virtual firewall to the CSC.	– 9.8 Interoperability testing of firewall between the CSC and CSP
48	7.3.8 Gateway	– It is recommended that the IaaS CSP provides necessary network interworking functions so that the CSC uses provisioned infrastructure resources as if they are at the CSC's premises.	– 9.4 Interoperability testing of network isolation between the CSC and CSP
49	7.3.9 Network configuration	– It is recommended that the IaaS CSP provides the CSC with operations handling mechanisms related to the network configurations according to the objectives of the SLA.	See other network related testing objects: – 9.5 Interoperability testing of IP address allocation between the CSC and CSP – 9.2 Interoperability testing of network QoS between the CSC and CSP – 9.3 Interoperability testing of network address translation between the CSC and CSP

Bibliography

[b-ETSI GS NFV-TST 002 V1.1] ETSI GS NFV-TST 002 V1.1 (2016), *Network Functions Virtualisation (NFV); Testing Methodology; Report on NFV Interoperability Testing Methodology*.


SMS
25
SMS
25
SMS
25

Cloud computing interoperability activities

Supplement 65 to ITU-T Q.3900-series Recommendations

(07/2014)

SERIES Q: SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

Summary

Supplement 65 to ITU-T Q-series Recommendations provides the summary information for cloud computing interoperability activities of existing standards development organizations (SDOs) and the groups, forums and open sources developing the specifications that have the potential to utilize cloud computing interoperability testing tools. This supplement should also be helpful for the development of cloud testing specifications.

Table of Contents

1 Scope

This supplement describes the summary information of cloud computing interoperability activities of existing standards development organizations (SDOs) and the groups, forums and open sources developing the specifications that have potential to utilize cloud computing interoperability testing tools. This supplement also provides summary list of activities by the SDOs including those of cloud computing interoperability testing areas.

2 References

ITU-T references

[ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014), *Information technology –Cloud computing – Overview and vocabulary*.

[ITU-T Y.3501] Recommendation ITU-T Y.3501 (2013), *Cloud computing framework and high-level requirements.*

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), *Information technology — Cloud computing -Reference architecture.*

[ITU-T Y.3510] Recommendation ITU-T Y.3510 (2013), *Cloud computing infrastructure requirements.*

[ITU-T Y.3512] Recommendation ITU-T Y.3512 (2014), *Cloud computing - Functional requirements of Network as a Service*.

[ITU-T Y.3513] Recommendation ITU-T Y.3513 (2014), *Cloud computing - Functional requirements of Infrastructure as a Service.*

[ITU-T Y.3520] Recommendation ITU-T Y.3520 (2013), *Cloud computing framework for end to end resource management.*

ETSI references

[ETSI TR 102 997] ETSI TR 102 997 V1.1.1 (2010), *CLOUD; Initial analysis of standardization requirements for Cloud services*.

[ETSI TR 103 125] ETSI TR 103 125 V1.1.1 (2012), *CLOUD; SLAs for Cloud services*.

[ETSI TR 103 126] ETSI TR 103 126 V1.1.1 (2012), *CLOUD; Cloud private-sector user recommendations*.

[ETSI TS 103 142] ETSI TS 103 142 V1.1.1 (2013), *CLOUD; Test Descriptions for Cloud Interoperability*.

IEEE references

[IEEE P2301] IEEE P2301, *Guide for Cloud Portability and Interoperability Profiles (CPIP)*.

[IEEE P2302] IEEE P2302, *Standard for Intercloud Interoperability and Federation (SIIF)*.

IETF references

[IETF RFC 2330] IETF RFC 2330 (1998), *Framework for IP Performance Metrics*

[IETF RFC 4110] IETF RFC 4110 (2005), *A Framework for Layer 3 Provider-Provisioned Virtual Private Networks*.

[IETF RFC 6749] IETF RFC 6749 (2012), *The OAuth 2.0 Authorization Framework*.

NIST references

[NIST SP 500-292] NIST SP 500-292 (2011), *NIST Cloud Computing Reference Architecture*.

[NIST SP 500-293vol1] NIST SP 500-293, *US Government Cloud Computing Technology Roadmap Volume I Release 1.0: High-Priority Requirements to Further USG Agency Cloud Computing Adoption*.

[NIST SP 500-293vol2] NIST SP 500-293, *US Government Cloud Computng Technology Roadmap Volume II Release 1.0: Useful Information for Cloud Adopters*.

[NIST SP 800-145] NIST SP 800-145 (2011), *The NIST Definition of Cloud Computing*.

OASIS references

[OASIS TOSCA-v1.0] OASIS TOSCA-v1.0, *Topology and Orchestration Specification for Cloud Applications Version 1.0*.

TM Forum references

[TMF GB917] TMF GB917, *SLA Management Handbook*.

[TMF GB963] TMF GB963, *Cloud SLA Application Note*.

[TMF TR174] TMF TR174, *Enterprise-Grade External Compute IaaS Requirements*.

[TMF TR178] TMF TR178, *Enabling End-to-End Cloud SLA Management*.

[TMF TR194] TMF TR194, *Multi-Cloud Service Management Accelerator Pack-Introduction*.

3 Abbreviations and acronyms

This supplement uses the following abbreviations and acronyms:

3CPP	China Cloud Computing Promotion and Policy Forum
BPaaS	Business Process as a Service
CCI	Cloud Computing Interoperability
CDMI	Cloud Data Management Interface
CIMI	Cloud Infrastructure Management Interface
CMI	Cloud Management Initiative
CPIP	Cloud Portability and Interoperability Profile
CSC	Cloud Service Customer
CSMIC	Cloud Services Measurement Initiative Consortium
CSP	Cloud Service Provider
CT-CCVOCAB	Collaborative Teams on Cloud Computing Overview and Vocabulary
DAPS	Distributed Application Platforms and Services
DMTF	Distributed Management Task Force
ENISA	European Network Information Security Agency
ETSI	European Telecommunications Standards Institute
GICTF	Global Inter-Cloud Technology Forum
IaaS	Infrastructure as a Service
ICT	Information and Communication Technology
IEEE	Institute of Electrical and Electronics Engineers
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IT	Information Technology

NaaS	Network as a Service
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OCC	Open Cloud Consortium
OCCI	Open Cloud Computing Interface
OCCI-WG	OCCI Working Group
ODCA	Open Data Center Alliance
OGF	Open Grid Forum
OVF	Open Virtualization Format
PaaS	Platform as a Service
PoC	Proof of Concept
REST	Representational State Transfer
SaaS	Software as a Service
SAJACC	Standards Acceleration to Jumpstart the Adoption of Cloud Computing
SCIM	System for Cross-domain Identity Management
SDO	Standards Development Organization
SIIF	Standard for Inter-cloud Interoperability and Federation
SLA	Service Level Agreement
SMI	Simple Management Interface
SNIA	Storage Networking Industry Association
SOA	Service Oriented Architecture
SPEC	Standard Performance Evaluation Corporation
VM	Virtual Machine

NOTE – Abbreviations not described in this supplement can be found in [ITU-T Y.3500] and other reference documents listed in clause 2.

4 Introduction

The purpose of this supplement is to provide the list of existing cloud computing interoperability and testing related activities. Clause 5 describes cloud computing interoperability activities by different standards development organizations (SDOs) while clause 6 identifies potential cloud computing interoperability testing areas. This supplement is intended to be of help for developing cloud computing interoperability testing Recommendations.

5 Existing cloud computing interoperability activities

5.1 Standards development organizations for cloud computing interoperability

Many SDOs are developing cloud standards. Some of them are listed in ITU-T FG-Cloud technical reports. From an interoperability testing perspective, some SDOs do not conduct testing themselves but conduct joint/collaborative/sponsored testing groups as described in clause 5.2. For example, Distributed Management Task Force (DMTF), European Telecommunications Standards Institute (ETSI), Organization for the Advancement of Structured Information Standards (OASIS), Storage Networking Industry Association (SNIA) and some SDOs sponsored Cloud Plugfest as part of the Cloud Interoperability Week where, during the testing of specifications, they improved such Cloud standards as cloud data management interface (CDMI), open cloud computing interface (OCCI), cloud infrastructure management interface (CIMI) and open

virtualization format (OVF). Open Data Center Alliance (ODCA) proof of concept (PoC) shows how OASIS topology and orchestration specification for cloud applications (TOSCA) standard can be used to fulfil industry requirements for application portability in the enterprise cloud. TM Forum, OASIS, W3C cover platform as a service (PaaS)/software as a service (SaaS) level cloud interoperability and testing to some extent.

This clause lists and briefly describes representative cloud computing SDOs' activities/specifications which are used in cloud interoperability testing.

5.1.1 DMTF

The mission of Distributed Management Task Force (DMTF) is to create standards that enable interoperability among multi-vendor systems, tools and solutions within the enterprise.

DMTF works on cloud computing management interface related aspects of common core identifiers (CCIs).

DMTF's cloud management initiative (CMI) is focused on developing interoperable cloud infrastructure, management standards and promoting adoption of those standards in the industry.

Cloud management working group (CMWG) and Open virtualization format working group (OVFWG) of DMTF are developing cloud computing interoperability related standards. The CIMI developed by CMWG is a self-service interface for infrastructure clouds, allowing cloud users to dynamically provision, configure and administer their cloud usage using a high level interface that abstracts away much of complexity of system management. OVF developed by OVFWG is a packaging standard designed to address the portability and deployment of virtual appliances. OVF enables simplified and error-free deployment of virtual appliances across multiple virtualization platforms.

Table 5-1 – DMTF documents and work items related to CCI

Reference	Name/Title	Status
DSP-IS0101	Interoperable clouds	Published
DSP0264	CIMI-CIM specification	Published
DSP0263	CIMI model and RESTful HTTP-based protocol	Published
DSP0243	Open virtualization format specification	Published

5.1.2 ETSI

The European Telecommunications Standards Institute (ETSI) is an independent, non-profit, standardization organization in the telecommunications industry (equipment makers and network operators) in Europe, with worldwide projection.

The goal of ETSI Technical Committee CLOUD (ETSI TC CLOUD, TC GRID renamed TC CLOUD in 2010) is to address issues associated with the convergence between information technology (IT) and telecommunications, paying particular attention to the lack of interoperable cloud solutions.

ETSI works on definitions, service level agreements (SLAs) and testing methodologies related to aspects of CCI.

ETSI TC CLOUD has developed technical reports on standardization requirements for cloud services. Portability and interoperability of clouds is one of the main requirements [ETSI TR 102 997].

ETSI TC CLOUD have also developed CCI testing related standards including interoperability testing specification for OCCI and CDMI [ETSI TS 103 142] and cloud specific SLA standards [ETSI TR 103 125].

Test descriptions for cloud interoperability [ETSI TS 103 142] specifies interoperability test descriptions for OCCI and CDMI standards.

SLAs for cloud services [ETSI TR 103 125] aims to review previous work on SLAs and to derive potential requirements for cloud specific SLA standards.

Table 5-2 – ETSI documents and work items related to CCI

Reference	Name/Title	Status
[ETSI TS 103 142]	CLOUD; Test descriptions for cloud interoperability	Published
[ETSI TR 103 125]	CLOUD; SLAs for cloud services	Published
[ETSI TR 103 126]	CLOUD; Cloud private-sector user recommendations	Published
[ETSI TR 102 997]	CLOUD; Initial analysis of standardization requirements for Cloud services	Published

5.1.3 GICTF

Global Inter-Cloud Technology Forum (GICTF) aims to promote standardization of network protocols and the interfaces through which cloud systems interwork with each other and to enable the provision of more reliable cloud services.

GICTF works on standardization of inter-cloud interoperability, including functional requirements and interface.

GICTF has developed requirements for inter-cloud computing and inter-cloud interface specification. The functional requirements of inter-cloud systems have been identified and the inter-cloud interface has been developed. Three reference points for the interface specified in GICTF's documents are the interface between inter-cloud service controls, the interface between inter-cloud service controls and data centre operation systems, and the interface between the inter-cloud service controls and the network operation systems.

Table 5-3 – GICTF documents and work items related to CCI

Reference	Name/Title	Status
GICTF WhitePaper 2012-2	Intercloud interface specification draft (Cloud resource data model)	published
GICTFWhitePaper 2012-2	Intercloud interface specification draft (Intercloud protocol)	published
GICTF White Paper 2012-1	Technical requirements for supporting the inter-cloud networking	published
GICTF WhitePaper	Use cases and functional requirements for inter-cloud Computing	published

5.1.4 IEEE

The Institute of Electrical and Electronics Engineers (IEEE) is a professional association that is dedicated to advancing technological innovation and excellence.

IEEE works on inter-cloud related aspects of CCI.

The IEEE cloud computing initiative (CCI) is a broad-based collaborative project for the cloud to be introduced by IEEE. Several products and services that are now being introduced by IEEE CCI, including a website, conferences, continuing education courses, publications, standards and a platform for testing cloud computing applications.

Two major cloud computing standards of IEEE CCI are currently in process: [IEEE P2301] Guide for Cloud Portability and Interoperability Profiles (CPIPs) and [IEEE P2302] Standard for Intercloud Interoperability and Federation (SIIF). The purpose of CPIP is to advise cloud computing ecosystem participants (cloud vendors, service providers and users) of standards-based choices in areas such as application interfaces, portability interfaces, management interfaces, interoperability interfaces, file formats, and operation conversions. CPIP groups these choices into multiple logical profiles, which are organized to address different cloud personalities.

SIIF defines topology, functions and governance for cloud-to-cloud interoperability and federation. Topological elements include clouds, roots, exchanges (which mediate governance between clouds) and gateways (which mediate data exchange between clouds). Functional elements include name spaces, presence, messaging, resource ontologies (including standardized units of measurement), and trust

infrastructure. Governance elements include registration, geo-independence, trust anchor, and potentially compliance and audit. The standard does not address intra-cloud (within cloud) operation, as this is cloud implementation-specific, nor does it address proprietary hybrid-cloud implementations.

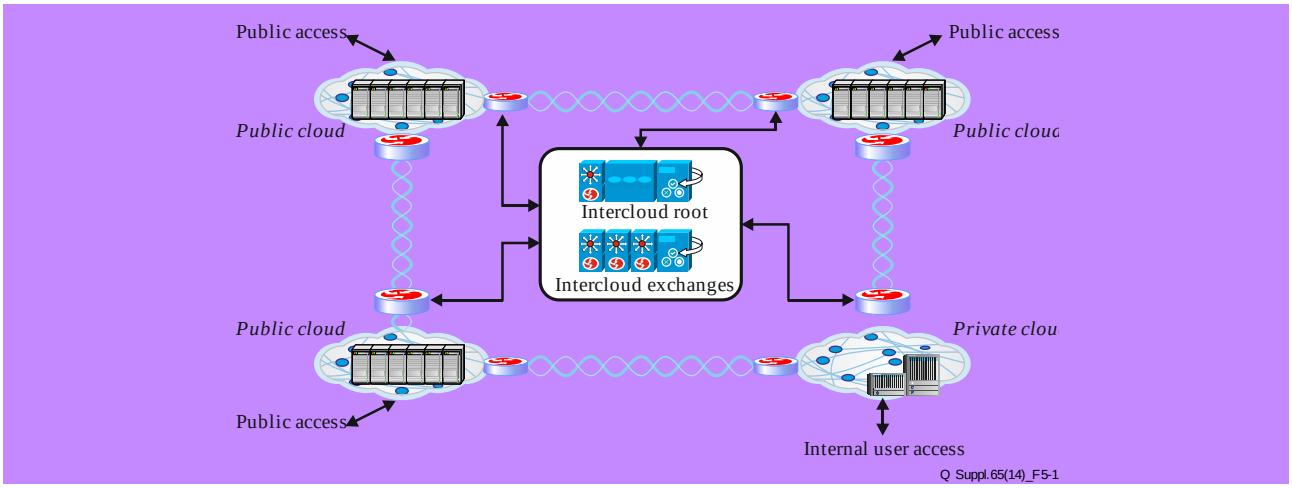


Figure 5-1 – Reference network inter-cloud topology

(Reference: IEEE Cloud Computing Initiative: http://cloudcomputing.ieee.org/intercloud)

Table 5-4 – IEEE documents and work items related to CCI

Reference	Name/Title	Status
IEEE P2301	Guide for Cloud Portability and Interoperability Profiles (CPIP)	In process
IEEE P2302	Standard for Intercloud Interoperability and Federation (SIIF)	In process

Another area IEEE plans to explore involves developing environments for creating and testing protocols for the IEEE P2302 Draft Standard for intercloud interoperability and federation. IEEE has partnered with universities and research institutions around the world that already have cloud computing resources. The goal is to create a well-connected standards-based platform.

5.1.5 IETF

The IETF is an international organization that develops standards and specifications applicable to the Internet.

IETF works on cloud computing interface, and testing methodology related aspects of CCI Cloud related working groups are:

- IETF/l3vpn (Layer 3 Virtual Private Networks);
- IETF/oauth (Web Authorization Protocol);
- IETF/scim (System for Cross-domain Identity Management);
- IETF/ippm (IP Performance Metrics).

The L3VPN, OAUTH, system for cross-domain identity management (SCIM) working groups work on cloud computing protocol related aspects of CCI.

The L3VPN working group is responsible for defining, specifying and extending BGP/MPLS IP VPNs solutions for supporting provider-provisioned L3VPN.

The OAUTH working group develops OAuth for authorization. OAuth provides client applications a 'secure delegated access' to server resources on behalf of a resource owner.

The SCIM working group is developing SCIM specification that is designed to make managing user identity in cloud based applications and services easier.

The IPPM working group works on testing methodology related aspects of CCI.

The IPPM working group develops and maintains standard metrics that can be applied to the quality, performance, and reliability of Internet data delivery services and applications running over transport layer protocols (e.g., TCP, UDP) over IP.

Some CCI related individual Internet drafts have also been submitted to IETF.

The draft Cloud Reference Framework presents a cloud reference framework that intends to provide a basis for designing interoperable cloud services and their integration into existing open Internet and enterprise IT infrastructures [draft-khasnabish-cloud-reference-framework].

Table 5-5 – IETF documents and work items related to CCI

Reference	Name/Title	Status
IETF RFC 2330	Framework for IP Performance Metrics	Published
IETF RFC 4110	A Framework for Layer 3 Provider-Provisioned Virtual Private Networks	Published
IETF RFC 6749	The OAuth 2.0 Authorization Framework	Published
I-D. draft-ietf-scim-core-schema-03	System for Cross-domain Identity Management: Core Schema	Draft
I-D. draft-khasnabish-cloud-reference-framework	Cloud Reference Framework	Draft

5.1.6 ISO/IEC JTC1

ISO/IEC JTC 1 is the Joint Technical Committee 1 of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Its purpose as a technical committee is to develop, maintain, promote, and facilitate standards in the fields of IT and information and communication technology (ICT).

The scope of JTC1/SC38 (subcommittee 38 of JTC1, distributed application platforms and services (DAPS)) is standardization for interoperable DAPS including web services, service oriented architecture (SOA) and cloud computing.

The WG3 (working group on Cloud Computing) of JTC1/SC38 works on definitions related aspects of CCI. JTC1/SC38 developed Overview and Vocabulary [ISO/IEC WD 17788] and Reference Architecture of cloud computing [ISO/IEC DIS 17789].

ISO/IEC JTC 1/SC 38 (specifically WG 3: Cloud Computing) and ITU-T/SG 13 form the Collaborative Teams on Cloud Computing Overview and Vocabulary (CT-CCVOCAB) and Cloud Computing Reference Architecture (CT-CCRA). The purpose of the collaboration is to develop a common text, in the form of a new standard, between the two groups based on two documents: Draft new Recommendation Y.CCdef Cloud Computing Definition and Vocabulary (from ITU-T Q.26/13), and ISO/IEC WD 17788 – Cloud Computing Vocabulary and ISO/IEC WD 17789 – Cloud Computing Reference Architecture (from ISO/IEC JTC 1/SC 38/WG 3).

Cloud computing interoperability (CCI) is defined in CT-CCVOCAB as follows:

Interoperability in the context of cloud computing includes the ability of a cloud service customer (CSC) to interact with a cloud service and exchange information according to a prescribed method and obtain predictable results.

Interoperability also includes the ability for one cloud service to work with other cloud services, either through a cloud service provider-to-provider relationship, or where a CSC uses multiple different cloud services in some form of composition to achieve their business goals.

Interoperability stretches beyond the cloud services themselves and also includes the interaction of the CSC with the cloud service management facilities of the cloud service provider (CSP). Ideally, the CSC should have a consistent and interoperable interface to the cloud service management functionality and be able to interact with two or more CSPs without needing to deal with each provider in a specialized way.

Table 5-6 – ISO/IEC documents and work items related to CCI

Reference	Name/Title	Status
ISO/IEC WD 17788	Cloud Computing Vocabulary	Published
ISO/IEC DIS 17789	Information technology -- Cloud computing -- Reference architecture	Published

5.1.7 ITU-T

The ITU Telecommunication Standardization Sector (ITU-T) is one of the three sectors (divisions or units) of the International Telecommunication Union (ITU); it coordinates standards for telecommunications.

Cloud computing is an important part of ITU-T Study Group (SG) 13 work and the group develops standards that detail requirements and functional architectures of the cloud computing ecosystem, covering inter- and intra-cloud computing and technologies supporting X as a service (XaaS).

ITU-T works on definition, cloud computing management interface related aspects of CCI.

This work of SG 13 includes infrastructure and networking aspects of cloud computing models, as well as deployment considerations and requirements for interoperability and data portability.

SG 13 also develops standards enabling consistent end-to-end, multi-cloud management and monitoring of services exposed by and across different service providers' domains and technologies.

Table 5-7 – ITU-T documents and work items related to CCI

Reference	Name/Title	Status
ITU-T Y.3500	Recommendation ITU-T Y.3500 (2014), Information technology -Cloud computing – Overview and vocabulary	Published
ITU-T Y.3501	Recommendation ITU-T Y.3501 (2013), Cloud computing framework and high-level requirements	Published
ITU-T Y.3502	Recommendation ITU-T Y.3502 (2014), Information technology -Cloud computing - Reference architecture	Published
ITU-T Y.3510	Recommendation Y.3510 (2013), Cloud computing infrastructure requirements	Published
ITU-T Y.3512	Recommendation Y.3512 (2014), Cloud computing – Functional requirements of Network as a Service.	Published
ITU-T Y.3513	Recommendation Y.3513 (2014), Cloud computing – Functional requirements of Infrastructure as a service.	Published
ITU-T Y.3520	Recommendation Y.3520 (2013), Cloud computing framework for end to end resource management	Published
ITU-T Y.e2ecslm-Req	End-to-end cloud service lifecycle management	Draft
ITU-T Y.e2ecmrgb	Common Model for End-to-End Cloud Computing Resource Management	Draft

5.1.8 NIST

The National Institute of Standards and Technology (NIST) is a measurement standards laboratory, also known as a National Metrological Institute (NMI), which is a non-regulatory agency of the United States Department of Commerce.

NIST standards acceleration to jumpstart the adoption of cloud computing (SAJACC) working group: Focused on use case definition and refinement to produce testable cloud computing scenarios.

NIST SAJACC: Phase I is published project to define testable use cases that provide the basis for independent evaluation of cloud standards, products and processes. The output of the working group report "SAJACC Working Group Recommendations to NIST" has been delivered in February 2013.

Working group continues with Phase II to define and refine use cases with greater technical detail. SAJACC Phase II launched February 2013 to refine and extend Phase I use case test cases based on priority action plan.

Figure 5-2 shows the NIST Cloud Portal (currently in the form of a community Wikipedia website) and the main steps of starting the SAJACC process. SAJACC has completed several iterations of steps 1-3, and exploratory activities conducted in a community setting for the process described in step 4 of the figure, resulting in output that has been documented in the NIST Cloud Standards Wiki.

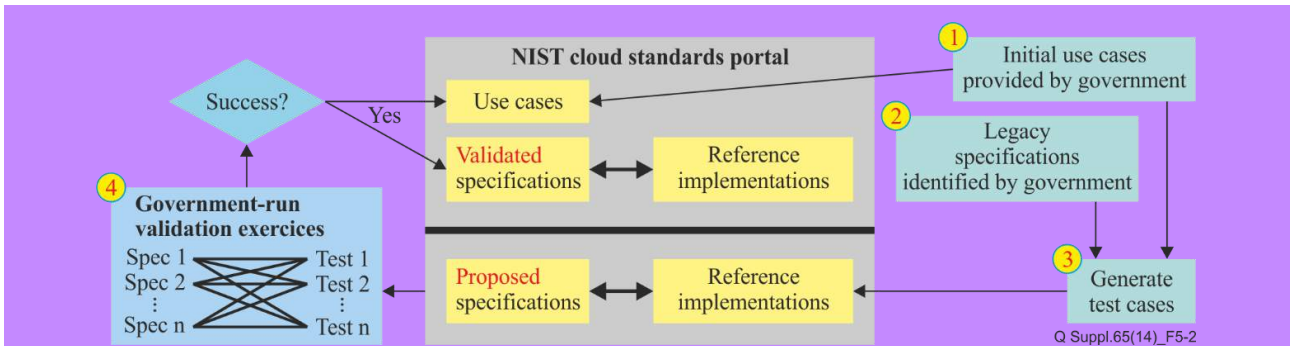


Figure 5-2 – NIST cloud standards portal (Reference: NIST cloud computing website)

Table 5-8 – NIST documents and work items related to CCI

Reference	Name/Title	Status
NIST SAJACC Internal Group Report	SAJACC working group recommendations to NIST	Published
NIST SAJACC White Paper	Virtual machine portability white paper	Draft
NIST SP 800-145	The NIST Definition of Cloud Computing	Published
NIST SP 500-292	NIST Cloud Computing Reference Architecture	Published
NIST SP 500-293vol1	US Government Cloud Computing Technology Roadmap Volume I Release 1.0: High-Priority Requirements to Further USG Agency Cloud Computing Adoption	Draft
NIST SP 500-293vol2	US Government Cloud Computing Technology Roadmap Volume II Release 1.0: Useful Information for Cloud Adopters	Draft

5.1.9 OASIS

OASIS is a non-profit consortium that drives the development, convergence and adoption of open standards for the global information society.

OASIS works on the TOSCA project which is cloud interoperability initiative related aspects of CCI.

Cloud includes several technical projects, such as OASIS TOSCA project which enhances the portability and management of cloud applications and services across their lifecycle. TOSCA will enable the interoperable description of application and infrastructure cloud services, the relationships between parts of the service and the operational behaviour of these services (e.g., deploy, patch, shutdown).

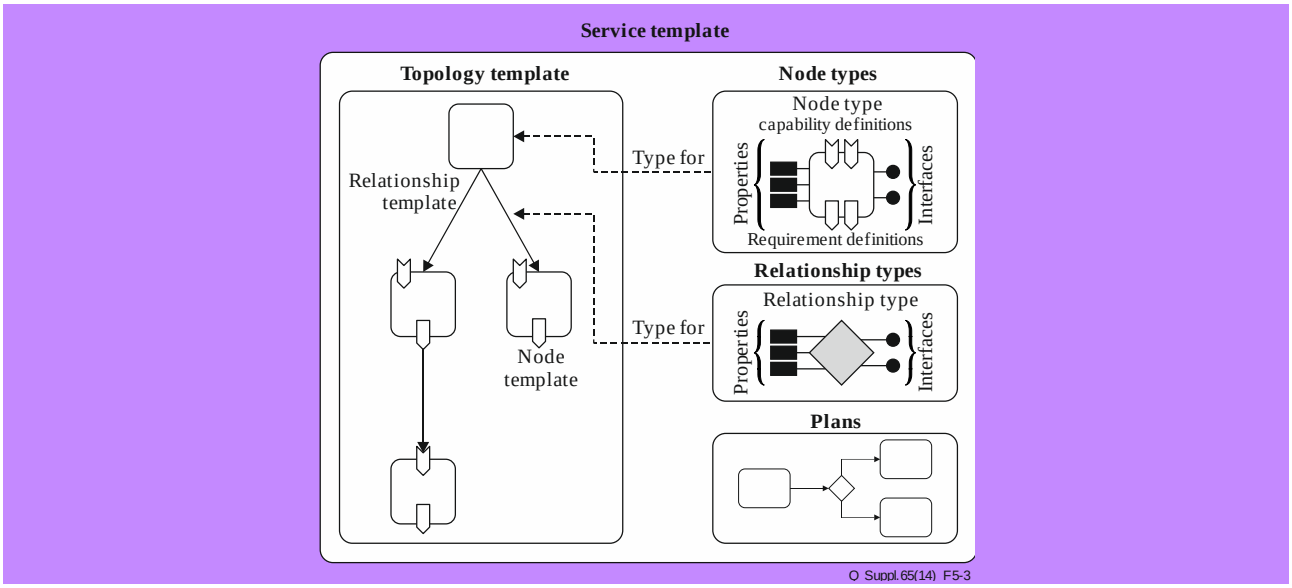


Figure 5-3 – Structural elements of a service template and their relations (Ref. Topology and orchestration specification for cloud applications version 1.0 OASIS standard)

Table 5-9 – OASIS documents and work items related to CCI

Reference	Name/Title	Status
OASIS TOSCA-v1.0	Topology and orchestration specification for cloud applications (TOSCA) Version 1.0	Published

5.1.10 ODCA

The ODCA is an independent organization created in October 2010 with the assistance of Intel Corporation to coordinate the development of standards for cloud computing. The organization has created a usage model roadmap featuring 19 prioritized usage models. The usage models provide detailed requirements for data centre and cloud solutions, and will include detailed technical documentation discussing the requirements for technology deployments.

Four CCI related usage models have been published by ODCA, while ODCA also initiated a new PoC project to determine where the virtual machine (VM) industry currently is in meeting interoperability requirements outlined in the ODCA VM interoperability usage model in 2013.

Table 5-10 – ODCA documents and work items related to CCI

Reference	Name/Title	Status
ODCA SAAS_Interop_UM_Rev1.0	Software as a service (SaaS) interoperability	published
ODCA PAAS_Interop_UM_Rev1.0	Platform as a service (PaaS) interoperability	published
ODCA VM_Interoperability_in_a Hybrid_Cloud_Enviroment_rev1.2	Virtual machine (VM) Interoperability in a hybrid cloud environment	published
ODCA VM_Interop_PoC_White_Paper	Implementing the Open Data Center Alliance Virtual Machine Interoperability Usage Model	published

A team led by T-Systems Telekom Innovation Laboratories, the FZI research team from the University of Karlsruhe and supported by Intel Corporation carried out a PoC project to implement the usages described in the document: Implementing the ODCA Virtual Machine Interoperability Usage Model.

The Implementing the ODCA Virtual Machine Interoperability Usage Model POC was developed within the ODCA Manageability and Services Workgroup and includes specifications for interoperability developed by DMTF, an ODCA partner organization.

The POC outlines testing criteria and procedures for documenting how hypervisor and VM solutions from both ODCA members and non-members interoperated in real-world enterprise cloud scenarios.

5.1.11 OGF

The Open Grid Forum (OGF) is a community of users, developers, and vendors leading the global standardization effort for distributed computing (including clusters, grids and clouds).

OGF works on OCCI that resource management interface related aspects of CCI.

The open cloud computing interface working group (OCCI-WG) of the OGF was established in 2009. The purpose of this group is the creation of a practical solution to interface with cloud infrastructures exposed as a service. It focuses on the creation of an API for interfacing infrastructure as a service (IaaS) cloud computing facilities, which is sufficiently complete to allow for the creation of interoperable implementations.

The OCCI developed by OGF OCCI-WG is a set of specifications for cloud computing service providers. OCCI has a set of implementations that act as proofs of concept. It builds upon world wide web fundamentals by using the representational state transfer (REST) approach for interacting with services.

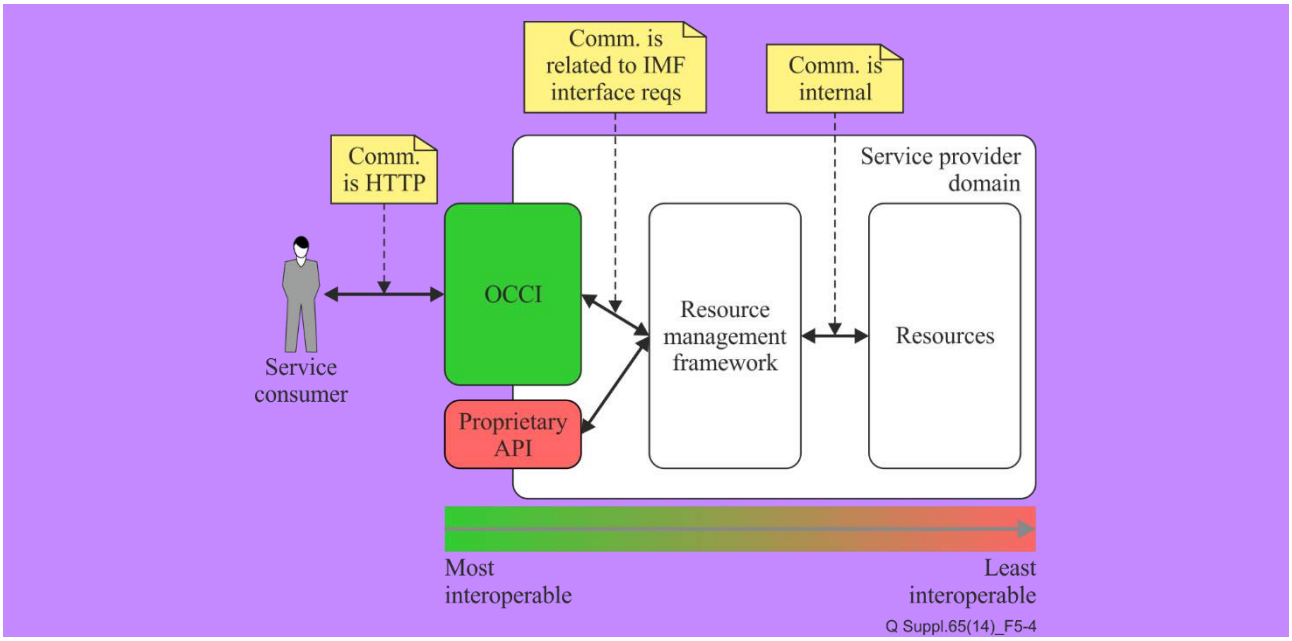


Figure 5-4 – OCCI's place in a provider's architecture (Reference: GFD-P-R.183 OCCI-WG Open Cloud Computing Interface – Core)

Table 5-11 – OGF documents and work items related to CCI

Reference	Name/Title	Status
OGF GFD.183	Open Cloud Computing Interface - Core	published
OGF GFD.184	Open Cloud Computing Interface - Infrastructure	published
OGF GFD.185	Open Cloud Computing Interface - RESTful HTTP Rendering	published
OGF GFD.192	Web Services Agreement Specification (WS-Agreement)	published
OGF GFD.193	WS-Agreement Negotiation	published

5.1.12 SNIA

SNIA is a SDO, published the CDMI as an SNIA architecture (April 2010) and also moving to standardization. SNIA is also a trade association for storage industry promoting the Cloud storage market overall and promoting the adoption of the CDMI standard, and promoting interoperability implementations (Plugfest, test suites, conformance programs). SNIA also produces open source software; CDMI reference implementation is available under BSD license.

SNIA works on cloud computing interface related aspects of the CCI.

CDMI standard defines an interoperable format for moving data and associated metadata between cloud providers interoperability. CDMI is an HTTP/RESTful protocol with TLS support for securing the data, metadata and communications.

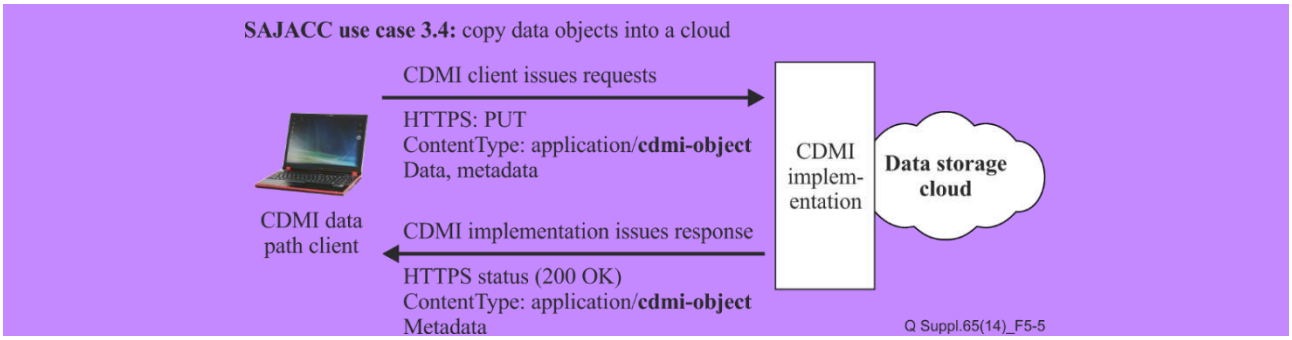


Figure 5-5 – SAJACC Use Case: Copy data objects into a cloud (Reference: SNIA, NIST)

Table 5-12 – SNIA documents and work items related to CCI

Reference	Name/Title	Status
ISO 17826:2012	Cloud data management interface v1.0.2	Published

5.1.13 TM Forum

TM Forum (formerly TeleManagement Forum) is the world's leading industry association focused on improving business effectiveness for service providers and their suppliers, including the production of best practices and standards.

TM Forum works on SLA management related aspects of CCI.

TM Forum published SLA related documents such as SLA Management Handbook [TMF GB917], Cloud SLA Application Note [TMF GB963] and Enterprise-Grade External Compute IaaS Requirements [TMF TR174].

SLA Management Handbook [TMF GB917] provides a full set of definitions, rules and methodology for the specification, deployment and management of SLAs, as well as useful tools and best practices, for use by both customers and service providers.

Cloud SLA Application Note [TMF GB963] is intended for enterprise CSPs desiring to offer a commercially credible SLA based on ECLC "Enterprise-Grade External Compute IaaS v1.0", and for an enterprise customer seeking enterprise-grade SLAs.

Enterprise-Grade External Compute IaaS Requirements [TMF TR174] describes the requirements for enterprise-grade external compute IaaS from the perspective of the enterprise consumer. SLA clarity and cross-service provider commonality of service level definitions are specified in this document as one of the key requirements of enterprise-grade IaaS.

Enabling End-to-End Cloud SLA Management [TMF TR178] recommends a set of business considerations and architecture design principles that are required to support end-to-end cloud SLA management with the aim to facilitate discussion regarding SLA consistency across cloud deployment models and services models.

Quick Start Pack for Cloud: Trouble to Resolve [TMF GB960] focuses on the detailed specification and delivery of a set of process flows, defined in business process management notation (BPMN), that utilize all currently defined business process framework level 3 process elements within project scope.

Table 5-13 – TM Forum documents and work items related to CCI

Reference	Name/Title	Status
TMF GB917	SLA Management Handbook	Published
TMF GB960	Quick Start Pack for Cloud: Trouble to Resolve	Published
TMF GB963	Cloud SLA Application Note	Published
TMF TR174	Enterprise-Grade External Compute IaaS Requirements	Published
TMF TR178	Enabling End-to-End Cloud SLA Management	Published
TMF TR194	Muli-Cloud Service Management Accelerator Pack-Introduction	Published

5.2 Testing groups, open sources and tools for cloud computing testing

5.2.1 Testing groups

3CPP

China Cloud Computing Promotion and Policy Forum (3CPP) is a non-profit organization initiated by the cloud industry. The objectives of 3CPP include facilitating the communication between government and the industry, and promoting the research on the standards, policies, plans and laws in cloud computing area in China. 3CPP has more than 60 members including Chinese cloud service and infrastructure providers.

3CPP works on cloud computing testing methodology related aspects of CCI.

3CPP initiated "Trusted Cloud Service Certification" in 2013, and established related documents including "Assessment Method for Trusted Cloud Service Certification" and "Cloud Computing Service Level Agreement Reference Framework", etc. In these documents, some evaluation indexes and evaluation methods are defined.

Table 5-14 – 3CPP documents and work items related to CCI

Reference	Name/Title	Status
3CPP TCSA Operation Method	Operation method of trusted cloud service assessment	Published
3CPP TCSC Assessment Method	Assessment method for trusted cloud service certification	Published
YDB144-2014	Cloud service agreement reference framework	Published

http://www.3cpp.org/lab/cloud/trustedcloudev/index.shtml

Cloud Plugfests

The Cloud Interoperability Plugfest series (or "Cloud Plugfests" for short) was originated out of community-based interoperability efforts started by OGF and SNIA in 2011, and expanded to include a variety of support tools provided by these organizations and ETSI to support the community. ETSI joined the Cloud Plugfest series as a full supporting partner in 2012. Furthermore, Cloud Plugfests developed into a cooperative venue to encourage interoperability on implementations of several relevant cloud software stacks, products and multiple cloud-related standards.

Cloud Plugfests works on cloud computing testing methodology related aspects of CCI. Test descriptions for cloud interoperability delivered by Cloud Plugfest specifies interoperability test descriptions for OCCI and CDMI standards. The test descriptions cover the OCCI and CDMI protocol specifications where relevant and more specifically: 1) OCCI interoperability testing, to prove that end-to-end functionality is as required by the standard. 2) CDMI interoperability testing, to prove that end-to-end functionality is as required by the standard. 3) OCCI + CDMI interworking testing, to prove that end-to-end functionality is as required by the standards. Cloud Plugfests works on cloud computing testing methodology related aspects of CCI.

Table 5-15 – Cloud Plugfests documents and work items related to CCI

Reference	Name/Title	Status
ETSI TS 103 142	CLOUD; Test Descriptions for Cloud Interoperability	Published

CSMIC

Cloud Services Measurement Initiative Consortium (CSMIC) is a consortium formed in May 2010 led by Carnegie Mellon University to address the need for industry-wide, globally accepted measures for calculating the benefits and risks of cloud-computing services.

CSMIC works on cloud computing testing methodology related aspects of CCI.

CSMIC defined service management index (SMI) for measuring any type of cloud services (IaaS, PaaS, SaaS, business process as a service (BPaaS) and big data). Service measurement index framework released in November 2012 and has been updated to version 2 in January 2014 by CSMIC.

The SMI is a hierarchical framework. The top level divides the measurement space into seven categories. Each category is further refined by three or more attributes. Then within each attribute a set of KPIs are defined that describe the data to be collected for each measure/metric.

Table 5-16 – CSMIC documents and work items related to CCI

Reference	Name/Title	Status
SMI Framework Version 2.0 draft	Service measurement index framework Version 2.0 draft	Published

OCC

The Open Cloud Consortium (OCC) is a non-profit organization that manages and operates cloud computing infrastructure to support scientific, medical, health care and environmental research.

The OCC is organized into different working groups. The open cloud testbed (OCT) working group (OCTWG) of OCC manages and operates the OCT. The OCT is a geographically distributed cloud testbed spanning four data centres and connected with 10 G and 100 G network connections. The OCT is used to develop new cloud computing software and infrastructure.

A current focus of the OCC OCTWG is on developing an OpenFlow enabled version of Hadoop, a project support by the National Science Foundation (NSF).

Reports and tools: http://etics.res.eng.it/tools/etics-gui/

OCEAN

Open Cloud for Europe, jApan and beyoNd (OCEAN), a FP7-ICT Support Action Project was established in August 2011 to foster the emergence of sustainable open source Cloud offering and boost market innovation in Europe, by generating greater efficiency and economics of scale among European FP7 collaborative research projects on open source cloud computing, and to support collaboration between Japanese and European research and open source projects on cloud computing.

SPEC

The Standard Performance Evaluation Corporation (SPEC) is a non-profit corporation formed to establish, maintain and endorse a standardized set of relevant benchmarks.

SPEC released SPECvirt_sc2010 in July 2010. The SPECvirt_sc2010 addresses performance evaluation of data centre servers used in virtualized server consolidation. It measures the end-to-end performance of all system components including the hardware, virtualization platform, and the virtualized guest operating system and application software. SPECvirt_sc2010 enables comparing of system performance across multiple hardware, virtualization platforms and applications.

SPECvirt_sc2010 measures the maximum number of workloads that a platform can simultaneously run while maintaining specific quality of service metrics. Each workload consists of a specific set of virtual machines. The benchmark utilizes several SPEC workloads representing applications that are common targets of virtualization and server consolidation. Scaling is achieved by running additional sets of virtual machines, called "tiles", until overall throughput reaches a peak.

SPEC release SPECvirt_sc2013, the new version of SPECvirt, was issued in May 2013. It utilizes heavier and busier workloads and further stress the system's ability to meet the benchmark's quality of service requirements.

SPECvirt_sc2013 shares the general benchmark architecture from SPECvirt_sc2010, including the benchmark harness and most of the application workloads and VM types. Heavier and more bursty workloads that require virtual machines with more memory and vCPUs and further stress the system's ability to meet the benchmark's quality of service requirements have been added in SPECvirt_sc2013.

Many computer system vendors have submitted SPECvirt benchmark results to SPEC.

5.2.2 Open sources

OpenStack

OpenStack is a global collaboration of developers and cloud computing technologists producing the ubiquitous open source cloud computing platform for public and private clouds. The project aims to deliver solutions for all types of clouds by being simple to implement, massively scalable, and feature rich. The technology consists of a series of interrelated projects delivering various components for a cloud infrastructure solution.

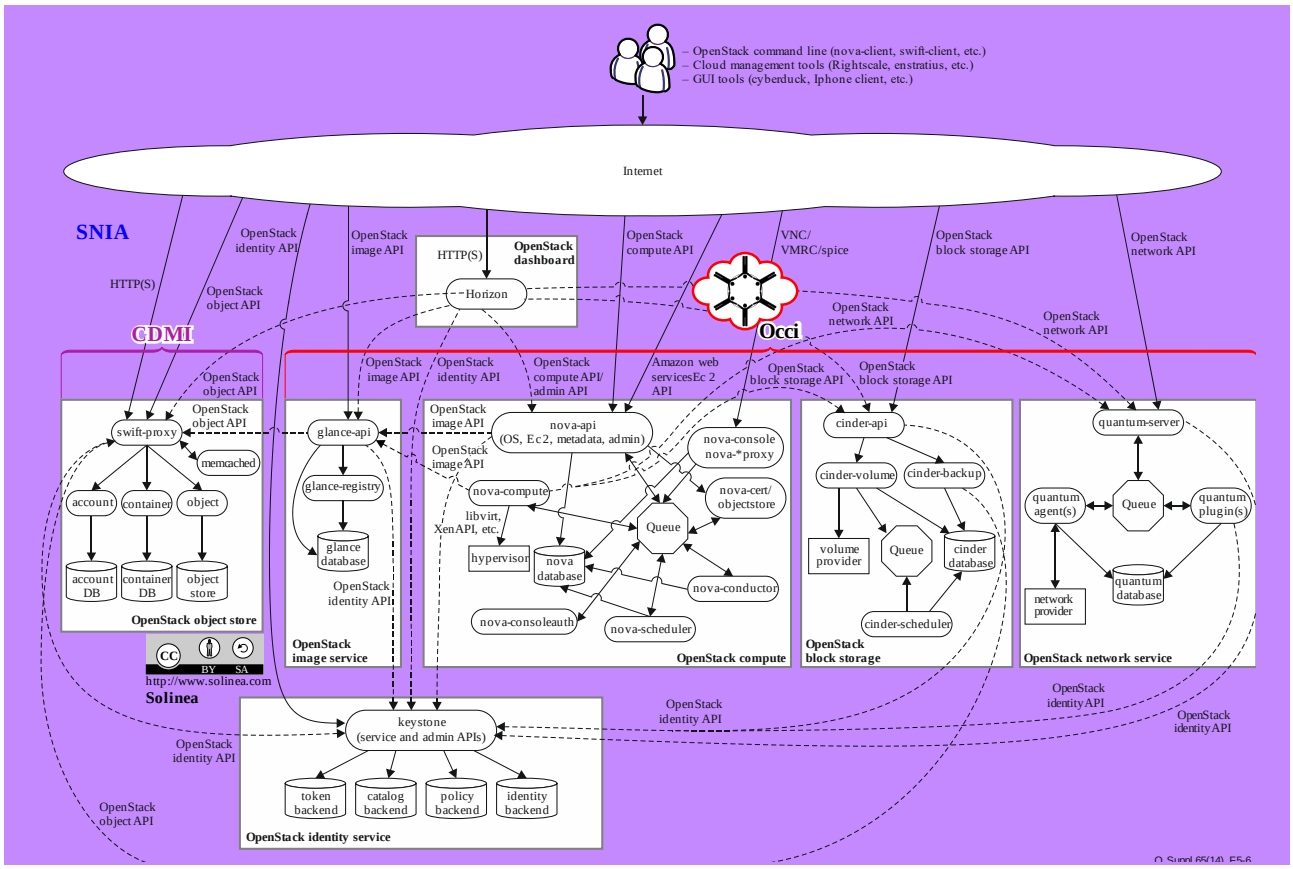


Figure 5-6 – The OpenStack API

OpenStack works on cloud computing interface related aspects of CCI. It is expected that OpenStack will provide a set of test for cloud computing functions.

Cloud interoperability is one of the most important targets in OpenStack project. In order to provide cloud interoperability, except for native APIs support, OpenStack project also support standardized API implementations in OpenStack project for interoperability insurance. By now, CDMI [ISO 17826:2012] and OCCI [OGF GFD.183] implementation is available for OpenStack. CDMI is used by OpenStack to support container creation, object upload and object retrieve and so on. OCCI is used by OpenStack to support authentication, instance creation, volume attachment and so on. Since OpenStack have implemented standard interoperable cloud API such as CDMI and OCCI, it can provide a suitable cloud interoperability testing environment for specific protocol and helping the study on cloud interoperability testing methodology. Details CDMI implementation for OpenStack refer to https://github.com/osaddon/cdmi. Details OCCI implementation for OpenStack refer to https://github.com/tmetsch/occi-os .

5.2.3 Tools

VMmark

VMmark is a free tool that hardware vendors, virtualization software vendors and other organizations use to measure the performance and scalability of applications running in virtualized environments. VMmark is a free virtual machine benchmark software suite provided by VMware, which is a commercial company that provides cloud and virtualization software and service.

VMware release Vmmark v1 in July 2007. VMmark v1 comprises a series of "sub-tests" that are derived from commonly used load-generation tools. The VMmark benchmark refers to this unit of work as a tile. The total number of tiles that a system can accommodate provides a coarse-grain measure of that system's consolidation capacity.

VMware released the new version Vmmark, Vmmark v2 in October 2010. VMmark 2 generates a realistic measure of virtualization platform performance by incorporating a variety of platform-level workloads such as dynamic virtual machine relocation (vMotion) and dynamic datastore relocation (storage vMotion), in addition to traditional application-level workloads. The benchmark system in VMmark 2 comprises a series of "sub-tests" that are derived from commonly used load-generation tools and commonly initiated virtualization administration tasks. The VMmark 2 benchmark features a tile-based scheme for measuring application performance and provides a consistent methodology that captures both the overall scalability and individual application performance. The total number of tiles that a multi-host platform can accommodate and the performance of each individual workload within the tile determine the overall benchmark score.

More than ten computer systems have submitted VMmark V2 benchmark results to VMware by now.

5.3 Cloud security standardization activities

Cloud security is an important subject with interoperability testing for the whole areas of CCI. This clause information is for future study in order to take into account the security interoperability aspects.

Several SDOs have begun to study cloud security and several governments are also leading the discussion, releasing documents from a wide security point of view taking into account many stakeholders. For example, European Network Information Security Agency (ENISA) issued Cloud computing security assessment and NIST started Fedramp. Cloud security includes also political aspects because it faces security threats affecting personal and organizational properties. As a result, this supplement lists major SDOs, and references appropriate security-related specifications case by case.

ENISA, CSA, DMTF, NIST, ISO/IEC JTC1/SC27, SC38, ITU-T SG 17, OASIS (Identity in the Cloud TC) are discussing Cloud security.

- CSA https://cloudsecurityalliance.org/
- DMTF http://www.dmtf.org/
- ENISA http://www.enisa.europa.eu/
- ISO/IEC JTC1/SC27 and SC38 http://www.iso.org/iso/jtc1_home.html
- ITU-T SG 17 http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/default.aspx
- NIST http://www.nist.gov/itl/cloud/
- OASIS https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=id-cloud

In ITU-T, Study Group 17 (SG 17) has been designated the lead study group for "Telecommunication Security" which includes developing and maintaining security outreach material; coordination of security-related work; and identification of needs and assignment and prioritization of work to encourage timely development of telecommunication security Recommendations.

6 Potential interoperability testing areas of cloud computing

Cloud computing involves a wide variety of technologies, from distributed processing to virtualization. The types of capabilities offered are also diverse: from IaaS, in which the cloud capabilities type provided to the CSC is an infrastructure capabilities type, and PaaS, in which the cloud capabilities type provided to the CSC is a platform capabilities type, to SaaS, in which the cloud capabilities type provided to the CSC is an application capabilities type.

The targets of cloud computing standardization are so diverse that many standards organizations are studying cloud computing focusing on their respective areas of expertise. Taking into consideration the targets of interoperability testing in clause 5, it is possible to identify the targets for interoperability testing as the follows:

- Target area A: Interaction between CSC and CSP (between user layer and access layer);
- Target area B: Collaboration among different cloud services (between service layers including inter-cloud);
- Target area C: Consistent and interoperable of manage interface (between multi-layer functions (e.g., BSS/OSS) and cloud services);
- Target area D: Collaboration with legacy network.

NOTE – Collaboration with legacy network is not defined in [ITU-T Y.3502]. Target area D is not illustrated in Figure 6-1.

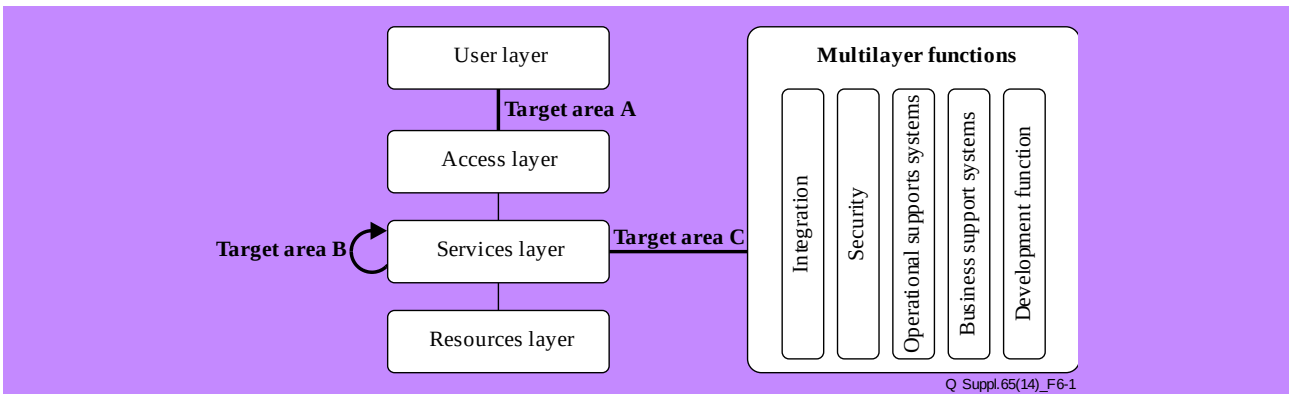


Figure 6-1 – Potential cloud computing interoperability target areas

There are three different cloud computing capabilities types:

- Infrastructure capabilities type ;
- Platform capabilities type ;
- Application capabilities type.

Different cloud capabilities types have different interoperability testing.

Table 6-1 shows the potential interoperability testing target areas of cloud computing with different cloud computing capabilities types. It is useful to identify the target areas. Each target area should include functional testing as well as performance testing.

Table 6-1 Potential cloud computing interoperability testing areas

Capability type / Target areas	Infrastructure capabilities type	Platform capabilities type	Application capabilities type
Target area A: CSC – CSP			
Target area B: CSP – CSP			
Target area C: CSP – management interface			
Target area D:CSP – legacy network			
"CSC – CSP" means interaction between CSC and CSP. "CSP – CSP" means collaboration among different cloud services. "CSP – management interface" means consistent and interoperable management interface. "CSP – legacy network" means collaboration with legacy network.			

Appendix I

Summaries of referenced documents

I.1 3CPP references and associated summaries

[3CPP TCSA Operation Method] – Operation method of trusted cloud service assessment

[3CPP TCSC Assessment Method] – Assessment method for trusted cloud service certification

[YDB144-2014] – Cloud service agreement reference framework

I.2 CSMIC references and associated summaries

[SMI Framework Version 2.0 draft] – Service measurement index framework Version 2.0 draft

I.3 DMTF references and associated summaries

[DSP-IS0101] – Interoperable clouds

This white paper describes a snapshot of the work being done in the DMTF Open Cloud Standards Incubator, including use cases and reference architecture as they relate to the interfaces between a CSP and a cloud service consumer. The goal of the Incubator is to define a set of architectural semantics that unify the interoperable management of enterprise and cloud computing. This paper summarizes the core use cases, reference architecture and service lifecycle. These building blocks will be used to specify the cloud provider interfaces, data artefacts and profiles to achieve interoperable management.

[DSP0264] – CIMI-CIM specification

This document defines a CIM representation for the CIMI logical model.

[DSP0263] –CIMI model and RESTful HTTP-based protocol

This specification describes the model and protocol for management interactions between a cloud IaaS provider and the consumers of an IaaS service. The basic resources of IaaS (machines, storage and networks) are modelled with the goal of providing consumer management access to an implementation of IaaS and facilitating portability between cloud implementations that support the specification. This document specifies a REST-style protocol using HTTP. However, the underlying model is not specific to HTTP, and it is possible to map it to other protocols as well.

[DSP0243] – Open virtualization format specification

This document describes an open, secure, portable, efficient and extensible format for the packaging and distribution of software to be run in virtual machines.

I.4 ETSI references and associated summaries

[ETSI TS 103 142] – CLOUD: Test descriptions for Cloud Interoperability

This document specifies interoperability test descriptions for OCCI and CDMI standards. The test descriptions cover the OCCI and CDMI protocol specifications where relevant and more specifically: 1) OCCI interoperability testing, to prove that end-to-end functionality is as required by the standard. 2) CDMI interoperability testing, to prove that end-to-end functionality is as required by the standard. 3) OCCI + CDMI interworking testing, to prove that end-to-end functionality is as required by the standards.

[ETSI TR 103 125] – CLOUD: SLAs for Cloud services

This document aims to review previous work on SLAs including ETSI guides from TC USER and contributions from EuroCIO, etc. and to derive potential requirements for cloud specific SLA standards.

[ETSI TR 103 126] – CLOUD: Cloud private-sector user recommendations

This document provides an overview of private sector user recommendations for cloud services especially from the viewpoint of large enterprises in the European context.

[ETSI TR 102 997] – CLOUD: Initial analysis of standardization requirements for Cloud services

This document describes standardization requirements for cloud services. It is based on the outcome of the ETSI TC GRID workshop, "Grids, Clouds and Service Infrastructures", 2nd and 3rd of December 2009. This event brought together key stakeholders of the grid, cloud and telecommunication domains to review state of the art and current trends. Needs for standardization, with a particular focus on the emerging area of cloud computing and services, were discussed. This document introduces and expands on the conclusions reached.

I.5 GICTF references and associated summaries

Intercloud interface specification draft (cloud resource data model)

The purpose of this document is to identify the functional requirements of inter-cloud systems and describe an inter-cloud interface in specific terms.

Intercloud interface specification draft (intercloud protocol)

The purpose of this document is to identify the functional requirements of inter-cloud systems and describes an inter-cloud interface in specific terms.

Technical requirements for supporting the intercloud networking

This paper attempts to clarify the "Technical requirements for the inter-cloud network which interconnects among cloud systems" and the "Expected functions in cloud systems from network perspective".

Use cases and functional requirements for inter-cloud computing

This document describes the required functionalities for inter-cloud systems and the requirements for inter-cloud interfaces.

I.6 IEEE references and associated summaries

[IEEE P2301] – Guide for Cloud Portability and Interoperability Profiles (CPIP)

The purpose of CCIP is to advise cloud computing ecosystem participants (cloud vendors, service providers, and users) of standards-based choices in areas such as application interfaces, portability interfaces, management interfaces, interoperability interfaces, file formats, and operation conversions. CCIP group these choices into multiple logical profiles, which are organized to address different cloud personalities.

[IEEE P2302] – Standard for Intercloud Interoperability and Federation (SIIF)

SIIF is to define topology, functions, and governance for cloud-to-cloud interoperability and federation. Topological elements include clouds, roots, exchanges (which mediate governance between clouds), and gateways (which mediate data exchange between clouds). Functional elements include name spaces, presence, messaging, resource ontologies (including standardized units of measurement), and trust infrastructure. Governance elements include registration, geo-independence, trust anchor and potentially compliance and audit. The standard does not address intra-cloud (within cloud) operation, as this is cloud implementation-specific, nor does it address proprietary hybrid-cloud implementations.

I.7 IETF references and associated summaries

[IETF RFC 2330] – Framework for IP Performance Metrics

[IETF RFC 4110] – A Framework for Layer 3 Provider-Provisioned Virtual Private Networks

[IETF RFC 6749] – The OAuth 2.0 Authorization Framework

[I-D. draft-ietf-scim-core-schema-03] – System for Cross-domain Identity Management: Core Schema

[I-D. draft-ietf-scim-core-schema-03] – System for Cross-domain Identity Management: Core Schema

[I-D. draft-khasnabish-cloud-reference-framework] – Cloud reference framework

I.8 ISO/IEC JTC 1 references and associated summaries

[ISO/IEC WD 17788] – Cloud Computing Vocabulary

[ISO/IEC DIS 17789] – Topology and orchestration specification for cloud applications (TOSCA) Version 1.0

I.9 NIST references and associated summaries

[NIST SAJACC Internal Group Report] – SAJACC working group recommendations to NIST

This document describes the work done by the SAJACC working group so far, which has resulted in a set of preliminary use cases developed for the first pass through the SAJACC process and a set of initial demonstration validation evaluations. Through a series of open workshops, and through public comment and feedback, NIST will continue to refine these use cases and add new use cases as appropriate.

[NIST SAJACC White Paper] – Virtual machine portability white paper

This white paper describes the current technologies, formats and tools that support virtual machine (VM) portability. It identifies challenges and opportunities for further improvements to interoperability, and presents a high-level summary of key VM portability problems faced by cloud consumers today.

[NIST SP 800-145] – The NIST Definition of Cloud Computing

The NIST definition characterizes important aspects of cloud computing and is intended to serve as a means for broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what is cloud computing to how to best use cloud computing. The service and deployment models defined form a simple taxonomy that is not intended to prescribe or constrain any particular method of deployment, service delivery or business operation.

[NIST SP 500-292] – NIST Cloud Computing Reference Architecture

This document presents the NIST cloud computing reference architecture (RA) and taxonomy (Tax) that will accurately communicate the components and offerings of cloud computing. The guiding principles used to create the RA were 1) develop a vendor-neutral architecture that is consistent with the NIST definition and 2) develop a solution that does not stifle innovation by defining a prescribed technical solution.

[NIST SP 500-293vol1] – US Government Cloud Computing Technology Roadmap Volume I Release 1.0: High-Priority Requirements to Further USG Agency Cloud Computing Adoption

Volume I to the US Government Cloud Computing Technology Roadmap, an interagency document developed to foster adoption of cloud computing by federal agencies and supports the private sector, and reduces uncertainty by improving the information available to decision.

[NIST SP 500-293vol2] – US Government Cloud Computing Technology Roadmap Volume II Release 1.0: Useful Information for Cloud Adopters

Volume I to the US Government Cloud Computing Technology Roadmap, an interagency document developed to foster adoption of cloud computing by federal agencies and supports the private sector, and reduces uncertainty by improving the information available to decision.

I.10 OASIS references and associated summaries

[OASIS TOSCA-v1.0] – Topology and Orchestration Specification for Cloud Applications Version 1.0

I.11 ODCA references and associated summaries

[ODCA SAAS_Interop_UM_Rev1.0] – Software as a service (SaaS) interoperability

This usage model outlines five usage scenarios based on two perspectives of interoperability, along with success and failure scenarios for each. In addition, service provider requirements and an industry call to action are presented.

[ODCA PAAS_Interop_UM_Rev1.0] – Platform as a service (PaaS) interoperability

This paper outlines five usage scenarios, along with success and failure scenarios for each. Finally, CSP requirements and an industry call to action are presented.

[ODCA VM_Interoperability_in_a Hybrid_Cloud_Enviroment_rev1.2] – Virtual machine (VM) Interoperability in a hybrid cloud environment

This document addresses a number of important additional dimensions including extending the portability concept, extending the life cycle model with states and conditions, and increased alignment with external activities such as that of the OVF specification

[ODCA VM_Interop_PoC_White_Paper] – Implementing the open data center alliance virtual machine interoperability usage model

A team led by T-Systems Telekom Innovation Laboratories, the FZI research team from the University of Karlsruhe and supported by Intel Corporation carried out a PoC project to implement the usages described in the document, described in this report.

I.12 OGF references and associated summaries

[OGF GFD.183] Open Cloud Computing Interface – Core

The OCCI core specification defines the OCCI core model. The OCCI core model can be interacted with renderings (including associated behaviours) and expanded through extensions.

[OGF GFD.184] – Open Cloud Computing Interface – Infrastructure

OCCI Infrastructure contains the definition of the OCCI Infrastructure extension for the IaaS domain. The specification defines additional resource types, their attributes and the actions that can be taken on each resource type.

[OGF GFD.185] – Open Cloud Computing Interface – RESTful HTTP Rendering

The OCCI HTTP rendering defines how to interact with the OCCI core model using the RESTful OCCI API. The specification defines how the OCCI core model can be communicated and thus serialized using the HTTP protocol.

[OGF GFD.192] – Web Services Agreement Specification (WS-Agreement)

The web services agreement specification (WS-Agreement), a web services protocol for establishing agreement between two parties, such as between a service provider and consumer.

[OGF GFD.193] – WS-Agreement Negotiation

The WS-Agreement Negotiation specification, a web services protocol for multi-round negotiation of an agreement between two parties, such as between a service provider and consumer. Works on top of WS-Agreement.

I.13 SNIA references and associated summaries

[ISO 17826:2012] – Cloud Data Management Interface

CDMI specifies the interface to access cloud storage and to manage the data stored therein. It is applicable to developers who are implementing or using cloud storage.

I.14 TMF references and associated summaries

[TMF GB917] – SLA Management Handbook

This document provides a full set of definitions, rules and methodology for the specification, deployment and management of SLAs, as well as useful tools and best practices, for use by both customers and service providers.

[TMF GB963] – Cloud SLA Application Note

This document is intended for enterprise CSPs desiring to offer a commercially credible SLA based on ECLC "Enterprise-Grade External Compute IaaS v1.0", and for an enterprise customer seeking enterprise-grade SLAs.

[TMF TR174] – Enterprise-grade IaaS requirements

This document describes the requirements for enterprise-grade external compute IaaS from the perspective of the enterprise consumer. SLA clarity and cross-service provider commonality of service level definitions are specified in this document as one of the key requirements of enterprise-grade IaaS.

[TMF TR178] – Enabling End-to-End Cloud SLA Management

This documents describes the requirements for enabling end-to-end cloud SLA management, which recommends a set of business considerations and architecture design principles that are required to support end-to-end cloud SLA management with the aim to facilitate discussion regarding SLA consistency across cloud deployment models and services models.

[TMF TR194] – Muli-Cloud Service Management Accelerator Pack-Introduction

Overview of multi-cloud management business challenges and how TM Forum is addressing them.

I.15 ITU-T draft Recommendation

[ITU-T Y.3512] – Cloud computing – Functional requirements of Network as a Service

This Recommendation provides use cases and functional requirements of network as a service (NaaS), one of the representative cloud service categories. This Recommendation covers the following:

- High level concept of NaaS;
- Functional requirements for NaaS;
- Typical use cases for NaaS.

This Recommendation provides use cases and requirements of NaaS application, NaaS platform and NaaS connectivity services. General requirements on NaaS can be found at [ITU-T Y.3501].

[ITU-T Y.3513] – Cloud computing – Functional requirements of Infrastructure as a service

This Recommendation provides use cases and functional requirements of IaaS, one of the representative cloud service categories. This Recommendation covers the following:

- General description of IaaS;
- Functional requirements for IaaS;
- Typical use cases for IaaS.

[ITU-T Y.e2ecslm-Req] – ITU-T draft Recommendation Y.35xx, End-to-end cloud service lifecycle management

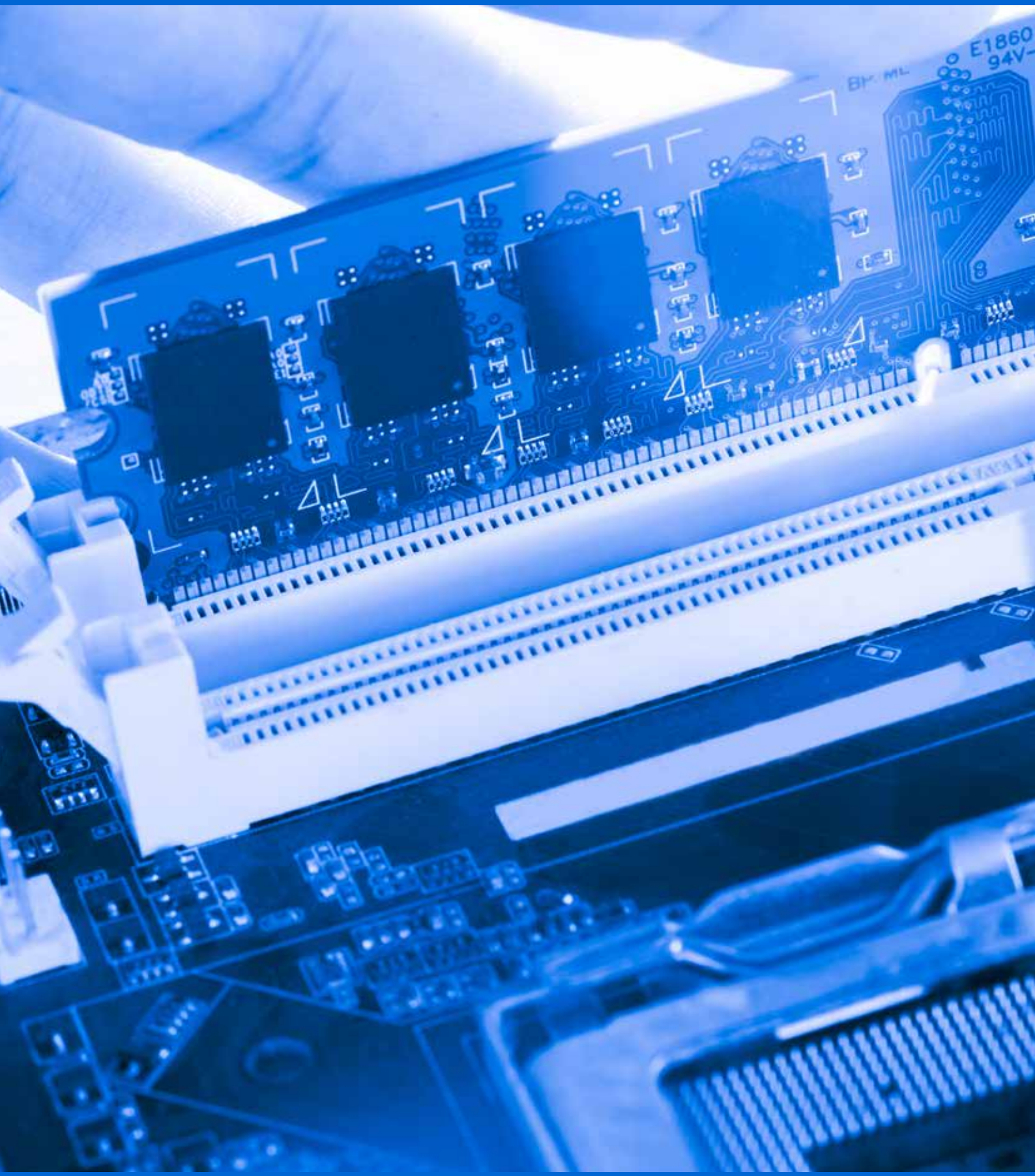
This draft Recommendation describes the functional requirement of the lifecycle for service management aspects of cloud services. The cloud service lifecycle management involves charging events management, policy management, management of role related information, service/application provisioning, resource management, context management and content management

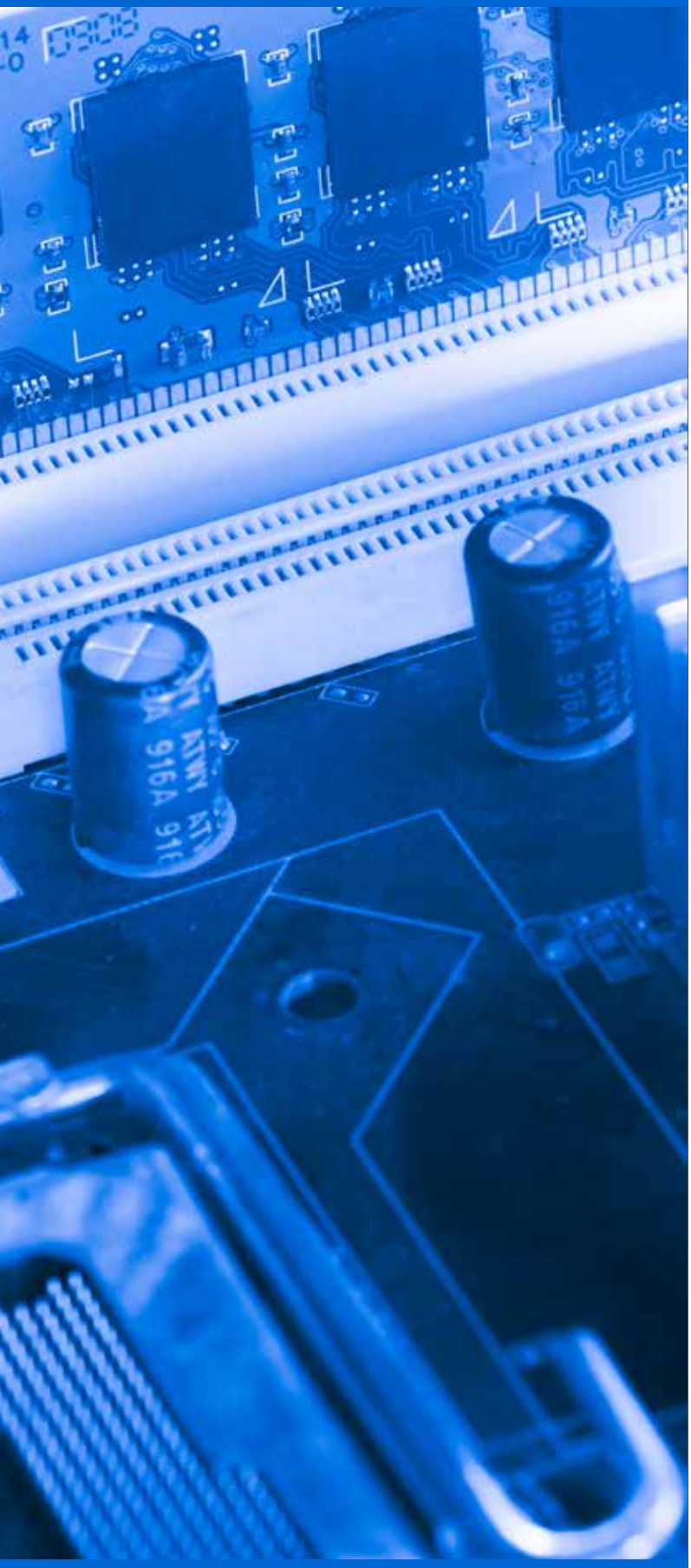
[ITU-T Y.e2ecmrgb] – ITU-T draft Recommendation Y.35xx, Common model for End-to-End Cloud Computing Resource Management

This draft Recommendation:

– Provides a model, based on SES simple management interfaces (SMIs), for all layers of cloud computing reference architecture.

– Demonstrates how such approach would result in development and deployment of fundamentally manageable cloud computing applications and solutions, in an end-to-end, multi-cloud environment, independent of choice of technology, run-time, programming language or tools made to develop the solutions.


E1860
94V-



6.

Monitoring


Software
as
a
Service
Platform
as
a
Service
Infrastructure
as
a
Service

Set of parameters of cloud computing for monitoring

Recommendation ITU-T Q.3914

(01/2018)

SERIES Q: SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

Summary

In accordance with the functional reference architecture of cloud computing that was defined in Recommendation ITU-T Y.3502, Recommendation ITU-T Q.3914 specifies the functional reference architecture of cloud computing according to Recommendation ITU-T Y.3500. This Recommendation provides a set of parameters that indicate the status and event of a cloud computing system, including resource layer, service layer and access layer.

Keywords

Cloud computing, monitoring, parameter.

Table of Contents

1 Scope

This Recommendation specifies the functional reference architecture of cloud computing according to [ITU-T Y.3500], in accordance with the functional reference architecture of cloud computing that was defined in [ITU-T Y.3502].

This Recommendation specifies parameters that should be monitored for the status identification of resource, service and management within a cloud system.

The parameters specified in this Recommendation include:

– monitoring parameters of the resource layer;

– monitoring parameters of the service layer;

– monitoring parameters of the access layer.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and Vocabulary*.

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014) | ISO/IEC 17789:2014, *Information technology – Cloud computing – Reference architecture.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 cloud computing [ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

3.1.2 cloud service [ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.3 cloud service provider [ITU-T Y.3500]: Party which makes cloud services available.

3.1.4 functional component [ITU-T Y.3502]: A functional building block needed to engage in an activity, backed by an implementation.

3.1.5 product catalogue [ITU-T Y.3502]: A listing of all the cloud service products which cloud service providers make available to cloud service customers.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 cloud service user: Natural person or entity acting on their behalf, associated with a cloud service customer that uses cloud services.

NOTE – This definition is paraphrased from clause 8.2.1.1 of [ITU-T Y.3502].

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CPU	Central Processing Unit
GPU	Graphics Processing Unit
IaaS	Infrastructure as a Service
I/O	Input/Output
IP	Internet Protocol
KPI	Key Performance Indicator
MDT	Mean Down Time
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
NF	Network Function
NFS	Network Function Status
OSS	Operational Support System
PaaS	Platform as a Service
QoS	Quality of Service
RAM	Random Access Memory
SC	Service Chain
SDN	Software-Defined Networking
SLA	Service Level Agreement
TCP	Transmission Control Protocol
TBF	Time Between Failures
TTR	Time To Repair
UPS	Uninterruptible Power System
URL	Uniform Resource Locator
VIP	Virtual Internet Protocol
VM	Virtual Machine

5 Conventions

None.

6 Functional reference architecture of cloud computing

The layering framework used in the cloud computing reference architecture has four layers, plus a set of functions that spans across the layers. The four layers are:

– user layer;
– access layer;
– services layer;
– resources layer.

The functions that span layers are called multilayer functions.

The layering framework is shown schematically in Figure 6-1.

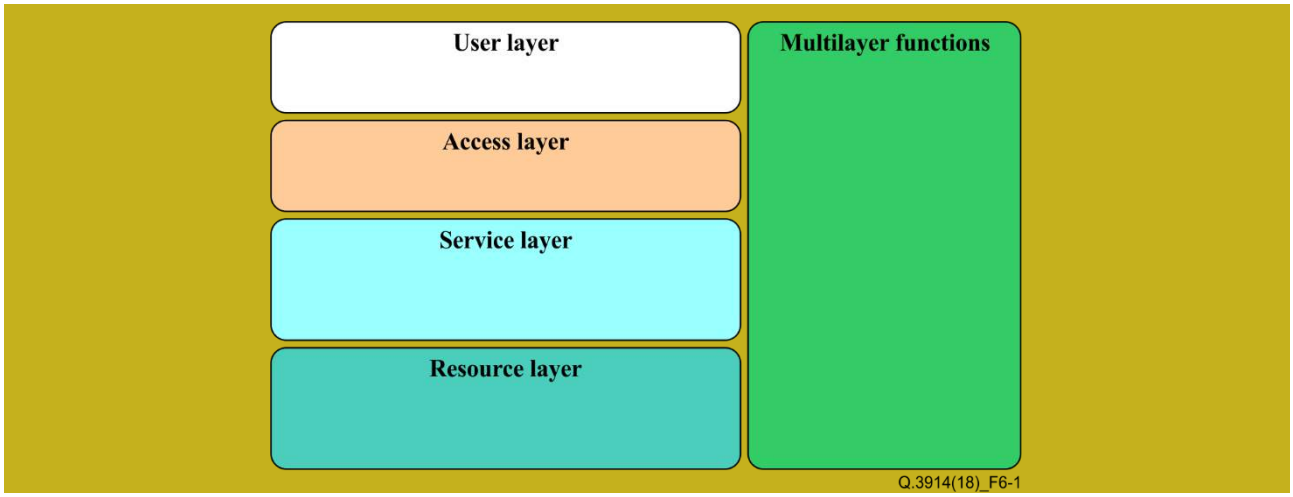


Figure 6-1 – Cloud computing layering framework

The function of each layer in the framework is described in clause 9.2.1 of [ITU-T Y.3502].

Figure 6-2 presents a high-level overview of the cloud computing reference architecture functional components organized by means of the layering framework.

The relevant monitoring functional components are as follows.

– Resource abstraction and control functional component: the resource abstraction and control functional component which resides in the resources layer enables control functionality, enabling monitoring and management capabilities implemented in the operational support systems functional component.

Monitoring and reporting functional component: the monitoring and reporting functional component that is one of the multilayer operational support systems provides capabilities for the following.

– Monitoring the activities of other functional components throughout the cloud provider's system. This includes the functional components that are involved in the direct use of cloud services by customer cloud service users such as service access and service implementation (e.g., the invocation of cloud service operation by a particular user). This also includes functional components involved in the support of cloud services, such as functional components in the operational support system (OSS) itself, like the service automation functional component (e.g., the provisioning of a service instance for a particular customer).
– Providing reports on the behaviour of the cloud service provider's system, which may take the form of alerts for behaviour that has a time-sensitive aspect (e.g., the occurrence of a fault, the completion of some task) or may take the form of aggregated forms of historical data (e.g., service usage data).
– Storage and retrieval of monitoring and event data as logging records.

Service level management functional component: the service level management functional component, which also resides in the operational support systems, obtains monitoring information from the monitoring and reporting functional component in order to measure and record key performance indicators (KPIs) for the cloud service. Capacity is allocated or de-allocated based on the basis of these KPIs.

The details of the functional components are described in clause 9.2 of [ITU-T Y.3502].

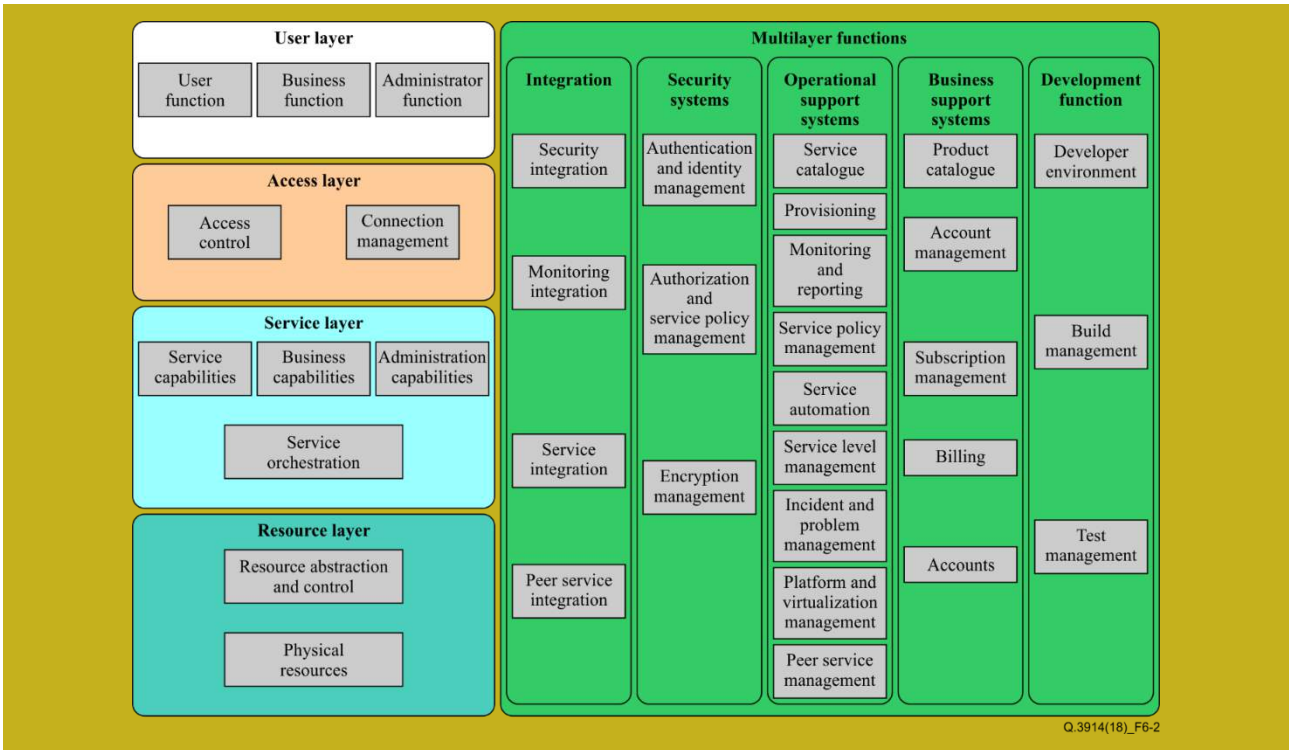


Figure 6-2 – Functional components of the cloud computing reference architecture

7 Monitoring parameters

Monitoring cloud resources and services is a key tool that helps cloud computing providers and consumers in designing, building and improving a cloud system, eliminating performance bottlenecks and identifying security flaws. Applications (e.g., streaming, web, indexing, compute and storage services) are distributed across cloud layers including platform as a service (PaaS) and infrastructure as a service (IaaS). In consequence, all parameters performed across all layers of the cloud stack need to be metered and monitored. These include not only cloud resource and network access, but also deployed services and applications.

7.1 Resource layer parameters

The resources layer is where the physical and virtual resources, as well as generic software, reside. This layer includes equipment typically used in a data centre such as servers, networking switches and routers, storage devices, in addition to the corresponding non-cloud specific software that runs on the servers and other equipment such as host operating systems, hypervisors, device drivers and generic systems management software.

7.1.1 Physical computing resources

Physical computing resources include any hardware within a computer system for running an operating system and software. An IaaS administrator can add physical computing resources to or remove physical computing resources from a virtual machine (VM).

In order to ensure that the deployed software and hardware resources run at the required level to satisfy the service level agreement (SLA), a continuous physical resource monitoring process is desirable.

Processors, memory and disks are basic computing and storage resources. Monitoring these resources can detect system failures or corruption before they become completely non-recoverable. So, monitoring functions and status of these resources to ensure system availability benefits users.

See Table 7-1.

Table 7-1 – Parameters collected to monitor physical computing resources

Metric name	Description	Unit
Central processing unit (CPU) frequency	CPU frequency	MHz
CPU util	Average CPU utilization	%
CPU idle time	Time of CPU is in idle status	ns
CPU load	CPUs have been loaded	process
CPU input/output (I/O) wait time	CPU I/O wait time	ns
CPU idle percent	Percent of CPU is in idle status	%
CPU user percent	Percent of CPU is in using status	%
CPU I/O wait percent	Percent of CPU I/O is in waiting status	%
memory	Volume of random access memory (RAM)	MB
memory util	Average RAM utilization	%
memory used	Used physical memory size	kB
disk size	Total size of disk	GB or TB
disk size used	Total size of disk used	GB or TB
disk random/sequential read requests	Volume of read requests	request
disk random/sequential read request rate	Average rate of read requests	request/s
disk random/sequential read delay	Average delay of read request	ms
disk random/sequential read error	Volume of read error	kB
disk random/sequential write requests	Volume of write requests	request
disk random/sequential write request rate	Average rate of write requests	request/s
disk random/sequential write delay	Average delay of write request	ms
disk random/sequential write error	Volume of write error	kB
disk random/sequential read bytes	Volume of reads	MB
disk random/sequential read byte rate	Average rate of reads	MB/s
disk random/sequential write bytes	Volume of writes	MB
disk random/sequential write byte rate	Average rate of writes	MB/s
Graphics processing unit (GPU) util	Average GPU utilization	%
GPU idle time	Time of GPU is in idle status	ns
GPU load	GPUs have been loaded	process
GPU I/O wait time	GPU I/O wait time	ns
GPU idle percent	Percent of GPU is in idle status	%
GPU user percent	Percent of GPU is in using status	%
GPU I/O wait percent	Percent of GPU I/O is in waiting status	%
NOTE – All metrics should be measured over different durations, e.g., 1 min, 5 min, 15 min or 30 min.		

7.1.2 Virtual computing resources

Virtual computing resources include any virtual component within a virtual computer system for running an operating system, software and applications. Similarly to physical computing resources, running data and status of resources from VMs in which the applications are currently running require collection. These data provide a picture of how much of the VM is being utilized and helps in analysis and determination of the scaling requirement of applications.

See Table 7-2.

Table 7-2 – Parameters collected to monitor virtual computing resources

Metric name	Description	Unit
vCPUs	Number of virtual CPUs allocated to the virtual machine (VM)	CPU
vCPU idle time	Time of virtual CPUs is in idle status	ns
vCPU idle percent	Percent of vCPU is in idle status	%
vCPU user percent	Percent of vCPU is in using status	%
vCPU load	Virtual CPUs have been loaded	process
vCPU I/O wait time	Time of virtual CPUs I/O is in waiting status	ns
vCPU I/O wait percent	Percent of virtual CPU is in using status	%
vMemory	Volume of virtual RAM allocated to the VM	MB
vMemory utilization	Average virtual RAM utilization	%
vMemory used	Used virtual memory size	MB
vDisk size	Total size of virtual disk allocated to the VM	GB
vDisk size used	Total size of virtual disk used	MB
vDisk random/sequential read requests	Number of read requests of virtual disk	request
vDisk random/sequential read request rate	Average rate of read requests of virtual disk	request/s
vDisk random/sequential write requests	Number of write requests of virtual disk	request
vDisk random/sequential write request rate	Average rate of write requests of virtual disk	request/s
vDisk random/sequential read bytes	Volume of reads of virtual disk	kB
vDisk random/sequential read byte rate	Average rate of reads of virtual disk	kB/s
vDisk random/sequential read delay	Average delay of read request	ms
vDisk random/sequential read error	Volume of read error	kB
vDisk random/sequential write bytes	Volume of writes of virtual disk	kB
VDisk random/sequential write byte rate	Average rate of writes of virtual disk	kB/s
vDisk random/sequential write delay	Average delay of write request	ms
vDisk random/sequential write error	Volume of write error	kB
vGPU util	Average vGPU utilization	%
vGPU idle time	Time of vGPU is in idle status	ns
vGPU load	vGPUs have been loaded	process
vGPU I/O wait time	vGPU I/O wait time	ns
vGPU idle percent	Percent of vGPU is in idle status	%
vGPU user percent	Percent of vGPU is in using status	%
vGPU I/O wait percent	Percent of vGPU I/O is in waiting status	%
NOTE – All metrics should be measured over different duration, e.g., 1 min, 5 min, 15 min or 30 min.		

7.1.3 Virtual machine operation and control

VM operation and control are referred to the management of physical or virtual computing resources that allow users to create, edit, start and stop VMs.

The impetus behind cloud computing is the ever-increasing demand to manage growth and increase computing flexibility by dynamic resource operation and control based on demand. An example of resource control operation could be to horizontally scale a database server by migrating it from a small CPU resource configuration to an extra-large CPU resource to improve throughput. This basic requirement of cloud computing is supported by the resource operation and control system. An inefficient resource operation and control system has a direct negative effect on performance. It can also indirectly affect system functionality. Some system functions provided might become ineffective due to poor performance.

See Table 7-3.

Table 7-3 – Parameters collected to monitor VM operation and control

Metric name	Description	Unit
CPU of VM start	Time of CPU start	s
CPU of VM stop	Time of CPU stop	s
CPU of VM restart	Time of CPU restart	s
CPU of VM select	Time of CPU select	s
CPU of VM scale down	Time of CPU scale down	s
CPU of VM scale up	Time of CPU scale up	s
VM start	Time of VM start	s
VM acquisition	Time of VM acquisition	s
VM release	Time of VM release	s
memory of VM scale down	Time of memory scale down	s
memory of VM scale up	Time of memory scale up	s
disk of VM scale down	Time of disk scale down	s
disk of VM scale up	Time of disk scale up	s
upload file	Time of upload file	s
download file	Time of download file	s
allocation Internet protocol (IP)	Time of allocation IP	s
allocation ports	Time of allocation ports	s
allocation URL	Time of allocation uniform resource locator (URL)	s
VM live migration	Time that is needed to move a VM from two predefined resources	s
migration Interruption Time	Maximum time in which a customer has no access to migration to the resource	s
VM cloning	Time of VM cloning	s
VM backup	Time of VM backup	s
VM imaging	Time of VM imaging	s
recovery time	Time from the failure of a storage, to the successful restore from an existing backup	s
NOTE – VM backup time interval varies according to backup type, e.g., full backup or incremental backup.		

7.1.4 Network

High-performance computing requires large amounts of network bandwidth. Particularly for cloud computing, the network has a strong meaning, as all provided resources and services are available through a network. It has been found that poor network performance is caused by virtualization I/O overhead. A network monitoring system helps in realization of traffic, utilization and errors and then, based on accurate monitoring information, quality of service (QoS) policy validation, network outage resolution, performance problem troubleshooting, and in making important capacity planning decisions.

See Table 7-4.

Table 7-4 – Parameters collected to monitor a network

Metric name	Description	Unit
incoming bytes	Number of bytes received by network interface	KB
incoming byte rate	Average rate of bytes received by network interface per second	KB/s
maximum incoming byte rate	Maximum incoming byte rate during a specific period (5 minute/15 minutes/60 minutes)	KB/s
outgoing bytes	Number of bytes sent by network interface	KB
outgoing byte rate	Average rate of bytes sent by network per second	KB/s
maximum outgoing byte rate	Maximum outgoing byte rate (5 minute/15 minutes/ 60 minutes)	KB/s
incoming packets	Number of incoming packets	packet
incoming packet rate	Average rate of incoming packets per second	packet/s
average packets size incoming	Average packets size incoming (1 minute/5 minutes/ 15 minutes)	byte
outgoing packets	Number of outgoing packets	packet
outgoing packet rate	Average rate of outgoing packets per second	packet /s
average packets size outgoing	Average packets size outgoing (1 minute/5 minutes/ 15 minutes)	byte
outgoing errors	Sending error of network interface	packet
bandwidth of incoming	Total capacity of the connection of the incoming	Mb
utilization of incoming interface	Percentage of incoming byte rate with respect to bandwidth of incoming.	%
bandwidth of outgoing	Total capacity of the connection of the outgoing	Mb/s
utilization of outgoing interface	Percentage of outgoing byte rate with respect to bandwidth of outgoing link.	%
average latency	Average of delay of data transition	ms
Minimum latency	Minimum time interval between submitting a packet and arrival at its destination	ms
Maximum latency	Maximum time interval between submitting a packet and arrival at its destination	ms
packet loss	Percentage of packets lost with respect to packets sent.	%
jitter	The difference in end-to-end one-way delay	ms

7.1.5 Software-defined networking

Software-defined networking (SDN) is a concept that enables network operators and data centres to flexibly manage their networking equipment using software. SDN introduces new levels of flexibility and automation without manual interaction for networking.

7.1.5.1 Software-defined networking-based network

Network setup in SDN is now separated from a network engineer's regular activities; network issue troubleshooting and diagnosis have become more complex. The availability, performance, utilization and capacity of SDN monitoring can enable a cloud computing provider more confidently to adopt SDN in cloud computing.

See Table 7-5

Table 7-5 – Parameters collected to monitor a software-defined networking controller

Metric name	Description	Unit
latency of topology discovery	Latency of topology discovery	ms
latency of connection from switch to controller	Latency of connection from switch to controller	ms
number of active switches	Number of active switches	switch
incoming packets of the same source addresses	Numbers of incoming packets with the same incoming source addresses	packet
incoming packets of the same destination addresses	Numbers of incoming packets with the same incoming destination addresses	packet
outgoing packets of the same source addresses	Numbers of outgoing packets with the same outgoing source addresses	packet
outgoing packets of destination addresses	Numbers of outgoing packets with the same outgoing destination addresses	packet
incoming packets of the same source port	Numbers of incoming packets with the same incoming source port numbers	packet
incoming packets of the same destination port	Numbers of incoming packets with the same incoming destination port number	packet
outgoing packets of the same source port	Numbers of outgoing packets with the same outgoing source port numbers	packet
outgoing packets of the same destination port	Numbers of outgoing packets with the same outgoing destination port numbers	packet

7.1.5.2 Service chain

Cloud computing provides not only computing and storage resources to consumers as a resource pool, but also as a network resource pool. According to appointed service logic, network traffic passes though several service points (generally reference is made to firewall, load balance or any other network functions (NFs)). A service chain (SC) links these service points together. A cloud computing provider should consider the ’performance and status of an SC when it provides service to consumers.

See Table 7-6.

Table 7-6 – Parameters collected to monitor a service chain

Metric name	Description	Unit
NFS	Network function status	normal/fail
NF start	Time of network function start	s
NF stop	Time of network function stop	s
NF migration	Time that is needed to move a NF from two predefined resources	s
SC start	Time of a service chain established	s
SC stop	Time of a service chain destroy	s

7.1.6 Energy consumption

Voltage or power use out of the permissible range can damage electrical components or cause system failure. If the fan stops working, the server overheats, is damaged and goes out of service. So, it is important to monitor the voltage or wattage, fan and temperature to ensure that they are within safe operating limits.

In order to handle massive amounts of data generated by consumers and businesses, cloud computing typically needs a lot of power. A sharp increase in energy consumption can indicate server load unbalance that leads to performance degradation. Real-time monitoring is helpful for avoiding these consequences. Different states of the physical or VMs require different power levels. These states can normally be divided into six types: named as shutdown, work, idle, dormant, sleep and standby.

See Table 7-7.

Table 7-7 – Parameters collected to monitor energy consumption in each state

Metric name	Description	Unit
power of CPU	Current power of CPU consumption	w
power of GPU	Current power of GPU consumption	w
power of Memory	Current power of Memory consumption	w
power of storage	Current power of storage consumption	w
power of network	Current power of disk consumption	w
power of power Systems	Current power of power system consumption	w
temperature of CPU	Current temperature of CPU	°C

7.1.7 Environment

The server room environment requires strict control processes for temperature, humidity and power supply. A fully automated monitoring system can help prevent overheating of servers and condensation on equipment. Keeping temperatures within range and carefully monitoring humidity to prevent corrosion or static electricity reduce energy consumption and keep servers running smoothly. Voltage use out of the permissible range can damage electrical components or cause system failure. If the fan stops working, the server overheats, is damaged and goes out of service. So, it is important to monitor the voltage or wattage, fan and temperature to ensure that they are within safe operating limits.

See Table 7-8.

Table 7-8 – Parameters collected for the monitoring environment

Metric name	Description	Unit
temperature	Current temperature of server room	°C
voltage	Current voltage of electricity supply	V
electric current	Electric current of electricity supply	A
UPS voltage	Output voltage of an uninterruptible power system (UPS) battery	V
UPS output electric current	Output electric current of UPS battery	A
UPS charging electric current	Electric current of charging	A
humidity	Relative humidity of server room	%
fan rotations	Fan rotations per minute	rotations/min
power of fan	Current power of fan consumption	W

7.2 Service layer parameters

7.2.1 General

One of the most important areas for provider and consumer is service performance and availability when it comes to cloud computing. Cloud service provider and consumer need to get an entire view of the health of service. A lot of decision making and SLA determination are driven by service performance and availability. The monitoring system should report the service performance and availability parameters to identify whether the QoS specified in the SLA is fulfilled.

Different cloud services can be offered with different terminologies, specifications and features. Cloud services can achieve different levels of performance under various workloads generated by diverse applications. For example, unlike computation and communication-intensive applications, performance of data-intensive applications typically will be strongly affected by I/O performance and storage access in a cloud infrastructure. The monitoring parameters of typical services are included in this clause. Others are for further study.

See Table 7-9.

Table 7-9 – Performance metrics for monitoring general cloud services

Category	Metric name	Description
Availability	MTBF	Mean time between failures
	MTTR	Mean time to repair
Performance	Response time	Response time for composite or atomic service
	Throughput	Number of transactions or requests processed per specified unit of time
Capacity	Bandwidth	Bandwidth of the connection that supports a service
	Storage capacity	Capacity of a temporary or persistent storage medium, such as RAM, disk or tape

7.2.2 Service availability

Service availability is the property of being accessible and usable upon demand by an authorized entity. Continuity is the key feature used to measure service availability, which ensures the service is available for a certain amount of time without any interruption. Furthermore, if there is an incident, continuity enables the service to be restarted and access to data and functionality of the service regained within a particular period. All elements, including computing, storage, network and power supplement, can affect service continuity. For example, for a public-cloud end user, availability of the cloud not only refers to the services provided by the cloud service provider, but also to the possibility of accessing those services remotely.

See Table 7-10.

Table 7-10 – Parameters collected for monitoring service availability

Metric name	Description	Unit
mean time between failures (MTBF)	Time between inherent failures of element or service during operation	h
maximum TBF	Maximum time between failures	h
minimum TBF	Minimum time between failures	h
mean time to repair (MTTR)	The average time repair a failed element or service	h
maximum TTR	Maximum time to repair	h
minimum TTR	Minimum time to repair	h
mean down time (MDT)	The average time that an element or service is non-operational. This includes all downtime associated with repair	h
maximum down time	Maximum time of down	h
minimum down time	Minimum time of down	h

7.2.3 Service performance

7.2.3.1 Transaction process

Transaction process metrics can give a clear picture of the performance of an application in a cloud, such as response time to complete service requests and transaction rate at which service requests are executed. Latency for service requests, which calculates the time taken for the application to respond to user requests, is the key metric.

See Table 7-11.

Table 7-11 – Parameters collected for monitoring the transaction process

Metric name	Description	Unit
transactions	Number of transactions during a period (1 min, 5 min, 15 min)	transaction
transaction rate	Transaction rate at which service requests are executed per second	transaction/s
errors	Number of error transactions	transaction
concurrent transactions	Average number of new transactions processed simultaneously	transaction
time per transactions	Average time necessary to process a single transactions item	ms
disk throughput rate	Throughput rate (input and output) for a specific service	kB/s
memory throughput rate	Throughput rate (input and output) for a specific service	kB/s
delay	Delay of message passing between processes	ms
time of task	Duration of specific predefined tasks	ms

7.2.3.2 Load balance

Load balancing of cloud computing is the process of distributing workloads across multiple computing resources, which provides an efficient solution to various issues residing in cloud computing environment usage.

See Table 7-12.

Table 7-12 – Parameters collected for monitoring the efficiency and effectiveness of load balancing

Metric name	Description	Unit
load balance pool	Number of load balance pools	pool
load balance VIPs	Number of virtual internet protocol (VIP) addresses	member
load balance member	Number of load balance member	member
load balance health monitor	Number of Load balance health monitor	monitor
load balance connections	Volume of Load balance connections	connection
load balance active connections	Volume of Load balance active connections	connection
load balance incoming bytes	Volume of Load balance incoming bytes	MB
load balance outgoing bytes	Volume of Load balance outgoing bytes	MB

7.2.3.3 Database

A cloud database is a database that typically runs on a cloud computing platform. Poor database performance can dramatically degrade QoS. Cloud providers who offer database as a service, without physically launching a VM instance for the database, should have a clear picture of how a database is running and what is needed by consumers.

A relational database is organized based on the relational model of the data. A non-relational database provides a mechanism for storage and retrieval of data that is modelled by means other than the tabular relations used in relational databases. Non-relational databases are increasingly used in big data and real-time web applications. The operation mechanisms of the two types of databases are entirely different. So relational and non-relational databases should be monitored separately.

See Table 7-13.

Table 7-13 – Parameters collected for monitoring database efficiency

Metric name	Description	Unit
space	Total space of DB	kB
space used	Total space used of DB	kB
queries	Total number of DB queries (select, insert, update, delete, replace)	query
replace request	Volume of replace requests	request
replace request rate	Average rate of replace requests per second	request/s
response time of replace request	Average time of responding replace request	ms
insert/set request	Volume of insert/set requests	request
insert/set request rate	Average rate insert/set request of per second	request/s
response time of insert/set request	Average time of responding insert/set request	ms
update request	Volume of update requests	request
update request rate	Average rate of update requests per second	request/s
response time of update request	Average time of responding update request	ms
delete request	Volume of delete requests	request
delete request rate	Average rate of delete requests per second	request/s
response time of delete request	Average time of responding delete request	ms
select/get request	Volume of select requests	request
select/get request rate	Average rate of select requests per second	request/s
response time of select/get request	Average time of responding select/get request	ms
connect	Connection number of concurrent clients	request
connect rate	Average rate of connections per second	request/s
slow/expired query	Volume of slow/expired queries	query
slow/expired query rate	Average rate of slow/expired queries per second	request/s

7.2.3.4 Web service performance

The main function of the web server is to provide an online information browsing service. There are three types of performance parameter for web service: throughput, concurrent transactions and response time.

See Table 7-14.

Table 7-14 – Parameters collected for monitoring web service performance

Metric name	Description	Unit
throughput	Number of service request that a web service can complete in a given period of time	request/s
users	Number of new connection users servicing per second	user/s
transactions per second	Average number of transactions processed per second	transaction/s
connection rate	Number of new transmission control protocol (TCP) connections setting up per second	link/s
response time	The time duration from receiving the request to the web service to sending the response from the web service	ms
round trip time	Time from sending SYN to receiving SYN ACK	ms
TCP setting up time	Average time of TCP link setting up	
simultaneous connections	Number of TCP connections setting up between client and server	link/s
cumulative transactions	Total number of transactions processing processed	transaction

7.3 Access layer parameters

Principally, access control involves the authentication of a user through the presentation and validation of credentials, followed by the authorization of this authenticated user to use specific services. Associated with this is identity management. Access behaviour and management events should be monitored for the access layer.

See Table 7-15.

Table 7-15 – Parameters collected for monitoring the access layer

Metric name	Description	Unit
account entries	Number of successful account logon events	event
unsuccessful account entries	Number of unsuccessful account logon events	event
account exits	Number of account logout events	event
create account	Number of successful account creation events	event
modify account	Number of successful account modification events	event
delete account	Number of successful account deletion events	event
unsuccessful account management	Number of unsuccessful account management events	event
policy change	Number of successful policy change events	event
unsuccessful policy change	Number of unsuccessful policy change events	event
data deletions	Number of successful data deletion events	event
unsuccessful data deletions	Number of unsuccessful data deletion events	event
data access	Number of successful data access events	event
unsuccessful data access	Number of unsuccessful data access events	event
data changes	Number of successful data changes events	event
unsuccessful data changes	Number of unsuccessful data change events	event
unauthorized access,	Number of unauthorized service access events	event
unauthorized modification	Number of unauthorized service modification events	event
unauthorized deletion	Number of unauthorized service deletion events	event

7.

Security

Security framework for cloud computing

Recommendation ITU-T X.1601

(10/2015)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Summary

Recommendation ITU-T X.1601 describes the security framework for cloud computing. The Recommendation analyses security threats and challenges in the cloud computing environment, and describes security capabilities that could mitigate these threats and address security challenges. A framework methodology is provided for determining which of these security capabilities will require specification for mitigating security threats and addressing security challenges for cloud computing. Appendix I provides a mapping table on how a particular security threat or challenge is addressed by one or more corresponding security capabilities.

Keywords

Cloud computing, confidentiality, data protection, security capabilities, security challenges, security framework, security threats.

Table of Contents

1 Scope

This Recommendation analyses security threats and challenges in the cloud computing environment, and describes security capabilities that could mitigate these threats and address security challenges. A framework methodology is provided for determining which of these security capabilities will require specification for mitigating security threats and addressing security challenges for cloud computing.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 **authentication** [b-NIST-SP-800-53]: Verification of the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

3.1.2 **capability** [b-ISO/IEC 19440]: Quality of being able to perform a given activity.

3.1.3 **cloud computing** [b-ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

3.1.4 **cloud service** [b-ITU-T Y.3500]: One or more capabilities offered via cloud computing (3.1.3) invoked using a defined interface.

3.1.5 **cloud service customer** [b-ITU-T Y.3500]: Party (3.1.17) which is in a business relationship for the purpose of using cloud services (3.1.4).

NOTE – A business relationship does not necessarily imply financial agreements.

3.1.6 **cloud service partner** [b-ITU-T Y.3500]: Party (3.1.17) which is engaged in support of, or auxiliary to, activities of either the cloud service provider (3.1.7) or the cloud service customer (3.1.5), or both.

3.1.7 **cloud service provider** [b-ITU-T Y.3500]: Party (3.1.17) which makes cloud services (3.1.4) available.

3.1.8 **cloud service user** [b-ITU-T Y.3500]: Natural person, or entity acting on their behalf, associated with a cloud service customer (3.1.5) that uses cloud services (3.1.4).

NOTE – Examples of such entities include devices and applications.

3.1.9 **Communications as a Service (CaaS)** [b-ITU-T Y.3500]: Cloud service category in which the capability provided to the cloud service customer (3.1.5) is real time interaction and collaboration.

NOTE – CaaS can provide both application capabilities type and platform capabilities type.

3.1.10 **community cloud** [b-ITU-T Y.3500]: Cloud deployment model where cloud services (3.1.4) exclusively support and are shared by a specific collection of cloud service customers (3.1.5) who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection.

3.1.11 **data controller** [b-key definition]: A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

3.1.12 **data processor** [b-key definition]: In relation to personal data, this means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

3.1.13 hypervisor [b-NIST-SP-800-125]: The virtualization component that manages the guest OSs on a host and controls the flow of instructions between the guest OSs and the physical hardware.

3.1.14 Infrastructure as a Service (IaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer (3.1.5) is an infrastructure capabilities type.

NOTE – The cloud service customer (3.1.5) does not manage or control the underlying physical and virtual resources, but does have control over operating systems, storage, and deployed applications that use the physical and virtual resources. The cloud service customer (3.1.5) may also have limited ability to control certain networking components (e.g., host firewalls).

3.1.15 multi-tenancy [b-ITU-T Y.3500]: Allocation of physical or virtual resources such that multiple tenants (3.1.26) and their computations and data are isolated from and inaccessible to one another.

3.1.16 Network as a Service (NaaS) [b-ITU-T Y.3500**]**: Cloud service category in which the capability provided to the cloud service customer (3.1.5) is transport connectivity and related network capabilities.

NOTE – NaaS can provide any of the three cloud capabilities types.

3.1.17 party [b- ISO/IEC 27729**]**: Natural person or legal person, whether or not incorporated, or a group of either.

3.1.18 personally identifiable information [b-ISO/IEC 29100]: Any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal.

3.1.19 Platform as a Service (PaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer (3.1.5) is a platform capabilities type.

3.1.20 private cloud [b-ITU-T Y.3500**]**: Cloud deployment model where cloud services (3.1.4) are used exclusively by a single cloud service customer (3.1.5) and resources are controlled by that cloud service customer (3.1.5).

3.1.21 public cloud [b-ITU-T Y.3500]: Cloud deployment model where cloud services (3.1.4) are potentially available to any cloud service customer (3.1.5) and resources are controlled by the cloud service provider (3.1.7).

3.1.22 security domain [b-ITU-T X.810]: A set of elements, a security policy, a security authority and a set of security-relevant activities in which the set of elements are subject to the security policy for the specified activities, and the security policy is administered by the security authority for the security domain.

3.1.23 security incident [b-ITU-T E.409]: A security incident is any adverse event whereby some aspect of security could be threatened.

3.1.24 service level agreement (SLA) [b-ISO/IEC 20000-1]: A documented agreement between the service provider and customer that identifies services and service targets.

NOTE 1 – A service level agreement can also be established between the service provider and a supplier, an internal group or a customer acting as a supplier.

NOTE 2 – A service level agreement can be included in a contract or another type of documented agreement.

3.1.25 Software as a Service (SaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer (3.1.5) is an application capabilities type.

3.1.26 tenant [b-ITU-T Y.3500]: One or more cloud service users (3.1.8) sharing access to a set of physical and virtual resources.

3.1.27 threat [b-ISO/IEC 27000]: A potential cause of an unwanted incident, which may result in harm to a system or organization.

3.1.28 virtual machine (VM) [b-NIST-SP-800-145]: An efficient, isolated, logical duplicate of a real machine.

3.1.29 vulnerability [b-NIST-SP-800-30]: A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 security challenge: A security "difficulty" other than a direct security threat arising from the nature and operating environment of cloud services, including "indirect" threats. See clauses 7 and 8.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API Application Programming Interface

BCP Business Continuity Plan

CaaS Communications as a Service

CPU Central Processing Unit

CSC Cloud Service Customer

CSN Cloud Service Partner

CSP Cloud Service Provider

CSU Cloud Service User

DNS Domain Name System

IaaS Infrastructure as a Service

IAM Identity and Access Management

ICT Information and Communication Technology

IP Internet Protocol

IT Information Technology

NaaS Network as a Service

OS Operating System

PaaS Platform as a Service

PII Personally Identifiable Information

PKI Public Key Infrastructure

SaaS Software as a Service

SIM Subscriber Identity Module

SLA Service Level Agreement

VM Virtual Machine

5 Conventions

None.

6 Overview

Cloud computing is a paradigm for enabling convenient, on-demand network access to a shared pool of configurable resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing customers can use these resources to develop, host and run services and applications on demand in a flexible manner in any device, anytime and anywhere in the cloud computing environment. Cloud computing services

are usually delivered in certain service categories, e.g., infrastructure as a service (IaaS), platform as a service (PaaS), software as a service (SaaS), network as a service (NaaS), and many others. These service categories enable cloud computing customers to launch or change their business quickly and easily without establishing new information and communication technology (ICT) infrastructure and systems and provide opportunities to provision resources elastically, as needed. For example, some cloud service providers (CSPs) might provide abstracted hardware and software resources which may be offered as a service (e.g., IaaS or NaaS). Other cloud service providers may provide cloud specific platforms (PaaS) or applications (SaaS) to enable customers and partners to rapidly develop and deploy new applications which can be configured and used remotely.

There are security threats and challenges in adopting cloud computing, and security requirements vary to a great extent for different cloud computing service deployment models and service categories. The distributed and multi-tenant nature of cloud computing, the prevalence of remote access to cloud computing services and the number of entities involved in each process make cloud computing inherently more vulnerable to both internal and external security threats than other paradigms. Many of the security threats can be mitigated with the application of traditional security processes and mechanisms. Security touches upon and impacts many parts of a cloud computing service. Therefore, the security management of the cloud computing services, as well as the associated resources, is a critical aspect of cloud computing.

Before the migration of the ICT system to cloud computing, a potential cloud service customer (CSC) should identify their security threats (see clause 7 below) and security challenges (see clause 8).

Based on these threats and challenges, a set of high-level security capabilities (see clause 9) are identified. Specific requirements for these capabilities are out of the scope of this Recommendation, but they will need to be identified for specific implementations of cloud computing services, based on risk assessment against the identified threats and challenges.

Based on the risk assessment, a CSC can determine whether to adopt cloud computing, and can make informed decisions over service providers and architecture. The above risk assessment should be performed by using an information security risk management framework (e.g., the risk management framework defined in [b-ISO/IEC 27005]). See also clause 10 below for a suggested framework methodology.

This Recommendation distinguishes between security threats and security challenges. Security threats are those associated with attacks (both active and passive), and also environmental failures or disasters. Security challenges comprise difficulties arising from the nature and operating environment of cloud services. When not properly addressed, security challenges may leave doors open for threats.

Based on these identified security threats and challenges, the security capabilities are described to mitigate security threats and address security challenges for cloud computing.

7 Security threats for cloud computing

Threats have the potential to harm assets such as information, processes and systems and therefore organizations. Threats may be of a natural or human origin, and could be accidental or deliberate. A threat may arise from within or from outside the organization. Threats can be classified as accidental or intentional and may be active or passive.

The specific threats encountered are highly dependent on the chosen specific cloud service. For example, for a public cloud, threats can arise from the split responsibilities between the CSC and CSP: complexities of specifying jurisdiction over data and processes, consistency and adequacy of data protection, and maintenance of confidentiality, etc. However, for a private cloud, the threats are simpler to address because the CSC controls all the tenants hosted by the CSP. Even though some of the threats identified in this Recommendation are also covered by existing industry documents (e.g., Recommendation ITU-T X.800), all the threats are relevant to cloud computing. The applicability of individual threats will depend on the specific cloud service.

This clause describes the various security threats that can arise in a cloud computing environment.

7.1 Security threats for cloud service customers (CSCs)

The following threats are those that directly affect CSCs. They may affect the CSCs' personal or business interests, confidentiality, lawfulness or safety. Not all CSCs will be at risk by all threats. The risk will be unequal depending on the nature of the CSC and of the cloud computing service being used. For example, a cloud service specific to the transcoding of commercial video files has no requirements to protect personally identifiable information (PII), but will have strong requirements around the protection of digital assets.

7.1.1 Data loss and leakage

As the cloud service environment is typically a multi-tenant one, loss or leakage of data is a serious threat to the CSC. A lack of appropriate management of cryptographic information, such as encryption keys, authentication codes and access privilege, could lead to significant damages, such as data loss and unexpected leakage to the outside. For example, insufficient authentication, authorization, and audit controls; inconsistent use of encryption and/or authentication keys; operational failures; disposal problems; jurisdiction and political issues; data centre reliability; and disaster recovery, can be recognized as major sources of this threat and may be associated with the challenges described in clauses 8.1.2 "Loss of trust", clause 8.1.3 "Loss of governance" and clause 8.1.4 "Loss of confidentiality".

7.1.2 Insecure service access

Identity credentials, including those of CSC administrators, are especially vulnerable to unauthorized users in the highly distributed environment of cloud computing, since unlike traditional telecommunications it is often difficult to rely on location (e.g., landline) or the presence of a specific hardware element (e.g., a mobile subscriber identity module (SIM)) to reinforce authentication of identity. As most of the service offerings are remote, unprotected connections expose potential vulnerability. Even when the connections are protected or local, other attack methods (such as phishing, fraud, social engineering and exploitation of software vulnerabilities) may also succeed. If an attacker gains access to users' or administrators' credentials, they can eavesdrop on activities and transactions, manipulate data, return falsified information, and redirect a CSC's clients to illegitimate sites. Passwords are often reused across multiple websites and services, which amplify the impact of such attacks since a single break can expose multiple services. Cloud computing solutions also add a new threat to the landscape. The CSC's account or service instances may become a new base for an attacker. From this point onwards, the attacker may leverage the power of the CSC's reputation and resources to launch subsequent attacks.

7.1.3 Insider threats

Where human beings are involved, there is always a risk of individuals acting in a manner that is not consistent with the security of the service. CSC employees sharing "administrator" passwords, or otherwise leaving credentials unsecure (e.g., written on notes stuck to a screen), careless or inadequately trained users (or family members in a consumer setting), or malicious actions by disgruntled employees will always pose a significant threat.

7.2 Security threats for cloud service providers (CSPs)

This clause identifies threats that directly affect CSPs. Such threats might affect the ability of a CSP to offer services, to do business, to retain customers, and to avoid legal or regulatory difficulties. Threats to a given CSP will also depend on their specific service offerings and environments.

7.2.1 Unauthorized administration access

The cloud computing service will include interfaces and software components that allow the CSC's own staff to administer those aspects of the cloud computing service that are under the CSC's control, such as the addition or removal of CSC employee accounts, connections to the CSC's own servers, changes to service capacity, updating the domain name system (DNS) entries and websites, etc. Such administrative interfaces can become a target of choice for attackers who impersonate the CSC's administrators to attack a CSP. Because such cloud computing services have to be accessible to the CSC's own staff, the protection of these services becomes a major concern for cloud computing security.

7.2.2 Insider threats

Where humans are involved, there is always a risk of individuals acting in a malicious or careless manner that puts the security of the service at risk.

CSP employees sharing "administrator" passwords, or otherwise leaving credentials unsecure (e.g., written on notes stuck to a screen), careless or inadequately trained users, or malicious actions by disgruntled employees will always pose a significant threat to any business.

CSPs in particular need to seriously consider the trustworthiness of their own employees. Even with good screening of employees, there is always the risk of a skilled intruder successfully obtaining a position on the CSP's data centre staff. Such an intruder might be seeking to undermine the CSP itself, or may be intending to penetrate specific CSC systems that are being supported, especially if the CSC is a high-profile corporation or government agency.

8 Security challenges for cloud computing

Security challenges comprise difficulties other than security threats arising from the nature and operating environment of cloud services, including "indirect" threats. An indirect threat is where a threat to one participant of a cloud service may have adverse consequences for others.

The challenges identified in this Recommendation are the ones that when not properly addressed, may leave the door open to threats. These challenges need to be considered when considering cloud computing services.

8.1 Security challenges for cloud service customers (CSCs)

This clause describes security challenges associated with environmental difficulties or indirect threats that may give rise to more direct threats to the interests of the CSC.

8.1.1 Ambiguity in responsibility

CSCs consume delivered resources through different service categories and deployment models. The customer-built ICT system thus relies on these services. Any lack of a clear definition of responsibility among CSCs and CSPs may introduce conceptual and operational conflicts. Any contractual inconsistency of provided services could induce an anomaly or incidents. For example, the problem of which entity is the data controller and which one is the data processor may be unclear at an international scale, even if the international aspect is reduced to a minimal third party outside of a specific region such as the European Union.

Due to legal and regulatory requirements, any related doubt (e.g., whether a given CSC or CSP is a "data controller" or "data processor") may lead to ambiguity as to which set of regulations they are required to adhere to. If this interpretation varies in different jurisdictions, a given CSC or CSP could find themselves subject to conflicting regulations on the same service or portion of data.

8.1.2 Loss of trust

Sometimes, it is difficult for a CSC to recognize their CSP's trust level due to the black-box feature of the cloud computing service. If there are no means of obtaining and sharing the provider's security level in a formalized manner, CSCs have no means to evaluate the security implementation level achieved by the provider. Such a lack of sharing at the security level with regard to CSP could become a serious security threat for some CSCs in their use of cloud computing services.

8.1.3 Loss of governance

The decision by CSCs to migrate a part of their own ICT system to a cloud computing infrastructure implies giving partial control to a CSP. This could be a serious threat to a CSC's data, notably regarding the role and privilege assignment to the provider. Coupled with a lack of transparency regarding cloud computing provider practices, this may lead to misconfiguration, or even enable a malicious insider attack.

When adopting cloud computing services, some CSCs may have concerns over a lack of control over their information and assets hosted in CSPs, over data storage, reliability of data backup (data retention issues), countermeasures for business continuity plans (BCPs) and disaster recovery, etc.

For example:

- A CSC wishes to delete a file for legal reasons, but the CSP retains a copy that the CSC does not know about.
- A CSP gives the CSC's administrator privileges that go beyond the CSC's policy.
- Some CSCs may have concerns regarding the exposure of data by a CSP to foreign governments which could impact the CSC's compliance with confidentiality laws, such as the European Union data protection directives.

8.1.4 Loss of confidentiality

When a CSP processes confidential information, there is a possibility of there being a violation of confidentiality, which could also include a violation of applicable data protection regulations, certifications or laws. This includes the leakage of confidential information, or the processing of personally identifiable information (PII) for a purpose that is not authorized by the CSC and/or the data subject.

8.1.5 Service unavailability

Availability is not specific to the cloud computing environment. However, because of the service-oriented design principle, service delivery may be impacted when upstream cloud computing services are not completely available. Moreover, the dynamic dependency of cloud computing offers more possibilities to an attacker. For example, a denial-of-service attack on one upstream service may affect multiple downstream services in the same cloud computing system.

8.1.6 Cloud service provider lock-in

High dependency on a single CSP could make it more difficult to replace a CSP by another. This could be the case where a CSP relies on non-standard functions or formats and does not provide interoperability. This could become a security threat if the locked-in CSP fails to address known security vulnerabilities, thus leaving the CSC vulnerable but unable to migrate to another CSP.

8.1.7 Misappropriation of intellectual property

When the CSC's software is run or other assets are stored by the CSP, the challenge exists that this material could be leaked to third parties or misappropriated for unauthorized use. This could include a violation of copyright or the exposure of trade secrets.

8.1.8 Loss of software integrity

Once the CSC's software is running in the CSP, there is the possibility of the software being modified or infected while it is out of the direct control of the CSC, thus causing their software to misbehave in some way. Although this possibility exists outside the CSC's control, it could seriously affect their reputation and thus their business.

8.2 Security challenges for cloud service providers (CSPs)

This clause describes security challenges associated with environmental difficulties or indirect threats that may give rise to more direct threats to the interests of the CSP.

8.2.1 Ambiguity in responsibility

Different roles (CSP, CSC, and CSN) may be defined in a cloud computing system. Ambiguity of the definition of responsibilities related to issues such as data ownership, access control or infrastructure maintenance may impact business or legal disputes (especially when dealing with third parties, or when the CSP is also a CSC or a CSN). This ambiguity risk increases when the CSP is operating and/or offering services across multiple jurisdictions where contracts and agreements may exist in different languages or legal frameworks. See also clause 8.2.4, "Jurisdictional conflict" below.

8.2.2 Shared environment

Cloud computing provides potential cost savings through massive resource sharing that occurs on a very large scale. This situation exposes many potentially vulnerable interfaces. For example, different CSCs consume services from the same cloud simultaneously. As a result, the CSC could potentially have unauthorized access to other tenants' virtual machines, network traffic, actual/residual data, etc. Any such unauthorized or malicious access to another CSC's assets might compromise integrity, availability and confidentiality.

For example, multiple virtual machines co-hosted on one physical server share both the central processing unit (CPU) and memory resources which are virtualized by the hypervisor. This example of challenges covers the failure of hypervisor isolation mechanisms, thus allowing unauthorized access to the memory or storage of other virtual machines.

8.2.3 Inconsistency and conflict of protection mechanisms

Due to the decentralized architecture of a cloud computing infrastructure, its protection mechanisms might be inconsistent among distributed security modules. For example, an access denied by one security module may be granted by another. This inconsistency might cause problems for an authorized user, and might be exploited by an attacker, thereby compromising confidentiality, integrity and availability.

8.2.4 Jurisdictional conflict

Data in the cloud can be moved around between data centres, or even across international borders. Depending on the host country, data will be governed by different applicable jurisdictions. For example, some jurisdictions, such as the European Union, require extensive protection of personally identifiable information (PII), which cannot usually be processed in places that do not provide a sufficient level of guaranteed protection. As a second example, some jurisdictions may treat communications as a service (CaaS) as an unregulated information service while others treat it as a regulated telephony service. This jurisdictional conflict can lead to legal complications that impact security, such as rules governing the lawful intercept of communications by law enforcement authorities, which may affect decisions on cryptography.

8.2.5 Evolutionary risks

One advantage of cloud computing is to postpone some choices from the system design phase to the execution phase. This means that some dependent software components of a system may be selected and implemented only when the function requiring them has been executed. However, conventional risk assessment methodology can no longer match such a dynamically evolving system. A system which has passed a security assessment during the design phase might have new vulnerabilities introduced during its lifetime due to changes in software components.

8.2.6 Bad migration and integration

Migrating to the cloud often implies moving large amounts of data and major configuration changes (e.g., network addressing). Migration of a part of an ICT system to an external CSP might require substantial changes in the system design (e.g., network and security policies). A bad integration caused by incompatible interfaces or inconsistent policy enforcement might result in both functional and non-functional impacts. For example, virtual machines that run behind a firewall in a private data centre are accidently exposed to the open Internet in the CSP's cloud.

8.2.7 Business discontinuity

Cloud computing allocates resources and delivers them as a service. The whole cloud computing ecosystem is composed of many interdependent parts. The discontinuity of any part (such as a blackout, denial-of-service or delay) might affect cloud computing service availability connected with clause 8.1.5 "Service unavailability", and then cause business discontinuity.

8.2.8 Cloud service partner lock-in

The platform of the CSP is built using software and hardware components from various suppliers. Some components may include proprietary features or extensions that are useful to the CSP. However, relying on these proprietary features limits the CSP's ability to migrate to another component supplier.

While lock-in is a business issue, it is not in itself a security threat. However, it can sometimes give rise to security concerns. For example, if the CSN who supplies a key component goes out of business, it may be that no further security patches are available. Where vulnerability in the component emerges, it may be very difficult or expensive to mitigate the risk.

8.2.9 Supply chain vulnerability

A CSP is at risk if hardware or software delivered to the platform through their supply chain undermines CSC or CSP security, for example, the accidental or deliberate introduction of malware or exploitable vulnerabilities.

A case in point would be bad software from the CSN. This security challenge exists for CSN software running in the CSP, such as customer facing, a virtual machine (VM) guest operating system (OS), applications, platform components, or audit/monitoring software (e.g., for a partner providing a service audit).

Another example is when a CSP is running software provided by a partner; the CSP is at risk if the partner fails to provide the necessary security updates in a timely manner.

8.2.10 Software dependencies

When vulnerability is detected, it may not be possible to apply updates immediately because doing so would break other software components (though those components may not otherwise require updating). This is particularly true if the dependency exists between components provided by one or more CSNs, rather than the CSPs themselves.

8.3 Security challenges for cloud service partners (CSNs)

This clause considers challenges that directly affect CSNs. Such challenges might affect the ability of a CSN to do business, to get paid, to protect their intellectual property, and to avoid legal or regulatory difficulties. Security challenges to a given CSN will depend on their specific business and environments, such as development, integration, audit, or otherwise.

8.3.1 Ambiguity in responsibility

Where there is a mix of CSP and CSN software running in the service, it may not be apparent to the CSC where the responsibility for mitigation and handling of security incidents resides. It may be quite difficult to determine the responsible entity by technical analysis. This could result in mutual finger-pointing between the CSP and CSN(s) as to who is at fault, which could result in further breaches if the root cause is not found.

8.3.2 Misappropriation of intellectual property

When partners submit software or other assets to the CSP for execution, the security challenge exists that this material could be leaked to third parties or misappropriated for unauthorized use. This could include a violation of copyright or the exposure of trade secrets.

8.3.3 Loss of software integrity

Once the partner's software is running in the CSP, there is a possibility of the software being modified or infected while it is out of the direct control of the CSN, thus causing their software to misbehave in some way. Although this possibility exists outside the CSN's control, it could seriously affect their reputation and thus their business.

9 Cloud computing security capabilities

This Recommendation identifies the following security capabilities against identified cloud computing security threats and challenges. Parameters related with these security capabilities may be stipulated in the security service level agreement (SLA), for example, an incident response time.

9.1 Trust model

A common trust model is necessary for any system where multiple providers cooperate to provide a trustworthy service.

Because of the highly distributed and multi-stakeholder nature of cloud computing, the cloud computing environment will need to incorporate an overall trust model. This trust model will enable the creation of islands and/or federations of trusted entities, such that disparate elements of the system will be able to authenticate the identity and authorized rights of other entities and components. Each island or federation of trust will be based on one or more trusted authorities (e.g., a public key infrastructure (PKI) certificate authority).

Multiple trust models exist today for both cloud and non-cloud purposes. The specific trust model to be adopted is out of the scope of this Recommendation.

9.2 Identity and access management (IAM), authentication, authorization and transaction audit

Multiple administrators and users are involved in cloud computing services, and these cloud computing services are accessed and used internally (CSPs) and externally (CSCs). Identity management is needed, not only to protect identities, but also to facilitate the access management, authentication, authorization and transaction audit processes in such a dynamic and open cloud computing infrastructure.

One or more common trust models (clause 9.1) are needed by IAM for the authentication of identities, and by developers, hypervisors and other system components for the authentication of system components such as downloaded software modules, applications or datasets.

IAM contributes to the confidentiality, integrity and availability of services and resources, and thus becomes essential in cloud computing.

Furthermore, IAM may enable the implementation of single sign-on and identity federation for clouds using different authentication mechanisms or distributed in different security domains.

Transaction audit protects against repudiation, enables forensic analysis after a security incident, and acts as a deterrent to attacks (both intrusion and insider). Transaction audit implies more than simple logging, but also includes active monitoring to flag up suspicious activities.

9.3 Physical security

Physical security needs to be achieved. Access to premises containing CSP equipment is restricted to authorized persons and only to those areas directly necessary for their job functions; this is part of the IAM process. However, the extent of physical security will depend on the value of the data and the extent to which multiple customers are permitted access.

9.4 Interface security

This capability secures interfaces open to CSCs and/or other contracted CSPs through which various kinds of cloud computing services are delivered, and secures communications based on these interfaces. Mechanisms available to ensure interface security include but are not limited to: unilateral/mutual authentication, integrity checksum, end-to-end encryption, digital signature, etc.

9.5 Computing virtualization security

Computing virtualization security refers to the security of the whole computing virtualization environment. It protects the hypervisor from attacks, protects the host platform from threats originating in the computing virtualization environment, and keeps VMs secure throughout the life-cycle. Specifically, this capability enables VM isolation, and protects the VM images and suspended VM instances in storage and during migration.

For CSP, the hypervisor often provides protection for hosted VMs, for example, by providing anti-virus and anti-spam processing inside hypervisors, so that VMs do not need to implement these functions separately. The hypervisor will normally be configured with the minimum set of services. Unnecessary interfaces and

application programing interfaces (APIs) will normally be closed, and irrelevant service components will normally be disabled.

VMs covered by this capability include those created by CSC in IaaS, as well as any VMs created by SaaS and PaaS. Virtual machines will usually be well isolated when sharing memory, a central processing unit (CPU) and storage capacities. Virtual machines will usually have intrinsic security capabilities and policy awareness (e.g., in the guest operating system).

9.6 Network security

In a cloud computing environment, network security enables both physical and virtual network isolation, and secures communications among all participants. It enables network security domain partition, network border access controls (e.g., firewall), intrusion detection and prevention, network traffic segregation based on security policies, and it protects the network from attacks in both the physical and virtual network environments.

9.7 Data isolation, protection and confidentiality protection

This capability addresses general data protection issues which often have legal implications.

- Data isolation

In a cloud computing context, a tenant is prevented from accessing data belonging to another tenant, even when the data is encrypted, except when explicitly authorized. Data isolation may be realized logically or physically, depending on the required isolation granularity and the specific deployment of cloud computing software and hardware.

NOTE 1 – In cloud computing, isolation occurs at the tenant level. A given CSC may have multiple tenants in the cloud, for example, to separate different subsidiaries, divisions or business units.

- Data protection

Data protection ensures that CSC data and derived data held in a cloud computing environment is appropriately protected so that it can only be accessed or changed as authorized by the CSC (or according to applicable law). This protection may include some combination of access control lists, integrity verification, error correction/data recovery, encryption and other appropriate mechanisms.

When a CSP provides storage encryption for CSCs, this function can be client-side encryption (e.g., within a CSP application) or server-side encryption.

- Confidentiality protection

Private information can include PII and confidential corporate data. The collection, use, transfer, handling, storage and destruction of private information can be subject to confidentiality regulations or laws. This restriction applies to both CSPs and their CSCs, e.g., a CSC must be able to permanently delete a data table containing private information, even though the CSP is not aware of the table contents. CSPs may also need to support the handling, e.g., searching of a CSCs' data in their transformed or encrypted form.

Confidentiality protection extends to private information that may be observed or derived from CSC activities, such as business trends, relationships or communications with other parties, activity levels and patterns, etc.

Confidentiality protection is also responsible for ensuring that all private information (including observed or derived data) is used only for those purposes which have been agreed between a CSC and CSP.

A risk assessment of private information (noted as "confidentiality risk assessment") can assist a CSP in identifying the specific risks of confidentiality breaches involved in an envisaged operation. The CSP should identify and implement capabilities to address the confidentiality risks identified by the risk assessment and treatment of private information.

NOTE 2 – In some jurisdictions, individual natural persons (i.e., human users) are treated separately from their employers for confidentiality purposes. In such circumstances, confidentiality of the cloud service user (CSU) will be appropriately protected in addition to that of the cloud service customer (CSC) or cloud service tenant.

9.8 Security coordination

Since different cloud computing services imply different implementations of security controls, this security capability coordinates heterogeneous security mechanisms to avoid protection conflicts.

Parties playing different roles in the cloud computing ecosystem, e.g., CSP, CSC, CSN, have different degrees of control over the physical or virtual resources and services, including the control of security.

For each party, there will be various security mechanisms including hypervisor isolation, IAM, network protection, etc.

One of the purposes of cloud computing is to enable a combination of these different parties to collaboratively design, build, deploy and operate various physical and virtualized resources together. Therefore, a CSP needs to be able to coordinate different security mechanisms across the different parties. Security coordination depends on the interoperability and harmonization of diverse security mechanisms.

9.9 Operational security

This capability provides security protection for the daily operation and maintenance of cloud computing services and infrastructure.

This operational security capability includes:

- defining sets of security policies and security activities such as configuration management, patch upgrade, security assessment, incident response (see also clause 9.10 "Incident management"), and ensuring these security measures are correctly enforced to fulfil the requirements of applicable laws and contracts including any security SLA;
- monitoring the CSP's security measures and their effectiveness, and giving appropriate reports to affected CSCs and applicable third-party auditors (acting as a CSN), which can enable the CSC to measure whether a CSP is delivering on SLA security commitments.

In the event that the CSP's security measures or their effectiveness changes, all downstream CSPs and CSCs will be alerted to such changes.

These reports and alerts enable authorized CSCs to see appropriate incidents, audit information, and configuration data relating to their cloud computing services.

9.10 Incident management

Incident management provides incident monitoring, prediction, alerting and response. In order to know whether the cloud computing service is operating as expected through the whole infrastructure, continuous monitoring is necessary (e.g., monitoring the real-time performance of virtualized platform and virtualized machine). This enables systems to capture the service security status, identify abnormal conditions, and provide early warning of security system overloads, breaches, service discontinuity, etc. After the occurrence of security incidents, the problem is identified and the incident is quickly responded to, either automatically or with the intervention of a human administrator. Closed incidents are logged and analysed for possible underlying patterns which can then be proactively addressed.

9.11 Disaster recovery

Disaster recovery represents the capability to respond to catastrophic disasters, to recover to a safe state and to resume normal operations as quickly as possible. This capability provides continuity of provided service with minimum interruption.

9.12 Service security assessment and audit

This capability enables the security evaluation of cloud computing services. It enables an authorized party to verify that a cloud service complies with the applicable security requirements. Security assessment or security audit could be performed by the CSC, CSP or a third party (CSN), and security certification could be performed by an authorized third party (CSN).

Appropriate security criteria are implemented so as to provide a mutual understanding of the security level between the CSC and CSP.

Each CSP and each of their services may have the security level regarding the CSP's security controls and their effectiveness. Advertised security levels of the CSPs and their services will help facilitate the comparison and selection of appropriate CSPs and cloud computing services. Independent trusted third parties may be used to provide reliable, independent and neutral security level assessments.

To avoid a CSP conducting individual security audits for each CSC, common service audit results will be appropriately reused. For a CSP covering a wide range of cloud computing services, security audits may be conducted on each cloud computing service. The CSP may provide the appropriate audit results of all or part of the cloud computing services to an authorized CSC (e.g., potential customer), and to certain other CSPs and CSNs (e.g., third-party auditor).

For a cloud computing service chain, the security audit results of a downstream service provider will integrate the relevant security audit results of upstream service providers.

9.13 Interoperability, portability and reversibility

This capability enables the coexistence and cooperation of heterogeneous components (interoperability), it enables CSCs to replace one CSP with another where appropriate (portability), and enables CSCs to transfer their ICT system from a cloud computing environment back to a non-cloud computing ICT infrastructure (reversibility). This reversibility will also enable the "right to be forgotten" if this is required by local laws or regulations.

NOTE 1 – This capability is only responsible for the interoperability and portability of cloud computing security functions, not of the actual data, metadata or message formats, which are the responsibility of other cloud computing platform functions. For example, this capability might provide transitional encryption, key management and identity information so that data and other content can be moved between two different encryption systems without exposing either the system(s) or the data in transit.

NOTE 2 – The "right to be forgotten" is not yet clearly defined and may in some cases be constrained by regulatory requirements to retain certain data for a minimum period, such as call records or connection information. It may therefore also be necessary to retain the relevant keys or other security information for the same period.

9.14 Supply chain security

A CSP uses a number of suppliers to build their services. Some of these will be cloud industry participants, e.g., a CSN, while others will be traditional information technology (IT) equipment or service suppliers, e.g., hardware manufacturers with no direct relationship with cloud computing. This capability enables the establishment of a trust relationship between the CSP and all participants in the supply chain by security activities. These supply chain security activities involve identifying and gathering information about the CSP's acquired components and services that are used to provide cloud computing services, and enforcing supply chain security policies.

For example, typical supply chain security activities in a CSP may include:

- confirmation of background information about the participants in the supply chain;
- validation of hardware, software and services employed by the CSP;
- inspection of the hardware and software purchased by the CSP so as to ensure that it was not tampered with while in-transit;
- providing mechanisms to verify the provenance of cloud service software, for example, code provided by a CSN. Where applicable, CSNs and their host CSPs provide a process to verify the integrity of the CSN's software component to ensure that it is exactly as delivered and has not been modified or compromised. Some CSNs may demand the means to verify this directly by themselves.

This capability is continuous to cover ongoing system evolution and updates.

10 Framework methodology

To develop a security framework for cloud computing means understanding what threats and challenges exist, as was discussed in clauses 7 and 8, for the chosen specific cloud service along with the business, technology and regulatory requirements which are to be taken together to identify security controls, policies and procedures that will be needed for a given cloud service. The capabilities described in clause 9 to address and mitigate these threats and challenges are then used to develop the security controls, policies and procedures for the chosen specific cloud computing service. This Recommendation focuses on what the needs are for security in a cloud computing environment, the threats and challenges of a traditional computing environment exist within the cloud environment and as such following the standards and best practices defined by the industry should be followed in addition to this Recommendation.

The methodology described here should be followed to create the framework that will identify what security controls, policies and procedures will be needed for a specific given cloud computing service. It is not possible to provide a single normative framework for all cloud computing services, since they vary greatly in business model, services offered and implementation choices:

- Step 1: Use clauses 7 and 8 to identify security threats and security implications of the challenges in the cloud computing service under study.
- Step 2: Use clause 9 to identify the needed high-level security capabilities based on identified threats and challenges which could mitigate security threats and address security challenges.
- Step 3: Derive security controls, policies and procedures which could provide the security abilities that are needed based on identified security capabilities.

NOTE – A set of appropriate requirements with respect to the security capabilities will need to be determined by the CSC and CSP using appropriate standards. This determination will be based on the risk assessment.

To identify which security threats and challenges are relevant for the cloud service under study, each threat or challenge should be reviewed. One approach could be as simple as a table showing a 'Y' next to the threat or challenge.

For an example using this approach, when the CSP provides file storage as a service to individual users, the CSP would like to understand what security threats and challenges users are mainly concerned about, and to analyse what security threats and challenges that CSP mainly needs to address. Table 1 demonstrates this approach.

Table 1 – Example of security framework analysis step 1 for file storage as a service

Area of analysis	Specific threat or challenge	Is this applicable to this service?
Clause 7.1 Security threats for cloud service customers (CSC)	Clause 7.1.1 Data loss and leakage	Y
	Clause 7.1.2 Insecure service access	Y
	Clause 7.1.3 Insider threats	
Clause 7.2 Security threats for cloud service providers (CSPs)	Clause 7.2.1 Unauthorized administration access	Y
	Clause 7.2.2 Insider threats	Y
Clause 8.1 Security challenges for cloud service customers (CSCs)	Clause 8.1.1 Ambiguity in responsibility	Y
	Clause 8.1.2 Loss of trust	Y
	Clause 8.1.3 Loss of governance	Y
	Clause 8.1.4 Loss of confidentiality	Y
	Clause 8.1.5 Service unavailability	Y
	Clause 8.1.6 Cloud service provider lock-in	Y
	Clause 8.1.7 Misappropriation of intellectual property	

Table 1 – Example of security framework analysis step 1 for file storage as a service

Area of analysis	Specific threat or challenge	Is this applicable to this service?
	Clause 8.1.8 Loss of software integrity	
Clause 8.2 Security challenges for cloud service providers (CSPs)	Clause 8.2.1 Ambiguity in responsibility	Y
	Clause 8.2.2 Shared environment	Y
	Clause 8.2.3 Inconsistency and conflict of protection mechanisms	Y
	Clause 8.2.4 Jurisdictional conflict	Y
	Clause 8.2.5 Evolutionary risks	
	Clause 8.2.6 Bad migration and integration	Y
	Clause 8.2.7 Business discontinuity	Y
	Clause 8.2.8 Cloud service partner lock-in	
	Clause 8.2.9 Supply chain vulnerability	Y
	Clause 8.2.10 Software dependencies	
Clause 8.3 Security challenges for cloud service partners (CSNs)	Clause 8.3.1 Ambiguity in responsibility	
	Clause 8.3.2 Misappropriation of intellectual property	
	Clause 8.3.3 Loss of software integrity	

Once the security threats and challenges have been identified, the security capabilities that could mitigate these threats and address these challenges can be identified. In Table I.1 there is an example of a mapping of cloud computing security threats and challenges to security capabilities. The letter 'Y' in a cell formed by the intersection of the table's columns and rows designate that a particular security threat and challenge is addressed by a corresponding security capability. This table shows all the threats and challenges and the corresponding security capability.

Once the capabilities required have been identified, the security controls, policies and procedures can be determined as to what is needed. Examples of controls that could be used are "Operations security" (clause 12 in [b-ISO/IEC 27002]) and "Information security incident management" (clause 16 in [b-ISO/IEC 27002]) which can be derived from the identified capabilities in clauses 9.9 and 9.10, respectively.

A cloud service may have a supply chain comprised of multiple CSPs. The companies participating in such a supply chain can refer to ITU and Industry standards on the topic of supply chain security (e.g., [b-ISO/IEC 28000]). Each CSP will need to clearly delineate their responsibility in the cloud computing service chain, and develop their security controls, policies and procedures based on the derived security capabilities by this three-step approach. To provide consistent security to CSCs, the upstream CSP may need to negotiate with their downstream CSPs on these security capabilities based on their security responsibilities. When needed, CSCs should follow this three-step procedure as well.

In addition, the above three-step procedure should be carried out periodically or when needed (e.g., when a serious security breach occurs, or when a CSP changes its upstream CSP).

Appendix I

Mapping of cloud computing security threats and challenges to security capabilities

(This appendix does not form an integral part of this Recommendation.)

Table I.1 shows a mapping of cloud computing security threats and challenges to some of the possible security capabilities.

The letter 'Y' in a cell formed by the intersection of the table's columns and rows designate that a particular security threat and challenge is addressed by a corresponding security capability.

Table I.1 – Mapping of cloud computing security threats and challenges to security capabilities

			Clause 9 Cloud computing security capabilities													
			Clause9.1 Trust model	Clause 9.2 Identity and access management (IAM), authentication, authorization and transaction audit	Clause 9.3 Physical security	Clause 9.4 Interface security	Clause 9.5 Computing virtualization security	Clause 9.6 Network security	Clause 9.7 Data isolation, protection and confidentiality protection	Clause 9.8 Security coordination	Clause 9.9 Operational security	Clause 9.10 Incident management	Clause 9.11 Disaster recovery	Clause 9.12 Service security assessment and audit	Clause 9.13 Interoperability, portability and reversibility	Clause 9.14 Supply chain security
Clause 7 Security threats for cloud compu-ting	Clause 7.1 Security threats for cloud service customers (CSCs)	Clause 7.1.1 Data loss and leakage	Y	Y	Y				Y				Y			
		Clause 7.1.2 Insecure service access	Y	Y		Y	Y	Y								
		Clause 7.1.3 Insider threats		Y	Y									Y		
	Clause 7.2 Security threats for cloud service providers (CSPs)	Clause 7.2.1 Unautho-rized administra-tion access	Y	Y	Y	Y										
		Clause 7.2.2 Insider threats		Y	Y									Y		
Clause 8 Security challenge s for cloud compu-ting	Clause 8.1 Security challenges for cloud service customers (CSCs)	Clause 8.1.1 Ambiguity in responsi-bility		Y							Y					
		Clause 8.1.2 Loss of trust	Y											Y		
		Clause 8.1.3 Loss of governance		Y	Y				Y		Y	Y	Y	Y		

Table I.1 – Mapping of cloud computing security threats and challenges to security capabilities

			Clause 9 Cloud computing security capabilities													
			Clause9.1 Trust model	Clause 9.2 Identity and access management (IAM), authentication, authorization and transaction audit	Clause 9.3 Physical security	Clause 9.4 Interface security	Clause 9.5 Computing virtualization security	Clause 9.6 Network security	Clause 9.7 Data isolation, protection and confidentiality protection	Clause 9.8 Security coordination	Clause 9.9 Operational security	Clause 9.10 Incident management	Clause 9.11 Disaster recovery	Clause 9.12 Service security assessment and audit	Clause 9.13 Interoperability, portability and reversibility	Clause 9.14 Supply chain security
		Clause 8.1.4 Loss of confidentiality		Y					**Y**					Y		
		Clause 8.1.5 Service unavailability								Y	Y	Y	Y			Y
		Clause 8.1.6 Cloud service provider lock-in													Y	
		Clause 8.1.7 Misappropriation of intellectual property		Y	Y				Y		Y					
		Clause 8.1.8 Loss of software integrity		Y			Y		Y							
Clause 8 Security challenges for cloud computing	Clause 8.2 Security challenges for cloud service providers (CSPs)	Clause 8.2.1 Ambiguity in responsibility		Y							Y					
		Clause 8.2.2 Shared environment					Y	Y	Y							
		Clause 8.2.3 Inconsistency and conflict of protection mechanisms								Y					Y	
		Clause 8.2.4 Jurisdictional conflict							Y		Y					
		Clause 8.2.5 Evolutionary risks									Y				Y	Y

Table I.1 – Mapping of cloud computing security threats and challenges to security capabilities

			Clause 9 Cloud computing security capabilities													
			Clause9.1 Trust model	Clause 9.2 Identity and access management (IAM), authentication, authorization and transaction audit	Clause 9.3 Physical security	Clause 9.4 Interface security	Clause 9.5 Computing virtualization security	Clause 9.6 Network security	Clause 9.7 Data isolation, protection and confidentiality protection	Clause 9.8 Security coordination	Clause 9.9 Operational security	Clause 9.10 Incident management	Clause 9.11 Disaster recovery	Clause 9.12 Service security assessment and audit	Clause 9.13 Interoperability, portability and reversibility	Clause 9.14 Supply chain security
		Clause 8.2.6 Bad migration and integration				Y	Y	Y	Y	Y	Y					
		Clause 8.2.7 Business discon-tinuity										Y	Y			
		Clause 8.2.8 Cloud service partner lock-in														Y
Clause 8 Security challenges for cloud compu-ting	Clause 8.2 Security challenges for cloud service providers (CSPs)	Clause 8.2.9 Supply chain vulnera-bility														Y
		Clause 8.2.10 Software depen-dencies														Y
	Clause 8.3 Security challenges for cloud service partners (CSNs)	Clause 8.3.1 Ambiguity in responsi-bility		Y							Y					
		Clause 8.3.2 Misappro-priation of intellectual property		Y	Y				Y		Y					
		Clause 8.3.3 Loss of software integrity		Y			Y		Y							

Bibliography

[b-ITU-T E.409] Recommendation ITU-T E.409 (2004), *Incident organization and security incident handling: Guidelines for telecommunication organizations.*

[b-ITU-T X.810] Recommendation ITU-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview.*

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud Computing – Overview and vocabulary.*

[b-ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014) | ISO/IEC 17789:2014, *Information technology – Cloud Computing – Reference architecture.*

[b-ISO/IEC 19440] ISO/IEC 19440:2007, *Enterprise integration – Constructs for enterprise modelling.*

[b-ISO/IEC 20000-1] ISO/IEC 20000-1:2011, *Information technology – Service management – Part 1: Service management system requirements.*

[b-ISO/IEC 27000] ISO/IEC 27000:2012, *Information technology – Security techniques – Information security management systems – Overview and vocabulary.*

[b-ISO/IEC 27002] ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management.*

[b-ISO/IEC 27005] ISO/IEC 27005:2011, I*nformation technology – Security techniques – Information security risk management.*

[b-ISO/IEC 27729] ISO/IEC 27729:2012, *Information and documentation – International standard name identifier (ISNI).*

[b-ISO/IEC 28000] ISO/IEC 28000:2007, *Specification for security management systems for the supply chain.*

[b-ISO/IEC 29100] ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy framework.*

[b-NIST-SP-800-30] NIST Special Publication 800-30 (2012), *Guide for Conducting Risk Assessments.*

[b-NIST-SP-800-53] NIST Special Publication 800-53 Rev.3 (2009), *Recommended Security Controls for Federal Information Systems and Organizations.*

[b-NIST-SP-800-125] NIST Special Publication 800-125 (2011), *Guide to Security for Full Virtualization Technologies.*

[b-NIST-SP-800-145] NIST Special Publication 800-145 (2011), *The NIST Definition of Cloud Computing.*

[b-CSA Matrix] CSA (2013), *Cloud Controls Matrix*, Cloud Security Alliance.

[b-key definition] Key definitions of the Data Protection Act, Information Commissioners Office <http://www.ico.gov.uk/for_organisations/data_protection/the_guide/key_definitions.aspx>


PROTECTION

Data security requirements for the monitoring service of cloud computing

Recommendation ITU-T X.1603

(03/2018)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Summary

Recommendation ITU-T X.1603 analyses data security requirements for the monitoring service of cloud computing which includes monitoring data scope requirements, monitoring data lifecycle, security requirements of monitoring data acquisition and security requirements of monitoring data storage. Monitoring data scope requirements include the necessary monitoring scope that cloud service providers (CSPs) should provide to maintain cloud security and the biggest monitoring scope of CSPs. Monitoring data lifecycle includes data creation, data store, data use, data migrate, data present, data destroy and data backup. Monitoring acquisition determines security requirements of the acquisition techniques of monitoring service. Monitoring data storage determines security requirements for CSPs to store the monitoring data.

Keywords

Cloud, data security, monitoring.

Table of Contents

1 Scope

This Recommendation describes data security requirements for the monitoring service of cloud computing. The Recommendation analyses data security threats and challenges associated with the monitoring service in a cloud computing environment, and describes data security requirements of the monitoring service including data scope, data lifecycle, data acquisition and data storage. This Recommendation can be used by cloud service providers (CSPs) who provide monitoring services to cloud service customers (CSCs).

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 authentication [b-NIST-SP-800-53]: Verification of the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

3.1.2 capability [b-ISO/IEC 19440]: Quality of being able to perform a given activity.

3.1.3 cloud computing [b-ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

3.1.4 cloud service [b-ITU-T Y.3500]: One or more capabilities offered via cloud computing (see clause 3.1.3) invoked using a defined interface.

3.1.5 cloud service customer [b-ITU-T Y.3500]: Party (see clause 3.1.15) which is in a business relationship for the purpose of using cloud services (see clause 3.1.4).

NOTE – A business relationship does not necessarily imply financial agreements.

3.1.6 cloud service partner [b-ITU-T Y.3500]: Party (see clause 3.1.15) which is engaged in support of, or auxiliary to, activities of either the cloud service provider (see clause 3.1.7) or the cloud service customer (see clause 3.1.5), or both.

3.1.7 cloud service provider [b-ITU-T Y.3500]: Party (see clause 3.1.15) which makes cloud services (see clause 3.1.4) available.

3.1.8 cloud service user [b-ITU-T Y.3500]: Natural person, or entity acting on their behalf, associated with a cloud service customer (3 see clause.1.5) that uses cloud services (see clause 3.1.4).

NOTE – Examples of such entities include devices and applications.

3.1.9 Communications as a Service (CaaS) [b-ITU-T Y.3500]: Cloud service category in which the capability provided to the cloud service customer (see clause 3.1.5) is real time interaction and collaboration.

NOTE – CaaS can provide both application capabilities type and platform capabilities type.

3.1.10 community cloud [b-ITU-T Y.3500]: Cloud deployment model where cloud services (see clause 3.1.4) exclusively support and are shared by a specific collection of cloud service customers (see clause 3.1.5) who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection.

3.1.11 hypervisor [b-NIST-SP-800-125]: The virtualization component that manages the guest OSs on a host and controls the flow of instructions between the guest OSs and the physical hardware.

3.1.12 Infrastructure as a Service (IaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer (see clause 3.1.5) is an infrastructure capabilities type.

NOTE – The cloud service customer (see clause 3.1.5) does not manage or control the underlying physical and virtual resources, but does have control over operating systems, storage, and deployed applications that use the physical and virtual resources. The cloud service customer (see clause 3.1.5) may also have limited ability to control certain networking components (e.g., host firewalls).

3.1.13 multi-tenancy [b-ITU-T Y.3500]: Allocation of physical or virtual resources such that multiple tenants (see clause 3.1.24) and their computations and data are isolated from and inaccessible to one another.

3.1.14 Network as a Service (NaaS) [b-ITU-T Y.3500**]**: Cloud service category in which the capability provided to the cloud service customer (see clause 3.1.5) is transport connectivity and related network capabilities.

NOTE – NaaS can provide any of the three cloud capabilities types.

3.1.15 party [b-ISO/IEC 27729**]**: Natural person or legal person, whether or not incorporated, or a group of either.

3.1.16 personally identifiable information [b-ISO/IEC 29100]: Any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal.

3.1.17 Platform as a Service (PaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer (see clause 3.1.5) is a platform capabilities type.

3.1.18 private cloud [b-ITU-T Y.3500]: Cloud deployment model where cloud services (see clause 3.1.4) are used exclusively by a single cloud service customer (see clause 3.1.5) and resources are controlled by that cloud service customer (see clause 3.1.5).

3.1.19 public cloud [b-ITU-T Y.3500]: Cloud deployment model where cloud services (see clause 3.1.4) are potentially available to any cloud service customer (see clause 3.1.5) and resources are controlled by the cloud service provider (see clause 3.1.7).

3.1.20 security domain [b-ITU-T X.810]: A set of elements, a security policy, a security authority and a set of security-relevant activities in which the set of elements are subject to the security policy for the specified activities, and the security policy is administered by the security authority for the security domain.

3.1.21 security incident [b-ITU-T E.409]: A security incident is any adverse event whereby some aspect of security could be threatened.

3.1.22 service level agreement (SLA) [b-ISO/IEC 20000-1]: A documented agreement between the service provider and customer that identifies services and service targets.

NOTE 1 – A service level agreement can also be established between the service provider and a supplier, an internal group or a customer acting as a supplier.

NOTE 2 – A service level agreement can be included in a contract or another type of documented agreement.

3.1.23 Software as a Service (SaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer (see clause 3.1.5) is an application capabilities type.

3.1.24 tenant [b-ITU-T Y.3500]: One or more cloud service users (see clause 3.1.8) sharing access to a set of physical and virtual resources.

3.1.25 threat [b-ISO/IEC 27000]: A potential cause of an unwanted incident, which may result in harm to a system or organization.

3.1.26 vulnerability [b-NIST-SP-800-30]: A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 **monitoring data**: Monitoring data is the output of the cloud monitor service, which helps cloud service provider (CSP) and cloud service customers (CSC) manage cloud platforms and cloud resources.

3.2.2 **monitor service**: The monitor service activity monitors the delivered service quality with respect to service levels as defined in the service level agreement (SLA) between cloud service customer and cloud service provider.

3.2.3 **necessary monitoring data**: Necessary monitoring data is used to maintain service level agreements (SLA). Necessary monitoring data could help cloud service provider (CSP) to keep cloud computing platforms security and stable. Necessary monitoring data could include, but is not limited to, management system monitoring data, physical resources monitoring data, network monitoring data and etc. Necessary monitoring data is mainly used by CSPs but could also be shared with cloud service customers (CSCs).

3.2.4 **optional monitoring data**: Optional monitoring data is provided on the demand of cloud service customers (CSCs) and to provide cloud monitor service. Optional monitoring data could include, but is not limited to, virtual machine monitoring data, data storage service monitoring data, CSCs' application on cloud monitoring data and etc.

3.2.5 **virtual machine (VM)**: An efficient, isolated, logical duplicate of a real machine.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API Application Programming Interface

BCP Business Continuity Plan

CaaS Communications as a Service

CPU Central Processing Unit

CSC Cloud Service Customer

CSN Cloud Service Partner

CSP Cloud Service Provider

CSU Cloud Service User

DDOS Distributed Denial of Service

DNS Domain Name System

DOS Denial of Service

IaaS Infrastructure as a Service

IAM Identity and Access Management

ICT Information and Communication Technology

IP Internet Protocol

IT Information Technology

NaaS Network as a Service

OS Operating System

PaaS Platform as a Service

PII Personally Identifiable Information

PKI Public Key Infrastructure

SaaS Software as a Service

SIM Subscriber Identity Module

SLA Service Level Agreement

VM Virtual Machine

5 Conventions

In this Recommendation:

The keywords "**is required to**" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "**is recommended**" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "**is prohibited from**" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Overview

This Recommendation analyses data security requirements for the monitoring service of cloud computing including monitoring data scope, monitoring data lifecycle, security threats and challenges, and monitoring data security requirements of cloud computing.

Monitoring data scope describes two types of cloud monitoring data: necessary and optional, and also explains the use cases.

Monitoring data lifecycle, and the security threats and challenges, describe the content and security threats and challenges of cloud monitoring data collection, storage, use, migration, analysis, presentation, destruction and backup.

Monitoring data security requirements describes the detailed requirements for each lifecycle stage of cloud monitoring data.

7 Scope of monitoring data for cloud computing

In a cloud computing environment, there are two types of monitoring data: necessary monitoring data and optional monitoring data.

Necessary monitoring data is that which is used to maintain service level agreements (SLAs). Necessary monitoring data can help the CSP run the cloud computing platform securely and stably. Necessary monitoring data may include, but is not limited to, management system monitoring data, physical resources monitoring data and network monitoring data. Necessary monitoring data is mainly used by CSPs but could also be shared with CSCs.

Optional monitoring data is that which is provided at the request of the CSC to provide the monitoring service by the CSP. Optional monitoring data may include, but is not be limited to, virtual machine monitoring data, data storage service monitoring data and the CSCs' data associated with the monitoring of their own application on cloud.

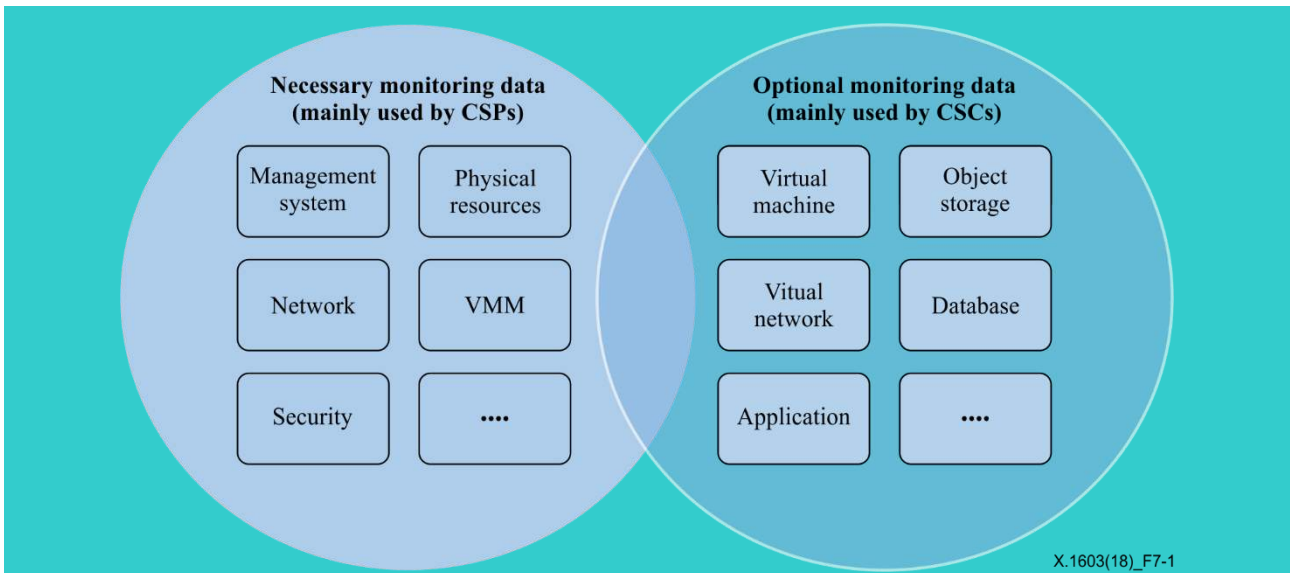


Figure 7-1 – Use cases of two types of monitoring data

Necessary monitoring data is mainly used by CSPs, but could also be used by CSCs. For example, monitoring data of cloud physical resources is mainly used by CSPs to maintain the stability of the cloud platform, but could also be used by CSCs if the cloud-related physical resources were provided to the customers as a service.

Optional monitoring data is provided as the request of CSCs and also mainly used by CSCs. CSPs could also use optional monitoring data to maintain SLAs. For example, CSCs could require the CSCs' data associated with the monitoring of their own applications in the cloud. This data is provided by CSP, and used to better manage their applications in the cloud. For example, a CSP could use database as a service (DBaaS) monitoring data to maintain the security and stability of database resources and service in cloud.

The relationship of these two types of monitoring data is illustrated in Figure 7-1.

8 Monitoring data lifecycle in cloud computing

This clause describes the lifecycle of monitoring data in cloud computing and clarifies the main differences between it and lifecycle of other data in cloud computing.

8.1 Monitoring data collection

Monitoring data collection results from the acquisition of monitoring data and the transmission of that data to a storage server. Most monitoring data is created by the use of the cloud service by the CSC. Necessary monitoring data can also be created by other cloud service monitoring activities.

8.2 Monitoring data storage

After creating a monitoring data collection, cloud monitoring data can be stored in the CSC cloud resources locally, or in monitoring data storage servers of the CSP.

8.3 Monitoring data use

Monitoring data can be used to maintain the performance and security of the cloud platform and the cloud service by the CSP; it can also be used to maintain cloud resources performance and security by CSCs.

8.4 Monitoring data migration

When cloud resources are migrated, monitoring data can migrate along with the cloud resources.

8.5 Monitoring data analysis

Monitoring data can be analyzed by the CSP and CSC to understand the status of the cloud platform resources in order to better manage and secure them.

8.6 Monitoring data presentation

It is recommended that monitoring data be presentable in meaningful ways in order to be useful for better management of SLAs and cloud security. Since the volume of cloud monitoring data can be very large, is recommended that these data be summarized in a manageable and understandable way.

8.7 Monitoring data destruction

To maintain monitoring data security, the CSP is required to destroy monitoring data as CSCs demand.

CSPs can optionally destroy monitoring data after an appropriate period of time after monitoring data creation.

8.8 Monitoring data backup

It is required to create monitoring data backups and to restore data from backups.

9 Security threats and challenges for monitoring data of cloud computing

The security threats and challenges for cloud computing, clauses 7 and 8 respectively in [b-ITU-T X.1601], have provided the security threats and challenges for the CSC and CSP in cloud computing; cloud monitoring data also faces similar security threats and challenges that are defined in [b-ITU-T X.1601. Some of these security threats and challenges for cloud monitoring data include but are not limited to those shown below:

a) data loss and leakage;

b) insecure service access;

c) unauthorized administration access;

d) insider threats;

e) loss of trust;

f) loss of governance;

g) loss of confidentiality;

h) service unavailability;

i) misappropriation of intellectual property;

j) shared environment;

k) jurisdictional conflict;

l) bad migration and integration.

For each monitoring data lifecycle stage, cloud monitoring data face some particular security threats and challenges.

9.1 Security threats and challenges in monitoring data collection stage

a) data collection without authorization: A CSP or attackers may collect the CSC's monitoring data without permission or authorization.

b) acquisition interface vulnerability: Attackers may use a monitoring data acquisition interface vulnerability.

c) spoofing: Attackers could masquerade as the management system, or data storage server, of cloud monitoring service, and cause the loss of monitoring data.

d) tampering and intercepting: Attackers could use man-in-the-middle or other network attacks to tamper with, or intercept monitoring data.

e) insecure service access: In the monitoring data collection stage, insecure access to the data collection interfaces could cause monitoring data loss.

f) unauthorized administration access: Unauthorized administration access to the CSP's monitoring data collection system, or the CSC's system could result in monitoring data loss. For example, attackers may use a system vulnerability to gain unauthorized administration access to the CSC's system and modify the monitoring collection destination IP address to that of the attackers.

9.2 Security threats and challenges in monitoring data storage stage

a) data loss and leakage: As the cloud service environment is typically a multi-tenant one, loss or leakage of data is a serious threat to both the CSC and CSP. A lack of appropriate management of cryptographic information, such as encryption keys, authentication codes and access privilege, could lead to significant damages, such as data loss and unexpected leakage to the outside. For example, insufficient authentication, authorization, and audit controls; inconsistent use of encryption and/or authentication keys; operational failures; disposal problems; jurisdiction and political issues; data centre reliability; and disaster recovery, can be recognized as major threats.

b) service unavailability: A monitoring data storage server can be attacked by a denial of service (DoS) or distributed denial of service (DDoS) attack; in addition, the monitoring data storage hardware could fail and cause data loss or destruction.

9.3 Security threats and challenges in monitoring data use stage

a) data misuse: CSC monitoring data could be misused by the CSP. Monitoring data could be used by a CSP to maintain SLA and the operation of cloud computing platform and resources; however, CSC monitoring data could also be used for other purposes by the CSP without CSC permission.

b) insider threats: An employee of a CSP or CSC could misuse the CSC's monitoring data for other than intended purposes.

c) system vulnerability: Monitoring data could be lost during data usage due to system vulnerabilities.

d) eavesdropping: Monitoring data could be subject to eavesdropping by attackers.

9.4 Security threats and challenges in monitoring data migration stage

a) data misuse: Monitoring data could migrate between different physical locations. It is very important not to allow data to be misused as a result of monitoring data being transmitted to different locations.

b) spoofing: Attackers could masquerade as the management system or data storage server of a cloud monitoring service, and cause the loss or misuse of monitoring data.

c) tampering and intercepting: Attackers could use man-in-the-middle or other network attacks to tamper and intercept monitoring data.

9.5 Security threats and challenges in monitoring data analysis stage

a) data misuse: CSC monitoring data could be misused by the CSP during data analysis.

b) system vulnerability: Monitoring data could be lost due to a data analysis system vulnerability.

c) DoS attack: A monitoring data analysis server could be attacked by DoS or DDoS attack.

9.6 Security threats and challenges in monitoring data presentation stage

a) data misuse: CSC monitoring data could be misused (or be presented without CSC permission) by the CSP during data presentation.

b) system vulnerability: Reporting and analysis data could be lost due to a data presentation system vulnerability.

c) misrepresentation: CSC monitoring data could be misrepresented during a data presentation.

9.7 Security threats and challenges in monitoring data destruction stage

a) spoofing: Attackers could masquerade as the management system of the cloud monitoring service and cause the loss of other monitoring data.

b) operating system vulnerability: Monitoring data could be lost during data usage due to a system vulnerability.

9.8 Security threats and challenges in monitoring data backup stage

a) operating system vulnerability: Monitoring data could be lost during the data backup and result in the inability to restore data due to a system vulnerability.

10 Security requirements for monitoring data of cloud computing

This clause identifies the data security requirements for the monitoring service of cloud computing.

10.1 Security requirements for monitoring data collection

The data security requirements for the monitoring data collection include the following:

a) optional monitoring data is required to be created only by CSC request;

b) it is recommended to provide notification to the CSC when necessary monitoring data is created;

c) it is recommended to notify the CSC of the scope of monitoring data;

d) it is required to maintain integrity and accuracy of monitoring data;

e) it is recommended to use standard data acquisition techniques;

f) it is recommended to provide access control methods to the interfaces of monitoring data acquisition such as white list, black list, etc.;

g) it is recommended to provide cryptographic methods to ensure the security of the monitoring data acquisition interface;

h) it is recommended to use standard network protocols between the cloud resources and monitoring data storage servers.

Table 10-1 provides a summary mapping of monitoring data collection security threats to security requirements.

Table 10-1 – Monitoring data collection: security threats mapping to security requirements

Security threats	Security requirements
Data collection without authorization	a), b), c)
Acquisition interface vulnerabilities	d), e), f), g)
Spoofing	d), e), f), g), h)
Tampering and interception	h)
Insecure service access	b), d), e), f), g), h)
Unauthorized administrative access	d), e), f), g), h)

10.2 Security requirements for monitoring data storage

The data security requirements for the monitoring data storage include the following:

a) it is recommended that the CSP provide the appropriate access control methods to the monitoring data storage servers;

b) it is recommended that the CSP identify the maximum period of time for monitoring data retention;

c) it is recommended that the CSP provide appropriate encryption methods for monitoring data.

Table 10-2 provides a summary mapping of monitoring data storage security threats to security requirements.

Table 10-2 – Monitoring data storage: security threats mapping to security requirements

Security threats	Security requirements
Data loss and leakage	a), b), c)
Service unavailability	a), c)

10.3 Security requirements for monitoring data use

The data security requirements for the monitoring data use include the following:

a) it is required that the CSP clearly identify how the monitoring data is going to be used to the CSC;

b) it is recommended that the CSP provide a formal monitoring data use declaration to the CSC, such as that illustrated in Figure 10-1.

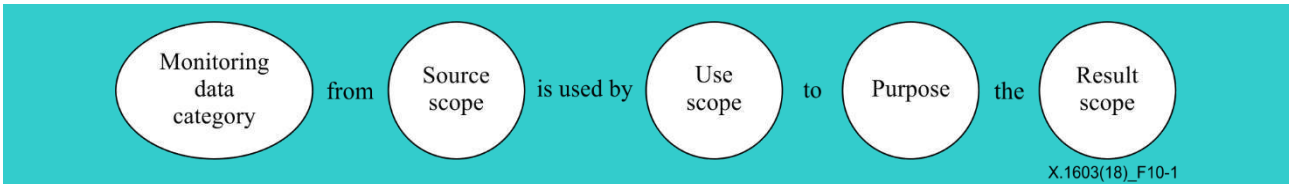


Figure 10-1 – Recommended monitoring data use declaration

c) it is required that the CSP provide notification and obtain CSC permission prior to the use of monitoring data for other than intended purpose;

d) it is required that the CSP support logging and auditing of monitoring data usage.

Table 10-3 provides a summary mapping of monitoring data use security threats to security requirements.

Table 10-3 – Monitoring data use: security threats mapping to security requirements

Security threats	Security requirements
Data misuse	a), b), c), d)
Insider threats	a), b), c), d)
System vulnerabilities	d)
Eavesdropping	d)

10.4 Security requirements for monitoring data migration

The data security requirements for the monitoring data migration include the following:

a) it is recommended that the CSP provide notification to the CSC of monitoring data migration;

b) it is required that the CSP ensure secure transmission during monitoring data migration;

c) it is required that the CSP support logging and auditing of monitoring data migration operations.

Table 10-4 provides a summary mapping of monitoring data migration security threats to security requirements.

Table 10-4 – Monitoring data migration: security threats mapping to security requirements

Security threats	Security requirements
Data misuse	a), c)
Spoofing	b), c)
Tampering and intercepting	b), c)

10.5 Security requirements for monitoring data analysis

The data security requirements for the monitoring data analysis include the following:

a) it is required that the CSP provide notification regarding the purpose of monitoring data analysis to the CSC;

b) it is required that the CSP implement defenses against the vulnerabilities of monitoring data analysis system, for example the CSP should prevent data loss and leakage in the monitoring data analysis system;

Table 10-5 provides a summary mapping of monitoring data analysis security threats to security requirements.

Table 10-5 – Monitoring data analysis: security threats mapping to security requirements

Security threats	Security requirements
Data misuse	a)
System vulnerability	b)
DoS attack	b)

10.6 Security requirements for monitoring data presentation

The data security requirements for the monitoring data presentation include the following:

a) it is required that the CSP maintain the integrity and accuracy of presented monitoring data;

b) it is required that the CSP implement authentication methods to protect access the monitoring data presentation;

c) it is required that the CSP support defenses against the vulnerabilities of the monitoring data presentation system, for example the CSP could use penetration testing methods to prevent vulnerabilities of the monitoring data presentation system.

Table 10-6 provides a summary mapping of monitoring data presentation security threats to security requirements.

Table 10-6 – Monitoring data presentation: security threats mapping to security requirements

Security threats	Security requirements
Data misuse	a), b)
System vulnerability	b), c)
Misrepresentation	a), b), c)

10.7 Security requirements for monitoring data destruction

The data security requirements for the monitoring data destruction include the following:

a) it is required that the CSP provide appropriate destruction methods for monitoring data;

b) it is required that the CSP prevent the unintended destruction of monitoring data;

c) it is required that the CSP prevent the incomplete destruction of monitoring data;

d) it is required that the CSP erase any CSC specific keys for encrypted data;

e) it is required that the CSP destroy copies of monitoring data;

f) it is required that the CSP provide notification of monitoring data destruction to the CSC.

Table 10-7 provides a summary mapping of monitoring data destruction security threats to security requirements.

Table 10-7 – Monitoring data destruction: security threats mapping to security requirements

Security threats	Security requirements
Spoofing	a), b), c), d), e), f)
Operating system vulnerability	b), c), d), e), f)

10.8 Security requirements for monitoring data backup

The data security requirements for the monitoring data backup include the following:

a) it is required that the CSP provide backup methods to prevent monitoring data loss;

b) it is required that the CSP maintain the integrity and accuracy of restored monitoring data;

c) it is required that the CSP support logging and auditing of monitoring data restoration.

Table 10-8 provides a summary mapping of monitoring data backup security threats to security requirements.

Table 10-8 – Monitoring data backup: security threats mapping to security requirements

Security threats	Security requirements
Operating system vulnerability	a), b), c)

Bibliography

[b-ITU-T E.409] Recommendation ITU-T E.409 (2004), *Incident organization and security incident handling: Guidelines for telecommunication organizations*.

[b-ITU-T X.810] Recommendation ITU-T X.810 (1995), *Information technology – Open System Interconnection – Security frameworks for open system: Overview*.

[b-ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing*.

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014), *Information technology – Cloud computing – Overview and vocabulary*.

[b-ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), *Information technology – Cloud computing – Reference architecture*.

[b-ISO/IEC 19440] ISO/IEC 19440 (2007), *Enterprise integration – Constructs for enterprise modelling*.

[b-ISO/IEC 19944] ISO/IEC 19944 (2016), *Information technology – Cloud services and devices: data flow, data categories and data use*.

[b-ISO/IEC 20000-1] ISO/IEC 20000-1 (2011), *Information technology – Service management – Part 1: Service management system requirements*.

[b-ISO/IEC 27000] ISO/IEC 27000 (2016), *Information technology –Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27729] ISO/IEC 27729 (2012), *Information and documentation – International standard name identifier (ISNI)*.

[b-ISO/IEC 29100] ISO/IEC 29100 (2011), *Information technology –Security techniques –Privacy framework*.

[b-NIST-SP-800-30] NIST Special Publication 800-30 (2012), *Guide for Conducting Risk Assessments*.

[b-NIST-SP-800-53] NIST Special Publication 800-53 Rev. 3 (2013), *Recommended Security Controls for Federal Information Systems and Organizations*.

[b-NIST-SP-800-125] NIST Special Publication 800-125 (2011), *Guide to Security for Full Virtualization Technologies*.

[b-NIST-SP-800-145] NIST Special Publication 800-145 (2011), *The NIST Definition of Cloud Computing*.


ENCRYPTION
STANDARDS
SECURITY
DATA PROTECTION
ANALYSIS
PROCESSING
PRIVACY

Guidelines for cloud service customer data security

Recommendation ITU-T X.1641

(09/2016)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Summary

Recommendation ITU-T X.1641 provides generic security guidelines for the cloud service customer (CSC) data in cloud computing. It analyses the CSC data security lifecycle and proposes security requirements at each stage of the data lifecycle. Furthermore, Recommendation ITU-T X.1641 provides guidelines on when each control should be used for best security practice.

Keywords

Cloud service customer data, data security controls, data security lifecycle.

Table of Contents

1 Scope

This Recommendation provides guidelines for cloud service customer (CSC) data security in cloud computing, for those cases where the cloud service provider (CSP) is responsible for ensuring that the data is handled with proper security. This is not always the case, since for some cloud services the security of the data is the responsibility of CSCs themselves. In other cases, the responsibility may be mixed.

For example, in some cases the CSP may be responsible for restricting access to the data, while the CSC remains responsible for deciding which cloud service users (CSUs) should have access to it, and the behaviour of any scripts or applications with which the CSU processes the data.

This Recommendation identifies security controls for CSC data that can be used in different stages of the full data lifecycle. These security controls can differ when the security level of the CSC data changes. Therefore, this Recommendation provides guidelines on when each control should be used for best security practice.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing*.

[ITU-T X.1631] Recommendation ITU-T X.1631 (2015) | ISO/IEC 27017:2015, *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 **authentication** [b-NIST-SP-800-53]: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

3.1.2 **cloud computing** [b-ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

3.1.3 **cloud service** [b-ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.4 **cloud service customer** [b-ITU-T Y.3500]: Party which is in a business relationship for the purpose of using **cloud services**.

NOTE – A business relationship does not necessarily imply financial agreements.

3.1.5 **cloud service customer data** [b-ITU-T Y.3500]: Class of data objects under the control, by legal or other reasons, of the cloud service customer that were input to the cloud service, or resulted from exercising the capabilities of the cloud service by or on behalf of the cloud service customer via the published interface of the cloud service.

NOTE 1 – An example of legal controls is copyright.

NOTE 2 – It may be that the cloud service contains or operates on data that is not cloud service customer data; this might be data made available by the cloud service providers , or obtained from another source, or it might be publicly available data. However, any output data produced by the actions of the cloud service customer using the capabilities of the cloud service on this data is likely to be cloud service customer data, following the general principles of copyright, unless there are specific provisions in the cloud service agreement to the contrary.

3.1.6 cloud service derived data [b-ITU-T Y.3500]: Class of data objects under cloud service provider control that are derived as a result of interaction with the cloud service by the cloud service customer.

3.1.7 cloud service provider [b-ITU-T Y.3500]: Party which makes cloud services available.

3.1.8 cloud service user [b-ITU-T Y.3500]: Natural person, or entity acting on their behalf, associated with a cloud service customer that uses cloud services.

NOTE – Examples of such entities include devices and applications.

3.1.9 infrastructure as a service (IaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer is an infrastructure capabilities type.

3.1.10 multi-tenancy [b-ITU-T Y.3500]: Allocation of physical or virtual resources such that multiple tenants and their computations and data are isolated from and inaccessible to one another.

3.1.11 platform as a service (PaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer is a platform capabilities type.

3.1.12 party [b-ITU-T Y.3500]: Natural person or legal person, whether or not incorporated, or a group of either.

3.1.13 personally identifiable information [b-ISO/IEC 29100]: Any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal.

3.1.14 PII principal [b-ISO/IEC 29100]: Natural person to whom the personally identifiable information (PII) relates.

NOTE – Depending on the jurisdiction and the particular data protection and privacy legislation, the synonym "data subject" can also be used instead of the term "PII principal".

3.1.15 software as a service (SaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer is an application capabilities type.

3.1.16 tenant [b-ITU-T Y.3500]: One or more cloud service users sharing access to a set of physical and virtual resources.

3.1.17 threat [b-ISO/IEC 27000]: Potential cause of an unwanted incident, which may result in harm to a system or organization.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CSC Cloud Service Customer

CSP Cloud Service Provider

CSU Cloud Service User

IaaS Infrastructure as a Service

PaaS Platform as a Service

PII Personally Identifiable Information

SaaS Software as a Service

5 Conventions

None.

6 Overview

6.1 Specification of the data in this Recommendation

CSC data includes private data of customers stored on a cloud platform and related data through cloud services for CSC, such as account information, login record and operation log.

The difference between the terms CSC (see clause 3.1.4) and CSU (see clause 3.1.8) is further distinguished as follows.

The CSC is the person or organization that enters into the legal relationship with the CSP. So the CSC could be an enterprise, a subsidiary, a government department or an individual consumer.

The CSU is the person, device or application that uses the cloud service that has been contracted for. The CSU could be a government employee, an application running on a smartphone, an individual consumer or a member of a household, such as a child. The CSC usually nominates some CSUs to act as administrators and manage the relationship between the CSC and the CSP. A CSU always acts on behalf of a CSC. Most employee CSUs need to have little or no visibility of what or how the CSP operates, or the services that the CSC has contracted for, unless the CSC decides they need to know (e.g. administrators and internal auditors).

A CSC can include multiple cloud tenants. A tenant can include multiple CSUs.

6.2 Data security threats for cloud service customers

As the cloud service environment is typically multi-tenant, loss or leakage of data is a serious threat to the CSC. The lack of appropriate management of cryptographic information, such as encryption keys, authentication codes and access privilege, could lead to significant damage, such as data loss and unexpected data leakage. For example, insufficient authentication, authorization and audit controls; inconsistent use of encryption or authentication keys; operational failures; disposal problems; jurisdiction and political issues; data centre reliability and disaster recovery, can be recognized as major sources of this threat and may be associated with the challenges.

As for the security of storage data, since all CSC data is actually stored in the equipment of CSPs, and the storage resources is shared by different CSCs, it may face several risks, including:

1) CSP insiders with privileges can gain unauthorized access resulting in leakage of CSC data;

2) malicious users or hackers can also gain unauthorized access resulting in leakage of CSC data;

3) cross-border data flow can lead to data leakage, especially for sensitive data;

4) software and hardware failures, power outages and natural disasters can result in data loss.

Data security also lies in the process of transmission. Data can be stolen or tampered with during transmission, thus lead to confidentiality leakage, if the data is not encrypted properly. If CSCs have not adopted adequate encryption, CSPs should verify the integrity of the data and take corresponding encryption measures.

Another threat is the leakage of residual data. When a CSC unsubscribes its service, its data is cleared and the storage space released or reallocated to other CSCs. It is the responsibility of the CSP to ensure that the residual data of one CSC or tenant cannot be recovered by another.

6.3 Existing requirements related to about data security

The security framework for cloud computing specified in [ITU-T X.1601] provides the requirements related to data security, including data isolation, protection and confidentiality protection.

1) Data isolation

   In a cloud computing context, a tenant is prevented from accessing data belonging to another tenant, even when the data is encrypted, except when explicitly authorized. Data isolation may be realized logically or physically, depending on the required isolation granularity and the specific deployment of cloud computing software and hardware.

   NOTE – In cloud computing, isolation occurs at the tenant level. A given CSC may have multiple tenants in the cloud, for example, to separate different subsidiaries, divisions or business units.

2) Data protection

Data protection ensures that CSC data and cloud service derived data held in a cloud computing environment is appropriately secured so that it can only be accessed or changed as authorized by the CSC (or according to applicable law). This protection may include some combination of access control lists, integrity verification, error correction/data recovery, encryption and other appropriate mechanisms. When a CSP provides storage encryption for CSCs, this function can be client-side encryption (e.g., within a CSP application) or server-side encryption.

3) Confidentiality protection

Private information can include personally identifiable information (PII) and confidential corporate data. The collection, use, transfer, handling, storage and destruction of private information can be subject to confidentiality regulations or laws. This restriction applies to both CSPs and their CSCs, e.g., a CSC must be able to permanently delete a data table containing private information, even though the CSP is not aware of the table contents. CSPs may also need to support information handling, e.g., searching of CSC data in its transformed or encrypted form.

Confidentiality protection extends to private information that may be observed or derived from CSC activities, such as business trends, relationships or communications with other parties, and activity levels and patterns.

Confidentiality protection is also responsible for ensuring that all private information (including observed or derived data) is used only for those purposes that have been agreed between a CSC and a CSP.

A risk assessment of private information (called a "confidentiality risk assessment") can assist a CSP in identifying the specific risks of confidentiality breaches involved in an envisaged operation. The CSP should identify and implement capabilities to address the confidentiality risks identified by the risk assessment and treatment of private information.

NOTE – In some jurisdictions, individual natural persons (i.e., human users) are treated separately from their employers for confidentiality purposes. In such circumstances, confidentiality of the CSU will be appropriately protected in addition to that of the CSC or tenant.

6.4 Data security lifecycle

Based on the actual situation of cloud service, the CSC data security lifecycle includes:

1) Creation: This is probably better named creation/update because it applies to creating or changing a data/content element, not just a document or database. Creation is the generation of new digital content, or the alteration/updating of existing content.

2) Transmission: This is the communication process of transferring data from one place to another.

3) Storage: Storage is the act of committing the digital data to some sort of repository, and typically occurs nearly simultaneously with creation.

4) Use: Data is viewed, processed, shared or otherwise used in some sort of activity.

5) Migration: Data migration is the process of transferring data between storage types, formats, or computer systems. It is a key consideration for any system implementation, upgrade, or consolidation. Data migration occurs for a variety of reasons, including: server or storage equipment replacements or upgrades; website consolidation; server maintenance; and data centre relocation.

6) Destruction: Data is permanently destroyed using physical or digital means (e.g., crypto shredding).

7) Backup and restoration: Users can create data backups and restore data from backups.

7 Guidelines for security controls related to data security

This clause provides guidelines for security controls related to the stages of the data security lifecycle described in clause 6.4.

7.1 Security controls in create stage

Guidelines for security controls in the create stage include the following:

a) CSPs should define categories of data sensitivity. User tagging of data may be leveraged to help classify the data.

b) Data should be classified according to its sensitivity when it is created.

c) CSPs should consider enterprise digital rights mechanisms or encryption to protect sensitive data from unauthorized access.

7.2 Security controls in transmit stage

Guidelines for security controls in the transmit stage include the following:

a) CSPs should apply technological methods to ensure the security of the authentication data.

b) CSPs should support users in the maintenance of secure transmission of critical operation data and management data.

c) Damage to data integrity should be detected promptly during transmission and necessary measures taken to restore data integrity after errors are detected.

7.3 Security controls in storage stage

Guidelines for security controls in the storage stage include the following:

a) CSPs should identify access controls available to the CSC to use with users' data from storage repositories, such as those defined in [ITU-T X.1631].

b) CSPs should apply encryption technology or other safeguards to ensure the storage confidentiality of authentication data.

c) CSPs should support users in the maintenance of confidential storage of critical operation data and management data.

d) CSPs should provide effective hard disk protection methods or adopt fragmentally storage mechanisms to prevent unauthorized users obtaining valid user data from the hard disk, even if it is stolen.

e) Damage to storage data integrity should be detected promptly and necessary measures taken to restore data integrity after errors are detected.

f) A user's optional configuration of encryption parameters, such as algorithms, strength and schemas, should be supported.

g) CSPs should support users in the selection of a third-party encryption mechanism to encrypt the key data.

h) CSPs should support data encryption using secure keys and support storage and maintenance of the secure keys locally.

i) CSPs should provide effective virtual machine image file loading protection methods to prevent unauthorized users running their own computing resources from the hard disk, even if it is stolen.

7.4 Security controls in use stage

Guidelines for security controls in the use stage include the following:

a) CSPs should authorize and verify the utilization of data.

b) Utilization of sensitive data should be audited, with audit logs generated.

c) CSPs should apply malicious activity monitoring and enforcement mechanisms according to their responsibility and rights to discover threats and control data usage.

7.5 Security controls in migrate stage

Guidelines for security controls in the migrate stage include the following:

a) Network connectivity should be assessed prior to data migration to ensure the safety of the migration process.

b) CSPs should ensure that data integrity and confidentiality is not affected during a migration.

c) CSPs should ensure that data migration does not affect the continuity of services and applications.

d) CSPs should conduct data backup and recovery-related work appropriately during data migration.

e) CSPs should establish a migration scheme, assess its feasibility and associated risks, then develop risk control measures accordingly as preparations for data migration.

7.6 Security controls in destroy stage

Guidelines for security controls in the destroy stage include the following:

a) CSPs should be able to erase all key material related to encrypted data.

b) CSPs should utilize physical destruction, such as degaussing of physical media when decommissioning storage hardware.

c) CSPs should utilize data recovery techniques to confirm destruction processes.

d) CSPs should be able to provide means to help clear legacy data caused by the migration of data among different cloud platforms, the termination of service and contract, and natural disasters.

e) CSPs should provide means to remove all copies of the data.

f) CSPs should ensure that the storage space for user authentication information, such as the user account and password, are not released or reallocated to other users until that information is fully cleared.

g) CSPs should ensure that the storage space for resources, such as files, directories and database records, are not released or reallocated to other users until those resources are fully cleared.

h) CSPs should provide means to prevent the recovery of destroyed data.

7.7 Security controls in backup and restore stage

Guidelines for security controls in the backup and restore stage include the following:

a) CSPs should utilize content recovery mechanisms, like those for data loss prevention, to assist in identifying and auditing data that needs to be backed up.

b) CSPs should support an appropriate encryption algorithm for long-term (archival) storage media backup, such as the use of long encryption keys and planning for replacement with an improved encryption algorithm.

c) CSPs should provide local data backup and recovery functions. Complete data backup should be conducted at least once a week and the incremental backup at least once a day.

d) A remote disaster recovery centre should be established, with facilities such as communication lines, network equipment and data processing equipment that are needed for disaster recovery integrated into them.

e) A redundancy disaster recovery centre could be established. It should provide a basic equivalent capability for business operation and synchronize data in real time via a high-speed link. It could share the operations of the business and management systems simultaneously while maintaining business continuity through an emergency switch in disaster situations.

f) For data that is categorized as either important or sensitive, the CSPs should provide remote data backup functions together with the capability for timely data recovery. One approach to providing this service would be via a network utilizing a disaster recovery centre.

Appendix I

Guidelines for using security controls

(This appendix does not form an integral part of this Recommendation.)

Table I.1 provides example sets of controls that could be used to meet the guidelines for some example data scenarios based on data classification and lifecycle stage.

Table I.1 – Example sets of controls

Type	Data lifecycle						
	Creation	Transmission	Storage	Use	Migration	Destruction	Backup and restoration
IaaS	7.1 a), b), c)	7.2 a), b), c)	7.3 a), b), c), d), e), h), i)	7.4 a), b), c)	7.5 a), b), c), d), e)	7.6 a), b), c), d), e), f), g), h)	7.7 a), c), d), e), f)
PaaS	7.1 a), b), c)	7.2 a), b), c)	7.3 a), b), c), d), e), f), i)	7.4 a), b), c)	7.5 a), b), c), d), e)	7.6 a), b), c), d), e), f), g), h)	7.7 a), b), c), d), e), f)
SaaS	7.1 a), b), c)	7.2 a), b), c)	7.3 a), b), c), d), e),f), g), h), i)	7.4 a), b), c)	7.5 a), b), c), d), e)	7.6 a), b), c), d), e), f), g), h)	7.7 a), b), c), d), e), f)

Bibliography

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary*.

[b-ISO/IEC 27000] ISO/IEC 27000:2014, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 29100] ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy framework*.

[b-NIST-SP-800-53] NIST Special Publication 800-53 Revision 4 (2015), *Security and privacy controls for Federal information systems and organizations*, Available [viewed 2016-12-10] at: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

SECURITY STANDARDS!

Guidelines for the operational security of cloud computing

Recommendation ITU-T X.1642

(03/2016)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Summary

Recommendation ITU-T X.1642 provides generic operational security guidelines for cloud computing from the perspective of cloud service providers (CSPs). It analyses the security requirements and metrics for the operation of cloud computing. A set of security measures and detailed security activities for the daily operation and maintenance are provided to help CSPs mitigate security risks and address security challenges for the operation of cloud computing.

Keywords

Cloud computing, operational security, security clause of the service level agreement (SLA).

Table of Contents

1 Scope

This Recommendation clarifies the security responsibilities between cloud service providers (CSPs) and cloud service customers (CSCs), and analyses the requirements and categories of security metrics of operational security for cloud computing. It defines sets of detailed security measures and security activities for the daily operation and maintenance for cloud computing services and infrastructure from the perspective of CSPs, to fulfil the requirements of operational security for cloud computing.

This Recommendation will be helpful for CSPs to reduce operational risks. The target audiences of this Recommendation are CSPs, such as traditional telecommunication operators and Internet service providers (ISPs).

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 cloud computing [b-ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

3.1.2 cloud service [b-ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.3 cloud service customer [b-ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

3.1.4 cloud service partner [b-ITU-T Y.3500]: Party which is engaged in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer, or both.

3.1.5 cloud service provider [b-ITU-T Y.3500]: Party which makes cloud services available.

3.1.6 infrastructure as a service (IaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer is an infrastructure capabilities type.

3.1.7 multi-tenancy [b-ITU-T Y.3500]: Allocation of physical or virtual resources such that multiple tenants and their computations and data are isolated from and inaccessible to one another.

3.1.8 network as a service (NaaS) [b-ITU-T Y.3500]: Cloud service category in which the capability provided to the cloud service customer is transport connectivity and related network capabilities.

3.1.9 party [b-ISO 27729]: Natural person or legal person, whether or not incorporated, or a group of either.

3.1.10 platform as a service (PaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the service customer is a platform capabilities type.

3.1.11 security challenge [b-ITU-T X.1601]: A security "difficulty" other than a direct security threat arising from the nature and operating environment of cloud services, including "indirect" threats.

3.1.12 security domain [b-ITU-T X.810]: A set of elements, a security policy, a security authority and a set of security-relevant activities in which the set of elements are subject to the security policy for the specified activities, and the security policy is administered by the security authority for the security domain.

3.1.13 security incident [b-ITU-T E.409]: A security incident is any adverse event whereby some aspect of security could be threatened.

3.1.14 service level agreement (SLA) [b-ISO/IEC 20000-1]: Documented agreement between the service provider and customer that identifies services and service targets.

3.1.15 software as a service (SaaS) [b-ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer is an application capabilities type.

3.1.16 tenant [b-ITU-T Y.3500]: One or more cloud service users sharing access to a set of physical and virtual resources.

3.1.17 threat [b-ISO/IEC 27000]: Potential cause of an unwanted incident, which may result in harm to a system or organization.

3.1.18 vulnerability [b-NIST-SP-800-30]: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACL Access Control List

API Application Programming Interface

BIA Business Impact Analysis

CCTV Closed Circuit Television

CPU Central Processing Unit

CSC Cloud Service Customer

CSN Cloud Service Partner

CSP Cloud Service Provider

DB Database

DDoS Distributed Denial of Service

DLP Data Leakage Prevention

DoS Denial of Service

IAM Identity and Access Management

IaaS Infrastructure as a Service

ICT Information and Communication Technology

IdM Identity Management

IDS Intrusion Detection System

IP Internet Protocol

IPS Intrusion Prevention System

ISP Internet Service Provider

IT Information Technology

JIT Just In Time

LDAP Lightweight Directory Access Protocol

NaaS Network as a Service

OS Operating System

PaaS Platform as a Service

RPO Recovery Point Objective

RTO Recovery Time Objectives

SaaS Software as a Service

SLA Service Level Agreement

SMS Short Message Service

SSO Single Sign-On

VDC Virtual Data Centre

VM Virtual Machine

5 Conventions

None.

6 Overview

With the rapid expansion of the cloud computing market and the establishment of industry chains, security issues continue to be a major and important topic that cannot be ignored. Cloud computing systems are facing more challenges than traditional information technology (IT) systems because they are more complicated, and huge amounts of users' private data have been stored in the cloud. Both security and privacy protection are the most important factors when customers evaluate the use of cloud computing services.

More and more cloud services will be supplied, and methods to guarantee the reliability of these cloud services have become more urgent. It is therefore necessary to thoroughly investigate the operational security of cloud computing to provide guidelines for cloud service providers (CSPs). The guidelines can help CSPs reduce the security risk from improper operation, unreasonable business design, etc., and improve the overall security level of operation for cloud computing services.

From the perspective of CSPs, the main security challenges of operational security are described below:

1) Challenges to the maintenance of cloud computing infrastructure: When cloud computing provides the users with IT infrastructure, a platform or software as a service, the stability, reliability and safe delivery of cloud services are a prerequisite to carry out business. In order to guarantee that customer service is not interrupted, the infrastructure of the cloud system should be ensured for a reliable and stable operation, and the necessary precautions should be adopted to protect the safety and privacy of user's information. Even in the event of a small failure, many CSCs may experience difficulties such as business interruption or data loss. CSPs should seriously consider how to quickly locate the faults and automatically switch to the backup system seamlessly to protect the availability of customers' service.

2) Challenges to the management mode of cloud computing: The characteristics of cloud computing, such as cross-regional services, huge computing power, separation of data management and ownership, distinguishes it from the traditional IT services. These challenges require effective management and co-operation between branch nodes to solve security problems by CSPs. For CSPs, some necessary technical measures, such as security configuration management, etc., a reasonable distribution of management authority, and a set of effective management rules and processes will be needed to prevent the leakage of user data. For example, CSPs should take measures to prevent the internal administrators from overstepping their authority so as to prevent users from abusing the cloud computing resources.

Overall, for the complete security of cloud applications operated on the cloud infrastructure, CSPs should adopt different technological methods and management mechanisms not only to maintain the security, stability and availability of the cloud infrastructure, but also to protect the business continuity and the user data of the cloud services operated.

7 Requirements of the security clause of the service level agreement

The security clause of the service level agreement (SLA) is the critical factor for CSP to obtain the user's trust. The relationship between CSCs and CSPs, such as security responsibility, should be described clearly by the security clause of SLA. CSPs should focus their operational security measures on fulfilling the requirements defined by the security clause of SLA.

7.1 Security responsibility between CSPs and CSCs

The responsibilities of both CSPs and CSCs should be delineated in as far as the security of cloud computing is concerned in accordance with the various control abilities over the infrastructure and resources of cloud computing.

The security responsibilities are closely related with the cloud service mode, as the cloud service mode reflects the resource control capability in the cloud environment for CSPs and CSCs. For instance, compared to platform as a service (PaaS) or infrastructure as a service (IaaS), CSPs in software as a service (SaaS) should undertake more security responsibilities as with a stronger resource control capability on hand.

For the service mode of IaaS, CSPs provide the infrastructure services, such as the virtual data centre (VDC) which includes hosted servers, storage resource, network and management tools. The fundamental security responsibilities of CSPs include physical security, network security, underlying system security and the reliability of the whole cloud infrastructure. CSCs should be in charge of all the security issues above the level of the cloud infrastructure which they purchase, such as the security of the guest operating system (OS), application software, etc.

For the service mode of PaaS, CSPs provide simplified, distributed software development, testing and deployment environment. CSPs should be responsible for the security of the application programming interface (API) of the application environment, the security of middleware, the availability of cloud platform, etc., as well as the security of the underlying infrastructure. On the other hand, CSCs should be responsible for the security of the application services running over the cloud platform environment.

For the service mode of SaaS, CSPs should guarantee the overall security from the infrastructure layer to the application layer, and CSCs should maintain the information security related to them, such as the security of identity management (IdM), password leakage proofing and so on.

Furthermore, CSCs should consider the security issues of the terminals that they use to access the cloud.

7.2 Requirements of the security clause of SLA

7.2.1 General requirements

The security clause of SLA should explicitly specify the security terms of the cloud services, as well as the responsibilities and liabilities of CSPs and CSCs.

From the CSC's perspective, CSCs should be able to stipulate their requirements concerning the security clause of SLA. The security clause of SLA can help them ensure that their CSPs have adequate protection for their information assets, resources and services customized while at rest, in use and in motion, and that corrective mechanisms have been implemented to comply with the regulations on data privacy associated with their governing jurisdiction.

From the CSP's perspective, the security clause of SLA stipulates the requirements and measureable terms of the security of the cloud service provided, which can be assessed, compared and customized by CSCs. CSPs should implement a series of appropriate technological and management mechanisms to improve the reliability and security of the cloud services, and fulfil the requirements of the security clause of SLA, which can ultimately obtain the trust of CSCs. Cloud services may have different types of SLAs due to the content of the services, the service grade, and even the region where the services are provided, but the minimal requirements of the security clause of SLA should meet the legal and regulatory requirements as well as those of related public industry standards.

The specific requirements of the security clause of SLA could be negotiated by CSPs and CSCs based on the customized requirements of CSCs and their control ability over the resources. For CSPs, disclaimer items should be stated clearly in a business contract or a product description to avoid unnecessary dispute or security risk, so that CSPs will not be held responsible in case of *force majeure*.

7.2.2 Elements of the security clause of SLA

The security clauses of SLA include but are not limited to the following elements.

7.2.2.1 Business continuity

CSPs should deploy adequate protection in case of a man-made or natural disaster to ensure service availability and business continuity. The detailed items or requirements are shown below:

1) Service availability

   The percentage of time at which the service is usable in a given period of time. For a given cloud service, the terms of its service ability should not be lower than the traditional information and communication technology (ICT) service generally.

2) Average recovery time

   The time to recover the lost data or resume the service from a fault occurrence or other disasters.

7.2.2.2 Data security protection

CSPs should have a comprehensive protection program to protect the CSC's data and other privacy information, and CSPs and CSCs should reach an agreement on the detailed mechanisms and requirements.

1) Storage physical security

   CSPs should implement measures to ensure storage physical security, such as entrance guard, fire protection system, backup power supply system, etc.

2) Data storage medium protection

   CSPs should deploy protection measures such as device reinforcing, patch upgrading and so on, to enhance the security of data storage medium.

3) Data encryption

   It should be stated which data is being encrypted in the process of storage or transmission, and the details of the encryption algorithms.

4) Data access control

   The access control measure of data should be specified to prevent illegal access.

5) Data isolation

   It should be noted that the data of different CSCs are isolated logically or physically.

6) Data deletion

   It includes the assurance of data deletion. It should be assured that the data be deleted permanently before the resources could be allocated to other CSCs.

7) Data backup

   It includes the terms of recovery point objective (RPO) and recovery time objective (RTO), retention policy, combination of on-site backup and off-site backup, etc.

8) Data operation audit

   CSPs should audit the operation of CSCs' data and be able to detect abnormal operations; the auditor should be certified to be qualified for auditing.

9) Data compliance

   Data collection, transfer, handling, storage and destruction should comply with the applicable regulations and laws in the CSC's governing jurisdiction. Similarly, the requirement of data retention should also comply with the allowed retention time of different jurisdictional restrictions.

7.2.2.3 Emergency response

CSPs should provide a hotline service number to provide a fault reporting service, available 5*8 or 7*24. Additionally, the service indicators should include failure acceptance time, troubleshooting time, and so on.

7.2.2.4 Security measures

CSPs should provide appropriate security measures for the whole cloud computing infrastructure.

1) Measures on computing virtualization

   CSPs should implement available measures to provide flow inspection, virtual firewall or other security features in the hypervisor layer, which can keep the behaviour of intra-virtual machines (VMs) visible and controlled by administrators.

2) Network and domain isolation

   CSPs should implement network and domain isolation measures, such as firewall, access control list (ACL) policies in routers, and domain controllers to keep strict isolation of different CSCs.

3) Privileged access

   CSPs should implement measures, such as just in time (JIT) access, to ensure privileged access.

4) Authentication

   CSPs should implement strong authentication methods, such as multi-factor authentication, fingerprint authentication, etc., to reinforce the security of the authentication.

5) Measures to secure network traffic

   CSPs should implement available measures to resist denial of service (DoS)/distributed denial of service (DDoS) attacks and circumvent network congestion, deploy intrusion detection or prevention systems to resist network intrusion.

6) Measures against malware

   CSPs should implement available measures to prevent infection by malware or virus.

7) Patch upgrade

   CSPs should regularly implement patch upgrade and version upgrade for the virtualization software, the operating system and database (DB) to keep them up to date.

7.2.2.5 Security audit

CSPs should carry out regular security audits over the whole cloud computing system. The audit can be executed by an internal independent audit team or third-party auditors (acting as cloud service partners (CSNs)). The audit results should be appropriately visible to CSCs.

7.2.2.6 Security monitoring for improving SLA

CSPs should provide a mechanism to monitor the quantitative parameters of services to improve SLA.

1) Monitoring objects

   Define the monitoring objects, such as the central processing unit (CPU) utilization, security warnings, and so on. The trigger condition should also be explicitly indicated.

2) Security event notification

   The mode and time of security event notification should be stipulated. The notification mode includes e-mail, telephone, short messages or other ways negotiated by CSPs and CSCs. The notification time means the average time from the event occurrence to notifying CSC.

   CSPs may provide appropriate capabilities for CSCs such as service-level self-monitoring and automatic supervision of the resources allocated to them.

7.2.2.7 Security certification

CSPs should be responsible for the acquisition of relevant security certifications, and they should regularly update these certifications to meet the requirements of CSCs.

The engineers and other CSP staff should take security training courses and should be qualified for the operations of the cloud computing platform.

7.2.2.8 Security activity documentation

CSPs can provide the security documents which show the efforts made to enhance the security of their cloud service, such as the security measures implemented, the security management procedures, and so on. The documents should be accessed conveniently and can be viewed or downloaded from their web portal.

8 Guidelines of daily operational security

CSPs should implement security measures and security activities for administrators and tenants in their daily security operation. The security clause of SLA should be achieved and guaranteed by security measures and activities implemented by CSPs. These security measures and activities include but are not limited to the following:

1) **Security measures**: CSPs are required to implement sets of security measures to provide basic capabilities and facilities to enforce the operational security of cloud computing.
   a) Identity management and access control is specified in clause 8.1.
   b) Data encryption and key management is specified in clause 8.2.
   c) System security monitoring is specified in clause 8.3.
   d) Disaster recovery is specified in clause 8.4.
   e) Security configuration management is specified in clause 8.5.
2) **Security activities**: CSPs are required to perform routine security activities to address security problems, securing the operation of cloud computing.
   a) Security events processing is specified in clause 8.6.
   b) Patch upgrade is specified in clause 8.7.
   c) Securing configuration management is specified in clause 8.8.
   d) Emergency response is specified in clause 8.9.
   e) Backup is specified in clause 8.10.
   f) Internal security audit is specified in clause 8.11.

8.1 Identity management and access control

8.1.1 Identity management

CSPs should provide unified identity management for internal administrators and external tenants, which can furnish the raw data for unified access control, authorization and audit.

1) It should support identity federation, which can achieve account information sharing, synchronization between different cloud applications in the same trust zone.
2) It should support life cycle management of identity, which include the whole life cycle control of identity, such as identity register, role and privileges assignment, privileges modification, identity deleting, etc. Furthermore, the registration and modification of identity should have the procedure of approval by administrators.
3) The policies of identity management include identity account naming policy, identity account application policy, etc. These sets of security policies should include:
   - The name of the identity account should be unique in the same trust zone.
   - The identity account should be locked when invalid passwords are input continuously.
   - The identity account should be disabled when unused for a long time.
   - The identity account should be forbidden when trying to log in repeatedly during a very short time.
4) In the framework of unified user account management, the account should be accurate to be associated with special individuals or a tenant. The users should be identified by the main account, and each user (administrator or tenant) should have only one main account. The main account can create a sub-account, and the sub-account can have the authorized privileges to manage the network cells, database servers, application servers, etc.

5) The unified account audit should mainly focus on the assignment of identity account, and the behaviour of log-in and log-out according to the access control modules, which can help to dig out the illegal accounts and overdue accounts, detect the account of over-authorization and lack of authorization, and prevent log-in attempts with abandoned accounts or faked accounts. It should submit the security events of accounts to the security audit module or systems to carry out a wider range of audit function, such as intrusion detection, fault monitoring audit, and so on.

6) It should support user password management, which includes the unified sets of user password policies based on the security policy of cloud platform, such as cryptographic algorithms, the length of a password, the complexity of a password and the cycle of password updating. It should support various types of passwords, such as graphical passwords, sound-based passwords and so on. Furthermore, it should support the functions of password synchronization and password reset.

7) It should provide self-service for tenants in account management. Some management work can be done by the tenants themselves, such as the modification of some simple user properties and password updating, which can lighten the maintenance burden of the management staff.

8.1.2 Access control management

CSPs should establish a unified, centralized authentication and authorization system to improve the security of access control in daily operation. Operational logs for access control to cloud computing systems should be recorded for later audit.

1) Unified authentication should support the functions below:

- Support single sign-on (SSO): It should support the parameters setting of SSO, such as the maximum session time, maximum idle time and maximum cache exist time.
- Support mainstream authentication technology, such as LDAP authentication, digital certification authentication, token authentication, biometric authentication, multifactor authentication and so on.
- Provide detailed authentication logs. It includes system identifications, logging users, log-in time, log-out time, log-in Internet protocol (IP) address, log-in terminal, logging results records (success or failure).
- Provide differentiated, optional authentication methods according to various systems and services. It can meet the balance between the security level and ease of use and even cost.

2) Unified authorization should support the functions below:

- Provide authorization to access cloud resources, according to the predefinition of users, user groups, and users' privileged level.
- Support the mechanisms of centralized authorization and hierarchical authorization, and the authorization range of hierarchical authorized administrators should be restricted by the authorization administrator.
- Support fine-grained authorization policy and coarse-grained authorization policy.
- Provide detailed authorization logs, including IP addresses, operator, authorization time, as well as granted and cancelled permissions.

3) Other requirements

- Control on accessing logs. CSPs should ensure that when administrators can access the logs, they have granted privileges to do so. The tenants should have privileges granted by the administrators to view the logs related to them appropriately through a self-service portal website or other client tools.
- Mechanisms of encryption. The sensitive data such as authentication data, authorization data, etc. should be encrypted in the procedure of storage and transmission.
- All the operational logs related to CSC should be visible appropriately.

8.2 Data encryption and key management

Encryption and key management are the core mechanisms to protect data in cloud computing systems. Encryption provides a resource protection capability, while key management provides cryptographic keys control which are used to protect resources.

The specific implementation of encryption should be clearly defined in the security clause of SLA. Furthermore, the encryption should follow the relevant industrial and governmental standards. CSPs or CSCs should seriously consider the following elements:

1) Encryption of data transmission in network. It is especially important to secure credentials such as financial information, passwords, etc.

2) Encryption of static data on the disk or in the database. It could be used to prevent malicious CSPs or malicious neighbour tenants.

3) Encryption of data in backup media. It could be used to prevent data leakage in case the backup media were lost or stolen.

If CSP is the main enforcer of data encryption, key management is an essential issue in daily operations. CSP should define and execute an integrated key management in the life cycle including the generation, use, store, backup, recovery, update and destroy. CSPs should also consider the following issues:

1) Protection of key storage: Key storage must be protected as any other sensitive data or even its security level must be higher than others. Only a specific entity can access the key storage. Related policies are also needed like separation of roles to enforce a stronger access control.

2) Backup and recovery: As an unexpected loss of a specific key may destroy a service, it is necessary to implement a key backup and recovery solution.

3) Introduction of the third party for key management: By a series of task separation, it could help CSPs avoid conflict with legal requirements when data in cloud computing systems is claimed to be provided.

8.3 System security monitoring

In daily operations, CSPs should undertake centralized real-time security monitoring on the cloud platform and infrastructure, which includes the running status of various physical and virtual resources. By considering the key terms of SLA (such as network performance, utilization of host resource and storage, etc.), and analysing all kinds of logs, CSPs can perform fault management, performance management and automatic inspection management to achieve the goal for real-time or quasi real-time monitoring of the health status of cloud resources.

In general, the monitoring logs are managed and strictly protected by CSPs. Nevertheless, once needed by CSC, CSP could provide CSC with related monitoring logs as they claimed, for instance, CSC might need related monitoring logs to do trouble shooting in emergency response.

CSPs can also proactively detect potential operational risks and resolve them timely. Furthermore, CSPs should provide the capability of correlation analysis between CSCs and their services provided by CSPs, which can be implemented to diagnose the quality and security status of cloud services.

There are two kinds of security monitoring modes: automatic monitoring and manual inspection, which rely on the technical means and management of individual CSPs. The object of security monitoring involves:

1) Health status monitoring of the cloud computing infrastructure: CSPs should provide the capability to collect and monitor the security event logs, vulnerability information, alteration of security device configuration, performance and operational status on all objects of the cloud computing infrastructure, which include virtual machine (VM) resources, cloud computing management platform, security devices, database, etc. This monitoring can help CSPs to keep a perceptive awareness of the overall health status and operating status of the cloud infrastructure.

2) Abnormal behaviour detection: The abnormal behaviour includes illegal log-in, illegal access to cloud management platform and violation access to other resources, the abnormal modifications of the configurations of network equipment and virtual machines, or other penetration attacks, which can be implemented by technical means, such as integrated auditing tools, DLP software or other security tools.

3) Abnormal network traffic monitoring: CSPs should have the capability to detect and analyse abnormal traffic in the physical network and the virtual network, especially intra-VMs traffic. It is necessary to keep awareness of network traffic and performance status, which can help CSPs improve the defence capability against worms, abnormal traffic attacks, and other potential security threats in the cloud computing environment.

4) Physical security monitoring: The objects of physical security monitoring include the temperature and humidity control system, closed circuit television (CCTV), entrance guard, a fire protection system, air-conditioner, a power supply system, surveillance, protective cages, etc., which can be inspected daily.

Above all, CSPs should run a full range check of the cloud computing environment to get the health status of the cloud computing services in the daily operation and maintenance. This can help CSPs quickly detect various indications, such as network performance quality, VM performance and CSC-oriented service quality, etc. Furthermore, the checking process can be customized to support threshold or even baseline value alerts. Based on the monitoring information gathered, CSPs should be able to quickly find the problems in the network, storage, physical machines and virtual platforms when failure happens.

CSPs should also have the capability to locate the other potentially affected CSCs by correlation analysis on each specific failure, based on the assumption that CSCs have the same weaknesses, the same applications, and the same specific version of OS, etc.

8.4 Disaster recovery

CSPs should implement security measures for disaster recovery with the same security level as the original systems. The security measure technology includes server clusters, synchronous remote mirroring and asynchronous remote mirroring to achieve a hot-standby capability for disaster recovery.

1) Server clustering

   Server clustering can coordinate and manage the errors and failures of the separated components, and can add components to the cluster transparently, with elasticity and scalability to reach a sufficient performance.

2) Synchronous remote mirroring

   Through remote mirroring software, the data of the primary site is synchronously replicated and transmitted to a remote site. Once the primary site fails, the running programs would switch to the remote site. The synchronous remote mirroring can guarantee business to continue without loss of data. The cost of this method is high as it depends on a delicately designed mirroring software and sufficient bandwidth of network. Synchronous remote mirroring is regularly implemented in systems of high security level.

3) Asynchronous remote mirroring

   This is another remote mirroring method which usually has a lower cost than the synchronous remote mirroring. The data of the primary site is periodically replicated and transmitted to a remote site. If things go well, it can ensure a complete copy in the remote site without degrading the performance of the primary site. But if something goes wrong during the mirroring period, loss of data is inevitable. Asynchronous remote mirroring could be chosen after a sufficient risk evaluation.

8.5 Security configuration management

Security configuration includes security rules configured in the cloud platform, network, virtual machines and various application components. It is different from a high-level security policy, which sets out the organization's approach to achieve its information security objectives.

CSPs should execute the integrated security configuration management to provide efficient implementation and fast deployment of the security configuration.

In security configuration management, it is suggested that CSPs set security policy configuration templates and security configuration policy baselines. Furthermore, CSPs should take measures to ensure the consistency and efficiency of security configuration when cloud environment changes and to isolate the security configuration between CSCs in a multi-tenancy environment.

Security configuration templates include main templates of security configuration that the current cloud computing environment needs, such as account management, authentication, access control policies, audit policies, dynamic response policies, application and software update policies, backup and recovery policies, etc.

Security configuration baselines provide a criterion for the security configuration requirements of the entire cloud computing environment, which can help CSPs evaluate whether the current security configuration meets the fundamental security level or not, and further provide detailed guidance to reinforcement. The categories of security configuration baselines should include but are not limited to the following: OS security configuration baselines, database security configuration baselines, firewall security configuration baselines, switch security configuration baselines, router security configuration baselines, etc.

Security configuration management involves the following measures:

1) Security configuration template management

   CSPs should set the main security templates for the demands of cloud environment to make security configuration deployment faster and more convenient. Security configuration template management should support customized templates, update and optimize templates continuously according to the changes of cloud platform, network status, service requirements, and so on.

   Furthermore, CSPs should provide CSCs with the capability to customize new security configuration templates according to their own requirements. Additionally, CSCs should be responsible for the effectiveness of the security configuration which they customized.

2) Security configuration process management

   CSPs should testify the effectiveness of the security configuration. Security configuration can be configured according to CSCs' and cloud services' requirements. The main process of security configuration management involves configuration request, configuration approval, testing and technical validation, implementing, configuration archiving and output report.

3) Security configuration baseline management

   CSPs should develop security configuration baseline by comprehensively considering the security requirements of cloud computing platform, cloud service, CSCs, the security clause of SLA, etc.

   The main process of security configuration baseline management involves security configuration checking request and record, approval, checking implementing, checking report output, reinforcement implementing, and reinforcement report output. Security configuration checking should be executed periodically during daily operations, and can be implemented through configuration collecting and baseline security analysis.

4) Security configuration conflict management

   In a resource sharing cloud environment, due to faults caused by either the security administrator or by other reasons, the security configuration might be compromised which may result in vulnerabilities in the cloud computing environment. CSPs should implement efficient measures to detect security configuration conflicts, and establish a security configuration conflict handling process and retrieval mechanisms.

   The handling process of security configuration conflict should involve conflict alarm, conflict analysis (which includes reasons and influences analysis), conflict handling and output report.

5) Security configuration migration management

When cloud computing resource or service changes (such as service capacity expansion, VM migration, etc.), CSPs should provide dynamic security configuration adjustment means. For example, during VM migration, automatic security configuration policy migration can be implemented through migration status sensing, automatic matching and redeployment of the original security configuration policy, which could ensure security configuration policy consistency and fast deployment in cloud environment, and improve the efficiency of the security operation.

6) Security configuration isolation management

In a multi-tenancy environment of cloud computing, CSPs should execute strict classification management of CSCs' security configuration, and take measures such as authentication, access control, etc. This is to ensure security configuration isolation between different CSCs.

8.6 Security event processing

CSPs should take certain activities to handle security events in cloud computing environment, such as threat alarms, vulnerability, emergency, etc. CSPs should also deploy technical measures to assist in detecting, alarming and handling of security events.

In general, the procedure of security events processing in the cloud computing environment involves the following steps: detecting, analysing, disposing, checking, reporting and recording. CSPs should explicitly specify the responsible persons in each step.

8.6.1 Detecting

CSPs should take measures to monitor the security status of the cloud platform mentioned in clause 8.3, and have the abilities to send timely alarms whenever the security events happen. They should ensure that alarms can be sent to the designated person, such as the security manager of the cloud computing platform. The alarms could be sent through e-mails, phone calls, short message service (SMS), etc. CSPs should be sure to monitor all kinds of security events stated in the security clause of SLA.

8.6.2 Analysing

CSPs should confirm the security events after receiving alarms, then analyse and diagnose them to determine the types of events, their causes and handling measures. CSPs can contact CSCs for assistance, if needed.

8.6.3 Disposing

CSPs should take handling measures according to the security events' types and levels, to minimize the impact of those events. CSPs should refer to the security activities mentioned in clauses 8.7, 8.8 and 8.9, which include but are not limited to the following:

1) For a security emergency, CSPs should take actions according to the emergency response plans.
2) For a security vulnerability, CSPs should take actions according to patch upgrade.
3) For a configuration weakness, CSPs should take actions according to securing configuration management.

CSPs should monitor and assess the security events dynamically, and inform CSCs of related information and handling progress.

8.6.4 Checking

After disposing of the security events, CSPs should further analyse the reasons and situations that may cause the security events, and check if other CSCs' system has similar vulnerabilities that may cause the same security events. If the vulnerability exists, CSPs should notify the related CSCs immediately and take corresponding actions. The notification should not involve any privacy of other CSCs.

8.6.5 Report and recording

CSPs should generate security events processing report which includes the security events' behaviour, causes, handling measures, etc., and send it to the related CSCs within the time limit stated in the security clause of SLA. CSPs should record the information of security events for later inspection and auditing. The appropriate reports can be given to the affected CSCs and applicable third-party auditors (acting as CSN).

8.7 Patch upgrade

8.7.1 Responsibilities

CSPs should optimize the patch management process of the cloud platform to reduce potential risks caused by vulnerabilities, and protect the stable operation of cloud platforms and services.

In cloud computing, the management of patches should be corporately implemented between CSPs and CSCs.

1) Responsibilities of CSP:
   - Following the vulnerability releases of mirror operating systems and timely finding the latest patches;
   - Testing security and adaptability of the patches;
   - Updating the patch of the mirror operating system and creating the latest image files;
   - Informing and helping CSCs to finish the patch update, and ensuring that the same vulnerability will not exist;
   - Implementing the effect test of these latest image files by creating a new virtual machine.
2) Responsibilities of CSC:
   - Helping CSPs follow the vulnerability releases and finding the latest patches;
   - Timely updating the virtual machine patches according to the information from CSPs.

Depending on the service mode of cloud computing, such as IaaS, PaaS and SaaS, CSP is only responsible for the resource controlled by itself, and so does CSC. For IaaS, CSPs should be responsible for the patch upgrade of the cloud computing infrastructure, and CSCs of the guest OS, application software and so on, which are controlled by CSCs.

8.7.2 Process of upgrading security patch

The components of the cloud platform that need patching include virtualization software, operating systems, network equipment, security equipment, database servers, management terminals, and other components of the cloud platform. The closed-loop process of patch upgrade involves four stages as shown below, which could help CSPs ensure the best timeliness on patching of their cloud platform.

1) Patch collect

CSPs should collect patch information from the vendor's official patch update website, use the automatic patch updating tools released by the vendor, or through other means to guarantee the integrity of the patches' requirements. CSPs should make an analysis of the patches collected, seek and record the vulnerabilities of the existing systems and applications, evaluate the potential effects and risks of patching and to determine the urgency and importance of the patches.

2) Patch test

CSPs should start a patch test to check the security, compatibility and stability of the patches. They should establish a test environment to emulate the target platform or systems before the patching stage. After testing, a report should be generated, which could suggest whether the patches should be released or not. The test report also provides detailed technical guidelines for patching steps and the program of rollback. It should provide a full description of the patches to help the patching engineers understand the functions and operations of the patch, the effects on the systems and applications, such as the problems generated by the patch, the affected systems, the affected files, whether the system or application should be reloaded or not, etc.

3) Patch update

CSPs should make an operation plan for patch update which includes the detailed operation steps according to the test report of the patch. An emergency plan should also be formulated which includes system and data backup, application switching, patch release timing control, patch uninstall and system rollback, in case of patch failure. For the large-scale patch release, CSPs should call for technical support from the vendors in advance to improve the emergency treatment capability upon unexpected situations.

CSPs should also be transparent with CSCs when the patch is released on the cloud platform, and they should communicate clearly with CSCs before patching. CSPs should try not to influence in any way CSC's services, and this is through adopting appropriate measures together with CSCs.

4) Patch check

After the patches are released, CSPs should regularly check the patches with patch management tools to make sure that the patches of the whole cloud platform are the latest. The document of patching records should be updated regularly and should be archived for later security audits.

The waiting time between patch collect and update and CSCs approval requirement of patch update should be explicit in the SLA, based on the priority type of the patch (e.g., critical, high, medium, and low).

The following is an example of a process of updating security patches, including updating the virtual machine and its image files. . In this process, if there are any latest patches being released, CSPs will test the security and adaptability of these patches. In addition, CSCs have the responsibilities to find and collect the latest patches. After a successful test of these latest patches, CSPs will inform CSCs to update these patches. At the same time, CSPs will update the patches of the current image files. CSPs could then create a new virtual machine with these new image files. CSPs will also implement a specific scan to make sure that CSCs have updated these patches successfully.

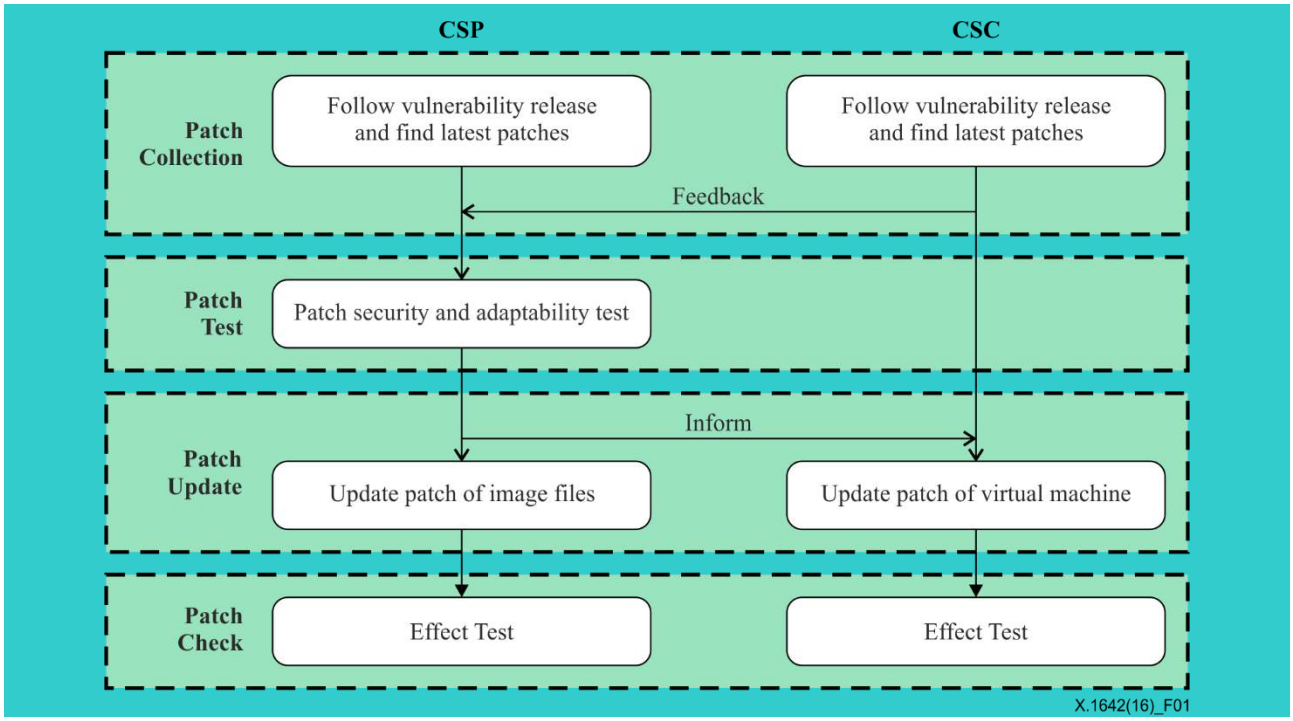


Figure 1 – Example process of upgrading security patch

8.8 Securing configuration management

CSPs should execute the security controls of the configuration management of the cloud platform, network configuration, and parameters of various application components, which could help reduce the operational risks induced by mis-configuration or misuse, and promote the security and stability of the cloud computing environment.

Configuration management usually includes configuration alteration management and release management. CSPs should take measures ensure that the configuration alteration and release have been monitored and recorded. For convenience of configuration management, an integrated configuration management database is usually constructed, which involves the current and historic records of all configuration files, security policy, the application profiles of each element and the component of cloud computing. CSPs should protect this database from non-authorized access, information leakage, etc.

Configuration management security involves the following measures:

1) Configuration management auditing

   Configuration management auditing is to ensure that the configuration alteration and release requirements have been implemented effectively and efficiently. It can help CSPs verify the correctness, consistency, completeness, validity, and traceability of each configuration item. Configuration management auditing should be executed periodically during the daily operation.

   All logs of user access, modification, archive and retrieval should be recorded and archived for online or offline audit.

   Furthermore, the report of configuration management auditing related to CSCs or their services should be appropriately visible to CSCs, to enable CSCs to supervise the security measures and the effectiveness of CSPs.

2) Configuration management monitoring

   CSPs should monitor all the alternations and other operations of configuration files of an entire cloud computing environment, to prevent non-authorized access, leakage, illegal modification and mis-configuration.

3) Configuration management database protecting

   CSPs should do precise maintenance and management of the configuration management database, such as role-based authority assignment, garbage removal, regular auditing, periodical backup, etc.

8.9 Emergency response plans

It is critical to ensure that the cloud computing systems are able to be operated effectively by CSPs without excessive interruption following a security incident. An emergency response plan supports this requirement by establishing an effective programme, procedures, and technical measures.

In order to reduce the impact of security incidents on the cloud computing platforms and services, CSPs' emergency response plan should provide a clear guidance for operators and strike a balance between the level of detail and degree of flexibility. The development and management of an emergency response plan is a cycle of continuous improvement process consisting of three phases: development phase, testing and implementation phase, and maintenance phase.

8.9.1 Development phase

Above all, the quantitative and qualitative analysis methods should be adopted to make a comprehensive risk assessment and business impact analysis (BIA) of the cloud computing systems. After that, the key features and components of the system could be obtained, as well as the impact of different security incidents. On this basis, according to the security clause of SLA between CSPs and CSCs, the regulatory requirements, and the recovery target of the emergency response can be formulated such as the scope of RTO and RPO. Furthermore, the characters of cloud service and classification of incidents should also be considered while developing an emergency response plan.

The emergency response plan includes:

1) Notification: A notification procedure should be developed to notify the response team, management staff and related CSCs once a security incident occurs.
2) Classification and grading of security events: The security assessment of a security incident should be implemented by the emergency response team to determine its category and grade.
3) Launching: After the classification and grading of the security events, it is urgent for CSPs and CSCs to activate the correspondingly pre-established response programme.
4) Action: After activating the response programme, countermeasures should be launched immediately to suppress the impact of security incidents. Additionally, recovery operations should be taken right after the incidents are effectively controlled.
5) Post-disposal: After the emergency action, it is important to make a conclusion of the latest emergency response, which includes actions to analyse and summarize the reasons for the incident, take the assessment of the loss and make the evaluation of the effectiveness and efficiency of the emergency response plan.

Furthermore, some details are essential, including:

1) The emergency response team members, the specific responsibilities and the contact information of each team member. Generally speaking, the emergency response team consists of management, business, technical, and administrative staff.
2) The BIA results involving the relationship between the various parts of the cloud computing system, the priority level of key components, etc.
3) The criterion procedures and checklists of the cloud computing system recovery.
4) The inventory of hardware, software, firmware, and other resources to support CSPs' daily operation, with each entry containing specifications like versions, quantities, etc.
5) The contact information of CSCs and the response procedures negotiated by the CSPs and CSCs according to the security clause of SLA to minimize CSCs' loss in a security accident.
6) Generally CSP could not have the privilege to access CSC's private data unless CSP have obtained the authorization of CSC. In the case of emergency launched by CSC, CSC might need CSP's help to make response more effectively and would give CSP the authorization for the data. As a part of compliance, CSP should not abuse the authorization to access CSC's data.

8.9.2 Testing and implementation phase

In order to test the effectiveness of the emergency response plan, CSPs should organize testing and drills of the emergency response plan, with the help of related personnel familiar with the response procedures. The testing and drills should meet the following requirements:

1) The programmes of testing, training and drills should be pre-established.
2) The detailed process of testing, training and drills should be recorded and reports should be written to this effect.
3) CSPs and CSCs are recommended to corporately complete a planned testing whenever significant changes occur inside or outside the cloud computing condition.

When security incidents or business interruption occurs, the emergency response plan should be strictly enforced once the conditions for the launch are met, and all operation logs should be recorded during the whole emergency process. Afterwards, according to the security clause of SLA, CSP should submit the response reports to CSCs.

Based on the testing, drills and implementation results, the emergency response plan should be revised to improve its effectiveness and feasibility.

8.9.3 Maintenance phase

To remain effective, the emergency response plan should always be maintained in a ready state that could reflect the requirements of the cloud computing systems, the SLA modification, configuration changes, and personnel changes. Generally, the plan should be reviewed annually to accommodate the changes of the actual cloud computing environment. The modification of the plan is based on the following elements:

1) The changes of premises, facilities, resources and services.
2) The changes of the security clause of SLA requirements, critical security configuration, significant patch upgrading and backbone team members.
3) The assessment of the plan's effectiveness upon the detailed records of the actual implementation of the plan during the testing and security accidents.

8.10 Backup

Backup capability is an important issue for CSCs and CSPs in the cloud computing environment. Before running the backup activities, CSPs need to address some specifications such as:

– the backup strategy for each CSC or a specific cloud service;
– the storage method including encryption or not;

- the storage location including local and/or remote;
- the retention periods for backup data;
- the procedures to test the backup data.

Before choosing CSP, CSC should confirm whether that CSP could meet the security clause of the SLA including the capability of backup. If CSP does not provide a backup capability, CSC should fully consider a backup strategy and implementation. Otherwise, if CSP provides a backup capability, then CSC should cooperate with CSP to carry out backup operations.

CSP should share the essential details of the backup mechanism with CSCs. When dealing with backup, CSPs should address the specifications to meet each of the following CSC's requirements:

1) Backup strategy: Since each CSC has individual needs in backup, the related factors should be primarily considered, which include:
   - Reasonable recovery point objective (RPO) and recovery time objectives (RTO). RPO indicates the time span between two consecutive backup activities, while RTO reflects how long it takes to roll-back to a backup.
   - Reasonable retention policy: The policy should specify the copy number of a backup.
   - Reasonable combination of file-level backup and virtual machine level backup: The combination should satisfy an optimal investment cost, which is based upon RPO and RTO.
   - Reasonable combination of on-site backup and off-site backup: The on-site backup is stored in the local site, which could meet the need of fast disaster recovery. The off-site backup is stored in a remote site, which is needed to cope with a major disaster. The combination depends on the requirement of the security clause of the SLA, and the investment cost.
   - Regular test procedures of recovery: The recovery test is the ultimate method to verify the validity of a backup.
2) Task arrangement: Once the backup strategy is determined, CSPs should make an appropriate task arrangement of backup operations. To reduce the impact on the performance of the cloud computing infrastructure, the backup task arrangement should depend on CSC's backup requirements, the network traffic pattern and the backup capability of CSP.
3) Procedures to check the validation of backup: A complete and correct data copy means a successful backup operation. Generally, the procedures should contain the following two main steps:
   - Using a one-way hash function to verify that the backup is consistent with the original data. If the backup is the same as the original, then go to the next step. Moreover, a digital signature method could be used to verify the backup operator, which can introduce some benefit to the management of backup operation.
   - Taking a recovery test for the backup. As the continuous change in the cloud computing environment, regular recovery test is critical.
4) Prudence about the snapshots of the virtual machine: In a cloud computing scenario, the snapshot method provides a quick and easy means of rollback, which could act as a backup method to a certain extent. However, the snapshot method should not be used frequently due to the following reasons:
   - Snapshots allow the same data to multiply and to be written in different snapshot files, which could easily bring about serious performance degradation and rapid storage occupancy in the cloud computing systems.
   - In order to reduce storage occupancy, a chain of an original virtual machine snapshots is often configured to merely contain the difference from the first snapshot. Once the first snapshot is destroyed, the successive snapshots would end up being invalid. The security risk is magnified as the rate of successive snapshots increases.

8.11 Internal security audit

Due to the wide range of security audit, this Recommendation only focuses on the internal security audit from the perspective of the operational security. A reliable and objective security audit can help to ensure that operational risk management activities have been thoroughly tested and reviewed, to enhance the transparency of cloud computing services, and even to meet the regulatory requirements.

8.11.1 Requisites of security audit

To ensure the objectivity and reliability of the security audit, CSPs and CSCs should negotiate to reach an agreement on the use of a common IT control and certification assurance framework, and the means how to collect, store, and share the audit trail (such as system logs, activity reports, system configurations). According to the security clause of the SLA between CSPs and CSCs, the security audit should be planned and targeted to satisfy some requisites:

1) Team and function: Firstly, the audit team members should include senior management, and staff from different business departments (administrative, and technical) to ensure fairness and scheduling of resource during the audit process. Secondly, the audit objective should include verifying the security management architecture of CSPs and/or CSCs, and validating the effectiveness and correctness of risk control measures. Thirdly, the audit process should be controlled by the audit team and should comply with the standardized workflow. Finally, the security audit should be carried out repeatedly in a proper period.

2) Requisites for the audit process: Firstly, and based on the above, audit activities should be fully recorded and well planned to avoid interrupting CSPs' or CSCs' business process. Secondly, the scope of the audit objectives and required resources should be clearly defined and guaranteed for their availability. Lastly, all the audit procedures and requirements should be documented as well as the audit team members' responsibilities.

3) Protection of audit tools: The use of audit tools should be restricted and standardized to avoid the misuse of cloud computing resources.

8.11.2 Specific audit requirements

Compared with the security audit procedures in the traditional information systems, the audit team members are especially required to be familiar with the challenges brought by virtualization and other cloud computing technologies. At the same time, the audit category need to expand from traditional security logs to the operation and maintenance of data, business data, and even the storage location of the user data. The audit items include but are not limited to:

1) Virtualization security audit: The main audit requirements include the means of encryption and integrity check for virtual image files, isolation and reinforcement of different virtual machines, access control and migration of virtual machines, monitoring of virtual machines processes, and vulnerability inspection in virtual machines, inner traffic monitoring and measures over the virtualized network.

2) Cloud platform architecture and components security audit: It is crucial to audit the rationality and effectiveness of the countermeasures including the policy of security domain division, the security redundancy of network architecture and core components, the vulnerability scanning and security reinforcement, the packaging and distribution of patches, and the configurations of the intrusion prevention system (IPS)/intrusion detection system (IDS), firewalls and virtualization security devices.

3) Operation, maintenance and business behaviour audit: Audit requirements mainly focus on operation and maintenance records, business access logs, access to data, and business behaviour inspection.

4) Identity and access management (IAM) and access control audit: The audit requirements are critical to ensure the correct operation in the cloud computing environment, which include the design and deployment of multifactor authentication, access control, single sign-on (SSO), segregation of duties, and management of privileged users.

5) Key management and data encryption audit: As encryption is the core mechanism to protect data in the cloud computing environment regardless of whether the service model is IaaS, PaaS or even SaaS, audit requirements should include the implementation and processing of key management and data encryption.

6) Emergency response and management audit: Audit requirements focus mainly on an emergency plan, a centralized management of security incidents, and a correlation analysis between the different security events.

Bibliography

[b-ITU-T E.409] Recommendation ITU-T E.409 (2004), *Incident organization and security incident handling: Guidelines for telecommunication organizations*.

[b-ITU-T X.810] Recommendation ITU-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

[b-ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing*.

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary*.

[b-ITU-T Y.3510] Recommendation ITU-T Y.3510 (2016), *Cloud computing infrastructure requirements*.

[b-ISO/IEC DIS 19086-1] ISO/IEC DIS 19086-1: 2016, *Information technology – Cloud computing – Service level agreement (SLA) framework and technology – Part 1: Overview and concepts*.

[b-ISO/IEC 20000-1] ISO/IEC 20000-1:2011, *Information technology – Service management – Part 1: Service management system requirements*.

[b-ISO/IEC 27000] ISO/IEC 27000:2012, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC DIS 27017] ISO/IEC DIS 27017:2015 , *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services*.

[b-ISO 27729] ISO 27729:2012, *Information and documentation – International standard name identifier (ISNI)*

[b-NIST-SP-800-30] NIST Special Publication 800-30 Rev. 1 (2012), *Guide for Conducting Risk Assessments*.


TECHNOLOGY
QUALITY
MANAGEMENT
STANDARD
NORM
WARRANTY
ISO 27002
VERIFIED
SYSTEM
SECURITY
CONTROL
BUSINESS
CERTIFICATE

Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services

Recommendation ITU-T X.1631

(07/2015)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Summary

Recommendation ITU-T X.1631 | ISO/IEC 27017 provides guidelines for information security controls applicable to the provision and use of cloud services by providing:

– additional implementation guidance for relevant controls specified in ISO/IEC 27002;

– additional controls with implementation guidance that specifically relate to cloud services.

This Recommendation | International Standard provides controls and implementation guidance for both cloud service providers and cloud service customers.

Table of Contents

Introduction

The guidelines contained within this Recommendation | International Standard are in addition to and complement the guidelines given in ISO/IEC 27002.

Specifically, this Recommendation | International Standard provides guidelines supporting the implementation of information security controls for cloud service customers and cloud service providers. Some guidelines are for cloud service customers who implement the controls, and others are for cloud service providers to support the implementation of those controls. The selection of appropriate information security controls and the application of the implementation guidance provided, will depend on a risk assessment and any legal, contractual, regulatory or other cloud-sector specific information security requirements.


CERTIFIED
ISO
27002

1 Scope

This Recommendation | International Standard gives guidelines for information security controls applicable to the provision and use of cloud services by providing:

– additional implementation guidance for relevant controls specified in ISO/IEC 27002;

– additional controls with implementation guidance that specifically relate to cloud services.

This Recommendation | International Standard provides controls and implementation guidance for both cloud service providers and cloud service customers.

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

2.1 Identical Recommendations | International Standards

– Recommendation ITU-T Y.3500 (in force) | ISO/IEC 17788: (in force), *Information technology – Cloud computing – Overview and vocabulary*.

– Recommendation ITU-T Y.3502 (in force) | ISO/IEC 17789: (in force), *Information technology – Cloud computing – Reference architecture*.

2.2 Additional References

– ISO/IEC 27000: (in force), *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

– ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls*.

3 Definitions and abbreviations

3.1 Terms defined elsewhere

For the purposes of this Recommendation | International Standard, the terms and definitions given in ISO/IEC 27000, Rec. ITU-T Y.3500 | ISO/IEC 17788, Rec. ITU-T Y.3502 | ISO/IEC 17789 and the following definitions apply:

3.1.1 The following term is defined in ISO 19440:

– **capability**: Quality of being able to perform a given activity.

3.1.2 The following terms are defined in ISO/IEC 27040:

– **data breach**: Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored, or otherwise processed.

– **secure multi-tenancy**: Type of multi-tenancy that employs security controls to explicitly guard against data breaches and provides validation of these controls for proper governance.

NOTE 1 – Secure multi-tenancy exists when the risk profile of an individual tenant is no greater than it would be in a dedicated, single-tenant environment.

NOTE 2 – In very secure environments, even the identity of the tenants is kept secret.

3.1.3 The following term is defined in ISO/IEC 17203:

– **virtual machine**: The complete environment that supports the execution of guest software.

NOTE – A virtual machine is a full encapsulation of the virtual hardware, virtual disks, and the metadata associated with it. Virtual machines allow multiplexing of the underlying physical machine through a software layer called a hypervisor.

3.2 Abbreviations

For the purposes of this Recommendation | International Standard, the following abbreviations apply:

IaaS Infrastructure as a Service

PaaS Platform as a Service

PII Personally Identifiable Information

SaaS Software as a Service

SLA Service Level Agreement

VM Virtual Machine

4 Cloud sector-specific concepts

4.1 Overview

The use of cloud computing has changed how organizations should assess and mitigate information security risks because of the significant changes in how computing resources are technically designed, operated and governed. This Recommendation | International Standard provides additional cloud-specific implementation guidance based on ISO/IEC 27002 and provides additional controls to address cloud-specific information security threats and risks considerations.

Users of this Recommendation | International Standard should refer to clauses 5 to 18 in ISO/IEC 27002 for controls, implementation guidance and other information. Because of the general applicability of ISO/IEC 27002, many of the controls, implementation guidance and other information apply to both the general and cloud computing contexts of an organization. For example, "6.1.2 Segregation of duties" of ISO/IEC 27002 provides a control that can be applied whether the organization is acting as a cloud service provider or not. Additionally, a cloud service customer can derive requirements for segregation of duties in the cloud environment from the same control, e.g., segregating the cloud service customers' cloud service administrators and cloud service users.

As an extension to ISO/IEC 27002, this Recommendation | International Standard further provides cloud service specific controls, implementation guidance and other information (see clause 4.5) that are intended to mitigate the risks that accompany the technical and operational features of cloud services (see Annex B). The cloud service customers and the cloud service providers can refer to ISO/IEC 27002 and this Recommendation | International Standard to select controls with the implementation guidance, and add other controls if necessary. This process can be done by performing an information security risk assessment and risk treatment in the organizational and business context where cloud services are used or provided (see clause 4.4).

4.2 Supplier relationships in cloud services

ISO/IEC 27002 clause 15 "Supplier relationships" provides controls, implementation guidance and other information for managing information security in supplier relationships. The provision and use of cloud services is a kind of supplier relationship, where the cloud service customer is an acquirer, and the cloud service provider is a supplier. Therefore, the clause applies to cloud service customers and cloud service providers.

Cloud service customers and cloud service providers can also form a supply chain. Suppose that a cloud service provider provides an infrastructure capabilities type service. In addition, another cloud service provider can provide an application capabilities type service. In this case, the second cloud service provider

is a cloud service customer with respect to the first, and a cloud service provider with respect to the cloud service customer using its service. This example illustrates the case where this Recommendation | International Standard applies to an organization both as a cloud service customer and as a cloud service provider. Because cloud service customers and cloud service providers form a supply chain through the design and implementation of the cloud service(s), clause "15.1.3 Information and communication technology supply chain" of ISO/IEC 27002 applies.

The multi-part International Standard ISO/IEC 27036, "*Information security for supplier relationships*", provides detailed guidance on the information security in supplier relationships to the acquirer and supplier of products and services. ISO/IEC 27036 Part 4 deals directly with the security of cloud services in supplier relationships. This standard is also applicable to cloud service customers as acquirers and cloud service providers as suppliers.

4.3 Relationships between cloud service customers and cloud service providers

In the cloud computing environment, cloud service customer data is stored, transmitted and processed by a cloud service. Therefore, a cloud service customer's business processes can depend upon the information security of the cloud service. Without sufficient control over the cloud service, the cloud service customer might need to take extra precautions with its information security practices.

Before entering into a supplier relationship, the cloud service customer needs to select a cloud service, taking into account the possible gaps between the cloud service customer's information security requirements and the information security capabilities offered by the service. Once a cloud service is selected, the cloud service customer should manage the use of the cloud service in such a way as to meet its information security requirements. In this relationship, the cloud service provider should provide the information and technical support that are necessary to meet the cloud service customer's information security requirements. When the information security controls provided by the cloud service provider are preset and cannot be changed by the cloud service customer, the cloud service customer may need to implement additional controls of its own to mitigate risks.

4.4 Managing information security risks in cloud services

Cloud service customers and cloud service providers should both have information security risk management processes in place. They are advised to refer to ISO/IEC 27001 for the requirements to conduct risk management in their information security management systems, and to refer to ISO/IEC 27005 for further guidance on information security risk management itself. ISO 31000, to which ISO/IEC 27001 and ISO/IEC 27005 conform, can also help general understanding of risk management.

In contrast to the general applicability of the information security risk management processes, cloud computing has its own types of risk sources, including threats and vulnerabilities, which are derived from its features, e.g., networking, scalability and elasticity of the system, resource sharing, self-service provisioning, administration on-demand, cross-jurisdictional service provisioning, and limited visibility into the implementation of controls. Annex B provides references that give information on these risk sources and associated risks in the provision and use of cloud services.

The controls and implementation guidance given in clauses 5 to 18 and Annex A of this Recommendation | International Standard address cloud computing specific risk sources and risks.

4.5 Structure of this standard

This Recommendation | International Standard is structured in a format similar to ISO/IEC 27002. This Recommendation | International Standard includes clauses 5 to 18 of ISO/IEC 27002 by stating the applicability of its texts at each clause and paragraph.

When objectives and controls specified in ISO/IEC 27002 are applicable without a need for any additional information, only a reference to ISO/IEC 27002 is provided.

When an objective with controls, or a control under an objective from ISO/IEC 27002, is needed in addition to those of ISO/IEC 27002, they are given in normative Annex A: Cloud service extended control set. When a control of ISO/IEC 27002 or Annex A of this Recommendation | International Standard needs additional cloud service specific implementation guidance related to the control, it is given under the subtitle "**Implementation guidance for cloud services**". The guidance is provided in one of the following two types:

Type 1 is used when there is separate guidance for the cloud service customer and the cloud service provider.

Type 2 is used when the guidance is the same for both the cloud service customer and the cloud service provider.

Type 1

Cloud service customer	Cloud service provider

Type 2

Cloud service customer	Cloud service provider

Additional information that might need to be considered is provided under the subtitle "**Other information for cloud services**".

5 Information security policies

5.1 Management direction for information security

The objective specified in clause 5.1 of ISO/IEC 27002 applies.

5.1.1 Policies for information security

Control 5.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
An information security policy for cloud computing should be defined as a topic-specific policy of the cloud service customer. The cloud service customer's information security policy for cloud computing should be consistent with the organization's acceptable levels of information security risks for its information and other assets. When defining the information security policy for cloud computing, the cloud service customer should take the following into account: – information stored in the cloud computing environment can be subject to access and management by the cloud service provider; – assets can be maintained in the cloud computing environment, e.g., application programs; – processes can run on a multi-tenant, virtualized cloud service;	The cloud service provider should augment its information security policy to address the provision and use of its cloud services, taking the following into account: – the baseline information security requirements applicable to the design and implementation of the cloud service; – risks from authorized insiders; – multi-tenancy and cloud service customer isolation (including virtualization); – access to cloud service customer assets by staff of the cloud service provider; – access control procedures, e.g., strong authentication for administrative access to cloud services; – communications to cloud service customers during change management;

Cloud service customer	Cloud service provider
– the cloud service users and the context in which they use the cloud service; – the cloud service administrators of the cloud service customer who have privileged access; – the geographical locations of the cloud service provider's organization and the countries where the cloud service provider can store the cloud service customer data (even temporarily).	– virtualization security; – access to and protection of cloud service customer data; – lifecycle management of cloud service customer accounts; – communication of breaches and information sharing guidelines to aid investigations and forensics.

Other information for cloud services

The cloud service customer's information security policy for cloud computing is one of the topic-specific policies described in ISO/IEC 27002 5.1.1. The information security policy of an organization deals with its information and business processes. When an organization uses cloud services, it can have a policy for cloud computing as a cloud service customer. An organization's information can be stored and maintained in the cloud computing environment, and the business processes can be operated in the cloud computing environment. General information security requirements stated in the information security policy at the top level are followed by the policy for cloud computing.

In contrast to this, the information security policy for providing cloud services deals with the cloud service customers' information and business processes, not with the cloud service provider's information and business processes. Information security requirements for the provision of the cloud service should meet those of the prospective cloud service customers. As a result, they might not be consistent with information security requirements of the information and business processes of the cloud service provider. The scope of the information security policy is often defined in terms of the service, but not solely by organizational structure or physical locations.

There are several virtualization security aspects for cloud computing, including lifecycle management of virtual instances, storage and access controls for virtualized images, handling of dormant or offline virtual instances, snapshots, protection of hypervisors and security controls governing use of self-service portals.

5.1.2 Review of the policies for information security

Control 5.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

6 Organization of information security

6.1 Internal organization

The objective specified in clause 6.1 of ISO/IEC 27002 applies.

6.1.1 Information security roles and responsibilities

Control 6.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should agree with the cloud service provider on an appropriate allocation of information security roles and responsibilities, and confirm that it can fulfil its allocated roles and responsibilities. The information security roles and responsibilities of both parties should be stated in an agreement. The cloud service customer should identify and manage its relationship with the customer support and care function of the cloud service provider.	The cloud service provider should agree and document an appropriate allocation of information security roles and responsibilities with its cloud service customers, its cloud service providers, and its suppliers.

Other information for cloud services

Even when responsibilities are determined within and between the parties, the cloud service customer is accountable for the decision to use the service. That decision should be made according to the roles and responsibilities determined within the cloud service customer's organization. The cloud service provider is accountable for the information security stated as part of the cloud service agreement. The information security implementation and provisioning should be made according to the roles and responsibilities determined within the cloud service provider's organization.

Ambiguity in roles and in the definition and allocation of responsibilities related to issues such as data ownership, access control, and infrastructure maintenance, can give rise to business or legal disputes, especially when dealing with third parties.

Data and files on the cloud service provider's systems that are created or modified during the use of the cloud service can be critical to the secure operation, recovery and continuity of the service. The ownership of all assets, and the parties who have responsibilities for operations associated with these assets, such as backup and recovery operations, should be defined and documented. Otherwise, there is a risk that the cloud service provider assumes that the cloud service customer performs these vital tasks (or vice versa), and a loss of data can occur.

6.1.2 Segregation of duties

Control 6.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

6.1.3 Contact with authorities

Control 6.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should identify the authorities relevant to the combined operation of the cloud service customer and the cloud service provider.	The cloud service provider should inform the cloud service customer of the geographical locations of the cloud service provider's organization and the countries where the cloud service provider can store the cloud service customer data.

Other information for cloud services

Information about geographical locations where the cloud service customer data can be stored, processed or transmitted can help the cloud service customer in determining the supervisory authorities and jurisdictions.

6.1.4 Contact with special interest groups

Control 6.1.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

6.1.5 Information security in project management

Control 6.1.5 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

6.2 Mobile devices and teleworking

The objective specified in clause 6.2 of ISO/IEC 27002 applies.

6.2.1 Mobile device policy

Control 6.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

6.2.2 Teleworking

Control 6.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

7 Human resource security

7.1 Prior to employment

The objective specified in clause 7.1 of ISO/IEC 27002 applies.

7.1.1 Screening

Control 7.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

7.1.2 Terms and conditions of employment

Control 7.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

7.2 During employment

The objective specified in clause 7.2 of ISO/IEC 27002 applies.

7.2.1 Management responsibilities

Control 7.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

7.2.2 Information security awareness, education and training

Control 7.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should add the following items to awareness, education and training programmes for cloud service business managers, cloud service administrators, cloud service integrators and cloud service users, including relevant employees and contractors: – standards and procedures for the use of cloud services; – information security risks relating to cloud services and how those risks are managed; – system and network environment risks with the use of cloud services; – applicable legal and regulatory considerations. Information security awareness, education and training programmes about cloud services should be provided to management and the supervising managers, including those of business units. These efforts support effective co-ordination of information security activities.	The cloud service provider should provide awareness, education and training for employees, and request contractors to do the same, concerning the appropriate handling of cloud service customer data and cloud service derived data. This data can contain information confidential to a cloud service customer or be subject to specific limitations, including regulatory restrictions, on access and use by the cloud service provider.

7.2.3 Disciplinary process

Control 7.2.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

7.3 Termination and change of employment

The objective specified in clause 7.3 of ISO/IEC 27002 applies.

7.3.1 Termination or change of employment responsibilities

Control 7.3.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

8 Asset management

8.1 Responsibility for assets

The objective specified in clause 8.1 of ISO/IEC 27002 applies.

8.1.1 Inventory of assets

Control 8.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer's inventory of assets should account for information and associated assets stored in the cloud computing environment. The records of the inventory should indicate where the assets are maintained, e.g., identification of the cloud service.	The inventory of assets of the cloud service provider should explicitly identify: – cloud service customer data; – cloud service derived data.

Other information for cloud services

There are cloud service applications that provide functions for managing information by adding cloud service derived data to the cloud service customer data. Identifying such cloud service derived data as assets and maintaining them in the inventory of assets can contribute to improving information security.

8.1.2 Ownership of assets

Control 8.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

Other information for cloud services

The ownership of assets will likely vary depending on the category of the cloud service being used. Application software will belong to the cloud service customer when using a platform as a service (PaaS) or infrastructure as a service (IaaS) service, whereas for a software as a service (SaaS) service, the application software will belong to the cloud service provider.

8.1.3 The acceptable use of assets

Control 8.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

8.1.4 Return of assets

Control 8.1.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

8.2 Information classification

The objective specified in clause 8.2 of ISO/IEC 27002 applies.

8.2.1 Classification of information

Control 8.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

8.2.2 Labelling of information

Control 8.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should label information and associated assets maintained in the cloud computing environment in accordance with the cloud service customer's adopted procedures for labelling. Where applicable, functionality provided by the cloud service provider that supports labelling can be adopted.	The cloud service provider should document and disclose any service functionality it provides allowing cloud service customers to classify and label their information and associated assets.

8.2.3 Handling of assets

Control 8.2.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

8.3 Media handling

The objective specified in clause 8.3 of ISO/IEC 27002 applies.

8.3.1 Management of removable media

Control 8.3.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

8.3.2 Disposal of media

Control 8.3.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

8.3.3 Physical media transfer

Control 8.3.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

9 Access control

9.1 Business requirements of access control

The objective specified in clause 9.1 of ISO/IEC 27002 applies.

9.1.1 Access control policy

Control 9.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

9.1.2 Access to networks and network services

Control 9.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer's access control policy for the use of network services should specify requirements for user access to each separate cloud service that is used.	(no additional implementation guidance)

9.2 User access management

The objective specified in clause 9.2 of ISO/IEC 27002 applies.

9.2.1 User registration and deregistration

Control 9.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
(no additional implementation guidance)	To manage access to cloud services by a cloud service customer's cloud service users, the cloud service provider should provide user registration and deregistration functions, and specifications for the use of these functions to the cloud service customer.

9.2.2 User access provisioning

Control 9.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
(no additional implementation guidance)	The cloud service provider should provide functions for managing the access rights of the cloud service customer's cloud service users, and specifications for the use of these functions.

Other information for cloud services

The cloud service provider should support third-party identity and access management technologies for its cloud services and the associated administration interfaces. These technologies can enable easier integration and easier user identity administration between the cloud service customer's systems and the cloud service, and can ease the use of multiple cloud services, supporting such capabilities as single sign-on.

9.2.3 Management of privileged access rights

Control 9.2.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should use sufficient authentication techniques (e.g., multi-factor authentication) for authenticating the cloud service administrators of the cloud service customer to the administrative capabilities of a cloud service according to the identified risks.	The cloud service provider should provide sufficient authentication techniques for authenticating the cloud service administrators of the cloud service customer to the administrative capabilities of a cloud service, according to the identified risks. For example, the cloud service provider can provide multi-factor authentication capabilities or enable the use of third-party multi-factor authentication mechanisms.

9.2.4 Management of secret authentication information of users

Control 9.2.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should verify that the cloud service provider's management procedure for allocating secret authentication information, such as passwords, meets the cloud service customer's requirements.	The cloud service provider should provide information on procedures for the management of the secret authentication information of the cloud service customer, including the procedures for allocating such information and for user authentication.

Other information for cloud services

The cloud service customer should control the management of secret authentication information by using its own or third party identity and access management technologies.

9.2.5 Review of user access rights

Control 9.2.5 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

9.2.6 Removal or adjustment of access rights

Control 9.2.6 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

9.3 User responsibilities

The objective specified in clause 9.3 of ISO/IEC 27002 applies.

9.3.1 Use of secret authentication information

Control 9.3.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

9.4 System and application access control

The objective specified in clause 9.4 of ISO/IEC 27002 applies.

9.4.1 Information access restriction

Control 9.4.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should ensure that access to information in the cloud service can be restricted in accordance with its access control policy and that such restrictions are realized. This includes restricting access to cloud services, cloud service functions, and cloud service customer data maintained in the service.	The cloud service provider should provide access controls that allow the cloud service customer to restrict access to its cloud services, its cloud service functions and the cloud service customer data maintained in the service.

Other information for cloud services

The cloud computing environment includes additional areas that require access controls. As part of the cloud service or cloud service functions, access to functions and services, such as the hypervisor management functions and administrative consoles, might need additional access control.

9.4.2 Secure log-on procedures

Control 9.4.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

9.4.3 Password management system

Control 9.4.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

9.4.4 Use of privileged utility programs

Control 9.4.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
Where the use of utility programs is permitted, the cloud service customer should identify the utility programs to be used in its cloud computing environment, and ensure that they do not interfere with the controls of the cloud service.	The cloud service provider should identify the requirements for any utility programs used within the cloud service. The cloud service provider should ensure that any use of utility programs capable of bypassing normal operating or security procedures is strictly limited to authorized personnel, and that the use of such programs is reviewed and audited regularly.

9.4.5 Access control to program source code

Control 9.4.5 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

10 Cryptography

10.1 Cryptographic controls

The objective specified in clause 10.1 of ISO/IEC 27002 applies.

10.1.1 Policy on the use of cryptographic controls

Control 10.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should implement cryptographic controls for its use of cloud services if justified by the risk analysis. The controls should be of sufficient strength to mitigate the identified risks, whether those controls are supplied by the cloud service customer or by the cloud service provider. When the cloud service provider offers cryptography, the cloud service customer should review any information supplied by the cloud service provider to confirm whether the cryptographic capabilities: – meet the cloud service customer's policy requirements; – are compatible with any other cryptographic protection used by the cloud service customer; – apply to data at rest and in transit to, from and within the cloud service.	The cloud service provider should provide information to the cloud service customer regarding the circumstances in which it uses cryptography to protect the information it processes. The cloud service provider should also provide information to the cloud service customer about any capabilities it provides that can assist the cloud service customer in applying its own cryptographic protection.

Other information for cloud services

In some jurisdictions, it might be required to apply cryptography to protect particular kinds of information, such as health data, resident registration numbers, passport numbers and driver's licence numbers.

10.1.2 Key management

Control 10.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should identify the cryptographic keys for each cloud service, and implement procedures for key management. Where the cloud service provides key management functionality for use by the cloud service customer, the cloud service customer should request the following information on the procedures used to manage keys related to the cloud service: – type of keys;	(no additional implementation guidance)

Cloud service customer	Cloud service provider
– specifications of the key management system, including procedures for each stage of the key life-cycle, i.e., generating, changing or updating, storing, retiring, retrieving, retaining and destroying; – recommended key management procedures for use by the cloud service customer. The cloud service customer should not permit the cloud service provider to store and manage the encryption keys for cryptographic operations when the cloud service customer employs its own key management or a separate and distinct key management service.	

11 Physical and environmental security

11.1 Secure areas

The objective specified in clause 11.1 of ISO/IEC 27002 applies.

11.1.1 Physical security perimeter

Control 11.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

11.1.2 Physical entry controls

Control 11.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

11.1.3 Securing offices, rooms and facilities

Control 11.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

11.1.4 Protecting against external and environmental threats

Control 11.1.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

11.1.5 Working in secure areas

Control 11.1.5 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

11.1.6 Delivery and loading areas

Control 11.1.6 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

11.2 Equipment

The objective specified in clause 11.2 of ISO/IEC 27002 applies.

11.2.1 Equipment siting and protection

Control 11.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

11.2.2 Supporting utilities

Control 11.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

11.2.3 Cabling security

Control 11.2.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

11.2.4 Equipment maintenance

Control 11.2.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

11.2.5 Removal of assets

Control 11.2.5 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

11.2.6 Security of equipment and assets off-premises

Control 11.2.6 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

11.2.7 Secure disposal or reuse of equipment

Control 11.2.7 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should request confirmation that the cloud service provider has the policies and procedures for secure disposal or reuse of resources.	The cloud service provider should ensure that arrangements are made for the secure disposal or reuse of resources (e.g., equipment, data storage, files, memory) in a timely manner.

Other information for cloud services

Additional information about secure disposal can be found in ISO/IEC 27040.

11.2.8 Unattended user equipment

Control 11.2.8 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

11.2.9 Clear desk and clear screen policy

Control 11.2.9 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

12 Operations security

12.1 Operational procedures and responsibilities

The objective specified in clause 12.1 of ISO/IEC 27002 applies.

12.1.1 Documented operating procedures

Control 12.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

12.1.2 Change management

Control 12.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer's change management process should take into account the impact of any changes made by the cloud service provider.	The cloud service provider should provide the cloud service customer with information regarding changes to the cloud service that could adversely affect the cloud service. The following will help the cloud service customer determine the effect the changes can have on information security: – categories of changes; – planned date and time of the changes; – technical description of the changes to the cloud service and underlying systems; – notification of the start and the completion of the changes. When a cloud service provider offers a cloud service that depends on a peer cloud service provider, then the cloud service provider might need to inform the cloud service customer of changes caused by the peer cloud service provider.

Other information for cloud services

The list of items that should be included in the notification can be identified in an agreement, e.g., a master service agreement or a service level agreement (SLA).

12.1.3 Capacity management

Control 12.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should ensure that the agreed capacity provided by the cloud service meets the cloud service customer's requirements. The cloud service customer should monitor the use of cloud services, and forecast their capacity needs, to ensure performance of the cloud services over time.	The cloud service provider should monitor the total resource capacity to prevent information security incidents caused by resource shortages.

Other information for cloud services

Cloud services involve resources that are under the control of the cloud service provider and made available to the cloud service customer under the terms of the master service agreement and a related SLA. These resources include software, processing hardware, data storage, and network connectivity.

Elastic, scalable and on-demand allocation of resources in a cloud service generally increases the total capacity of the service. However, the cloud service customer should be aware that the resources provided could have capacity constraints. Examples of capacity constraints include the number of processor cores for an application, the amount of storage available, or the network bandwidth available.

The constraints can vary depending on the particular cloud service or the particular subscription that the cloud service customer purchases. If the cloud service customer has requirements that exceed the constraints, the cloud service customer might need to change the cloud service or change the subscription.

In order for the cloud service customer to perform capacity management for cloud services, the cloud service customer should have access to relevant statistics on resource usage, such as:

– statistics for particular time periods;

– maximum levels of resource usage.

12.1.4 Separation of development, testing and operational environments

Control 12.1.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

12.2 Protection from malware

The objective specified in clause 12.2 of ISO/IEC 27002 applies.

12.2.1 Controls against malware

Control 12.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

12.3 Backup

The objective specified in clause 12.3 of ISO/IEC 27002 applies.

12.3.1 Information backup

Control 12.3.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
Where the cloud service provider provides backup capability as part of the cloud service, the cloud service customer should request the specifications of the backup capability from the cloud service provider. The cloud service customer should also verify that they meet their backup requirements. The cloud service customer is responsible for implementing backup capabilities when the cloud service provider does not provide them.	The cloud service provider should provide the specifications of its backup capabilities to the cloud service customer. The specifications should include the following information, as appropriate: – scope and schedule of backups; – backup methods and data formats, including encryption, if relevant; – retention periods for backup data; – procedures for verifying integrity of backup data; – procedures and timescales involved in restoring data from backup; – procedures to test the backup capabilities; – storage location of backups. The cloud service provider should provide secure and segregated access to backups, such as virtual snapshots, if such service is offered to cloud service customers.

Other information for cloud services

The allocation of responsibilities for making backups in the cloud computing environment is often unclear. In the case of IaaS, responsibility for making backups generally resides with the cloud service customer. However, a cloud service customer might not be aware of its responsibility to make backups of all cloud service customer data produced in the cloud computing system, such as executable files produced by the use of development capabilities of a PaaS service.

NOTE – Varying levels of backup and restore might be offered as a service at additional cost and, in this case, cloud service customers can choose what and when to backup.

12.4 Logging and monitoring

The objective specified in clause 12.4 of ISO/IEC 27002 applies.

12.4.1 Event logging

Control 12.4.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should define its requirements for event logging and verify that the cloud service meets those requirements.	The cloud service provider should provide logging capabilities to the cloud service customer.

Other **information** for cloud services

The responsibilities of the cloud service customer and the cloud service provider for event logging vary depending on the type of cloud service being used. For example, with IaaS, a cloud service provider's logging responsibility can be limited to that of cloud computing infrastructure components, and the cloud service customer can be responsible for logging the events of its own virtual machines and applications.

12.4.2 Protection of log information

Control 12.4.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

12.4.3 Administrator and operator logs

Control 12.4.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation **guidance** for cloud services

Cloud service customer	Cloud service provider
If a privileged operation is delegated to the cloud service customer, the operation and performance of those operations should be logged. The cloud service customer should determine whether logging capabilities provided by the cloud service provider are appropriate or whether the cloud service customer should implement additional logging capabilities.	(no additional implementation guidance)

Other information for cloud services

The allocation of responsibilities between the cloud service customer and the cloud service provider (see clause 6.1.1) should cover privileged operations related to the cloud service. Monitoring and logging the use of privileged operations are necessary to support preventive and corrective actions against incorrect use of these operations.

12.4.4 Clock synchronization

Control 12.4.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance **for** cloud services

Cloud service customer	Cloud service provider
The cloud service customer should request information about the clock synchronization used for the cloud service provider's systems.	The cloud service provider should provide information to the cloud service customer regarding the clock used by the cloud service provider's systems, and information about how the cloud service customer can synchronize local clocks with the cloud service clock.

Other information for cloud services

It is necessary to consider clock synchronization of the cloud service customer's systems with cloud service provider's systems, which run the cloud services used by the cloud service customer. Without such synchronization, it can be difficult to reconcile events on the cloud service customer's systems with events on the cloud service provider's systems.

12.5 Control of operational software

The objective specified in clause 12.5 of ISO/IEC 27002 applies.

12.5.1 Installation of software on operational systems

Control 12.5.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

12.6 Technical vulnerability management

The objective specified in clause 12.6 of ISO/IEC 27002 applies.

12.6.1 Management of technical vulnerabilities

Control 12.6.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should request information from the cloud service provider about the management of technical vulnerabilities that can affect the cloud services provided. The cloud service customer should identify the technical vulnerabilities it will be responsible to manage, and clearly define a process for managing them.	The cloud service provider should make available to the cloud service customer information about the management of technical vulnerabilities that can affect the cloud services provided.

12.6.2 Restrictions on software installation

Control 12.6.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

12.7 Information systems audit considerations

The objective specified in clause 12.7 of ISO/IEC 27002 applies.

12.7.1 Information systems audit controls

Control 12.7.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

13 Communications security

13.1 Network security management

The objective specified in clause 13.1 of ISO/IEC 27002 applies.

13.1.1 Network controls

Control 13.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

13.1.2 Security of network services

Control 13.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

13.1.3 Segregation in networks

Control 13.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should define its requirements for segregating networks to achieve tenant isolation in the shared environment of a cloud service and verify that the cloud service provider meets those requirements.	The cloud service provider should enforce segregation of network access for the following cases: – segregation between tenants in a multi-tenant environment; – segregation between the cloud service provider's internal administration environment and the cloud service customer's cloud computing environment. Where appropriate, the cloud service provider should help the cloud service customer verify the segregation implemented by the cloud service provider.

Other information for cloud services

Laws and regulations can require the segregation of networks or the isolation of network traffic.

13.2 Information transfer

The objective specified in clause 13.2 of ISO/IEC 27002 applies.

13.2.1 Information transfer policies and procedures

Control 13.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

13.2.2 Agreements on information transfer

Control 13.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

13.2.3 Electronic messaging

Control 13.2.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

13.2.4 Confidentiality or non-disclosure agreements

Control 13.2.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

14 System acquisition, development and maintenance

14.1 Security requirements of information systems

The objective specified in clause 14.1 of ISO/IEC 27002 applies.

14.1.1 Information security requirements analysis and specification

Control 14.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should determine its information security requirements for the cloud service and then evaluate whether services offered by a cloud service provider can meet these requirements. For this evaluation, the cloud service customer should request information on the information security capabilities from the cloud service provider.	The cloud service provider should provide information to the cloud service customers about the information security capabilities they use. This information should be informative without disclosing information that could be useful to someone with malicious intent.

Other information for cloud services

Care should be taken to limit disclosure of implementation details about security controls as they relate to the cloud service being provided to those cloud service customers or potential cloud service customers who have a non-disclosure agreement in place.

14.1.2 Securing applications services on public networks

Control 14.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

14.1.3 Protecting application services transactions

Control 14.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

14.2 Security in development and support processes

The objective specified in clause 14.2 of ISO/IEC 27002 applies.

14.2.1 Secure development policy

Control 14.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should request information from the cloud service provider about the cloud service provider's use of secure development procedures and practices	The cloud service provider should provide information about its use of secure development procedures and practices to the extent compatible with its policy for disclosure.

Other information for cloud services

Secure development procedures and practices of the cloud service provider can be critical to SaaS.

14.2.2 System change control procedures

Control 14.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

14.2.3 Technical review of applications after operating platform changes

Control 14.2.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

14.2.4 Restrictions on changes to software packages

Control 14.2.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

14.2.5 Secure system engineering principles

Control 14.2.5 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

14.2.6 Secure development environment

Control 14.2.6 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

14.2.7 Outsourced development

Control 14.2.7 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

14.2.8 System security testing

Control 14.2.8 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

14.2.9 System acceptance testing

Control 14.2.9 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

Other information for cloud services

In cloud computing, guidance for system acceptance testing applies to the use of a cloud service by the cloud service customer.

14.3 Test data

The objective specified in clause 14.3 of ISO/IEC 27002 applies.

14.3.1 Protection of test data

Control 14.3.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

15 Supplier relationships

15.1 Information security in supplier relationships

The objective specified in clause 15.1 of ISO/IEC 27002 applies.

15.1.1 Information security policy for supplier relationships

Control 15.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should include the cloud service provider as a type of supplier in its information security policy for supplier relationships. This will help to mitigate risks associated with the cloud service provider's access to and management of the cloud service customer data.	(no additional implementation guidance)

15.1.2 Addressing security within supplier agreements

Control 15.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should confirm the information security roles and responsibilities relating to the cloud service, as described in the service agreement. These can include the following processes: – malware protection; – backup; – cryptographic controls; – vulnerability management; – incident management; – technical compliance checking; – security testing; – auditing; – collection, maintenance and protection of evidence, including logs and audit trails; – protection of information upon termination of the service agreement; – authentication and access control; – identity and access management.	The cloud service provider should specify as part of an agreement the relevant information security measures that the cloud service provider will implement to ensure no misunderstanding between the cloud service provider and cloud service customer. The relevant information security measures that the cloud service provider will implement can vary based on the type of cloud service the cloud service customer is using.

15.1.3 Information and communication technology supply chain

Control 15.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
(no additional implementation guidance)	If a cloud service provider uses cloud services of peer cloud service providers, the cloud service provider should ensure information security levels to its own cloud service customers are maintained or exceeded. When the cloud service provider provides cloud services based on a supply chain, the cloud service provider should provide information security objectives to suppliers, and request each of the suppliers to perform risk management activities to achieve the objectives.

15.2 Supplier service delivery management

The objective specified in clause 15.2 of ISO/IEC 27002 applies.

15.2.1 Monitoring and review of supplier services

Control 15.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

15.2.2 Managing changes to supplier services

Control 15.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

16 Information security incident management

16.1 Management of information security incidents and improvements

The objective specified in clause 16.1 of ISO/IEC 27002 applies.

16.1.1 Responsibilities and procedures

Control 16.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should verify the allocation of responsibilities for information security incident management and should ensure that it meets the requirements of the cloud service customer.	As a part of the service specifications, the cloud service provider should define the allocation of information security incident management responsibilities and procedures between the cloud service customer and the cloud service provider. The cloud service provider should provide the cloud service customer with documentation covering: – the scope of information security incidents that the cloud service provider will report to the cloud service customer; – the level of disclosure of the detection of information security incidents and the associated responses; – the target timeframe in which notifications of information security incidents will occur; – the procedure for the notification of information security incidents; – contact information for the handling of issues relating to information security incidents; – any remedies that can apply if certain information security incidents occur.

16.1.2 Reporting information security events

Control 16.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should request information from the cloud service provider about the mechanisms for: – the cloud service customer to report an information security event it has detected to the cloud service provider; – the cloud service provider to receive reports regarding an information security event detected by the cloud service provider; – the cloud service customer to track the status of a reported information security event.	The cloud service provider should provide mechanisms for: – the cloud service customer to report an information security event to the cloud service provider; – the cloud service provider to report an information security event to a cloud service customer; – the cloud service customer to track the status of a reported information security event.

Other information for cloud services

The mechanisms should not only define the procedures but also give essential information like contact phone numbers, email addresses and service times for both the cloud service customer and the cloud service provider.

An information security event can be detected either by the cloud service customer or by the cloud service provider. Therefore, the main additional responsibility relating to cloud computing is that the party detecting the event should have procedures to report the event to the other party immediately.

16.1.3 Reporting information security weaknesses

Control 16.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

16.1.4 Assessment of and decision on information security events

Control 16.1.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

16.1.5 Response to information security incidents

Control 16.1.5 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

16.1.6 Learning from information security incidents

Control 16.1.6 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

16.1.7 Collection of evidence

Control 16.1.7 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer and the cloud service provider should agree upon the procedures to respond to requests for potential digital evidence or other information from within the cloud computing environment.	

17 Information security aspects of business continuity management

17.1 Information security continuity

The objective specified in clause 17.1 of ISO/IEC 27002 applies.

17.1.1 Planning information security continuity

Control 17.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

17.1.2 Implementing information security continuity

Control 17.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

17.1.3 Verify, review and evaluate information security continuity

Control 17.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

17.2 Redundancies

The objective specified in clause 17.2 of ISO/IEC 27002 applies.

17.2.1 Availability of information processing facilities

Control 17.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

18 Compliance

18.1 Compliance with legal and contractual requirements

The objective specified in clause 18.1 of ISO/IEC 27002 applies.

18.1.1 Identification of applicable legislation and contractual requirements

Control 18.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should consider the issue that relevant laws and regulations can be those of jurisdictions governing the cloud service provider, in addition to those governing the cloud service customer. The cloud service customer should request evidence of the cloud service provider's compliance with relevant regulations and standards required for the cloud service customer's business. Such evidence can be the certifications produced by third-party auditors.	The cloud service provider should inform the cloud service customer of the legal jurisdictions governing the cloud service. The cloud service provider should identify its own relevant legal requirements (e.g., regarding encryption to protect personally identifiable information (PII)) This information should also be provided to the cloud service customer when requested. The cloud service provider should provide the cloud service customer with evidence of its current compliance with applicable legislation and contractual requirements.

Other information for cloud services

The legal and regulatory requirements that apply to the provision and use of cloud services should be identified, particularly where the processing, storage and communication capabilities are geographically distributed and multiple jurisdictions can be involved.

It is important to note that compliance requirements, whether legal or contractual, remain the responsibility of the cloud service customer. Compliance responsibilities cannot be transferred to the cloud service provider.

18.1.2 Intellectual property rights

Control 18.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
Installing commercially licensed software in a cloud service can cause a breach of the licence terms for the software. The cloud service customer should have a procedure for identifying cloud-specific licensing requirements before permitting any licensed software to be installed in a cloud service. Particular attention should be paid to cases where the cloud service is elastic and scalable and the software can be run on more systems or processor cores than is permitted by the licence terms.	The cloud service provider should establish a process for responding to intellectual property rights complaints.

18.1.3 Protection of records

Control 18.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should request information from the cloud service provider about the protection of records gathered and stored by the cloud service provider that are relevant to the use of cloud services by the cloud service customer.	The cloud service provider should provide information to the cloud service customer about the protection of records that are gathered and stored by the cloud service provider relating to the use of cloud services by the cloud service customer.

18.1.4 Privacy and protection of personally identifiable information

Control 18.1.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

Other information for cloud services

ISO/IEC 27018, Code of practice for PII protection in public clouds acting as PII processors, offers additional information on this topic.

18.1.5 Regulation of cryptographic controls

Control 18.1.5 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should verify that the set of cryptographic controls that apply to the use of a cloud service comply with relevant agreements, legislation and regulations.	The cloud service provider should provide descriptions of the cryptographic controls implemented by the cloud service provider to the cloud service customer for reviewing compliance with applicable agreements, legislation and regulations.

18.2 Information security reviews

The objective specified in clause 18.2 of ISO/IEC 27002 applies.

18.2.1 Independent review of information security

Control 18.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should request documented evidence that the implementation of information security controls and guidelines for the cloud service is in line with any claims made by the cloud service provider. Such evidence could include certifications against relevant standards.	The cloud service provider should provide documented evidence to the cloud service customer to substantiate its claim of implementing information security controls. Where individual cloud service customer audits are impractical or can increase risks to information security, the cloud service provider should provide independent evidence that information security is implemented and operated in accordance with the cloud service provider's policies and procedures. This should be made available to prospective cloud service customers prior to entering a contract. A relevant independent audit as selected by the cloud service provider should normally be an acceptable method for fulfilling the cloud service customer's interest in reviewing the cloud service provider's operations, provided sufficient transparency is provided. When the independent audit is impractical, the cloud service provider should conduct a self-assessment, and disclose its process and results to the cloud service customer.

18.2.2 Compliance with security policies and standards

Control 18.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

18.2.3 Technical compliance review

Control 18.2.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

Annex A

Cloud service extended control set

(This annex forms an integral part of this Recommendation | International Standard.)

This annex provides additional control objectives, controls and implementation guidance as an extended control set for cloud services. ISO/IEC 27002 control objectives related to these controls are not repeated.

An organization intending to implement these controls in an information security management system (ISMS) that is to be conformant to ISO/IEC 27001, should extend its statement of applicability (SOA) by including the controls stated in this annex.

CLD.6.3 Relationship between cloud service customer and cloud service provider

Objective: To clarify the relationship regarding shared roles and responsibilities between the cloud service customer and the cloud service provider for information security management.

CLD.6.3.1 Shared roles and responsibilities within a cloud computing environment

Control

Responsibilities for shared information security roles in the use of the cloud service should be allocated to identified parties, documented, communicated and implemented by both the cloud service customer and the cloud service provider.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should define or extend its existing policies and procedures in accordance with its use of cloud services, and make cloud service users aware of their roles and responsibilities in the use of the cloud service.	The cloud service provider should document and communicate its information security capabilities, roles, and responsibilities for the use of its cloud service, along with the information security roles and responsibilities for which the cloud service customer would need to implement and manage as part of its use of the cloud service.

Other information for cloud services

In cloud computing, roles and responsibilities are typically divided between employees of the cloud service customer and employees of the cloud service provider. The allocation of roles and responsibilities should take into consideration the cloud service customer data and the cloud service customer applications for which the cloud service provider is a custodian.

CLD.8.1 Responsibility for assets

The objective specified in clause 8.1 of ISO/IEC 27002 applies.

CLD.8.1.5 Removal of cloud service customer assets

Control

Assets of the cloud service customer that are on the cloud service provider's premises should be removed, and returned if necessary, in a timely manner upon termination of the cloud service agreement.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should request a documented description of the termination of service process that covers return and removal of cloud service customer's assets followed by the deletion of all copies of those assets from the cloud service provider's systems. The description should list all the assets and document the schedule for the termination of service, which should occur in a timely manner.	The cloud service provider should provide information about the arrangements for the return and removal of any cloud service customer's assets upon termination of the agreement for the use of a cloud service. The asset return and removal arrangements should be documented in the agreement and should be performed in a timely manner. The arrangements should specify the assets to be returned and removed.

CLD.9.5 Access control of cloud service customer data in shared virtual environment

Objective: To mitigate information security risks when using the shared virtual environment of cloud computing.

CLD.9.5.1 Segregation in virtual computing environments

Control

A cloud service customer's virtual environment running on a cloud service should be protected from other cloud service customers and unauthorized persons.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
(no additional implementation guidance)	The cloud service provider should enforce appropriate logical segregation of cloud service customer data, virtualized applications, operating systems, storage, and network for: – the separation of resources used by cloud service customers in multi-tenant environments; – the separation of the cloud service provider's internal administration from resources used by cloud service customers. Where the cloud service involves multi-tenancy, the cloud service provider should implement information security controls to ensure appropriate isolation of resources used by different tenants. The cloud service provider should consider the risks associated with running cloud service customer-supplied software within the cloud services offered by the cloud service provider.

Other information for cloud services

Implementation of the logical segregation depends upon the technologies applied to the virtualization:

– Network and storage configurations can be virtualized when a software virtualization function provides a virtual environment (e.g., a virtual operating system). In addition, segregation of cloud service customers in software virtualized environments can be designed and implemented using segregation functions of the software.

– When a cloud service customer's information is stored in a physically shared storage area with the "meta-data table" of the cloud service, segregation of information from other cloud service customers can be implemented with access control on the "meta-data table".

Secure multi-tenancy and related guidance given in "ISO/IEC 27040, *Information technology – Security techniques – Storage security*" can apply to the cloud computing environment.

CLD.9.5.2 Virtual machine hardening

Control

Virtual machines in a cloud computing environment should be hardened to meet business needs.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
When configuring virtual machines, cloud service customers and cloud service providers should ensure that appropriate aspects are hardened (e.g., only those ports, protocols and services that are needed), and that the appropriate technical measures are in place (e.g., anti-malware, logging) for each virtual machine used.	

CLD.12.1 Operational procedures and responsibilities

The objective specified in clause 12.1 of ISO/IEC 27002 applies.

CLD.12.1.5 Administrator's operational security

Control

Procedures for administrative operations of a cloud computing environment should be defined, documented and monitored.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should document procedures for critical operations where a failure can cause unrecoverable damage to assets in the cloud computing environment. Examples of the critical operations are: – installation, changes, and deletion of virtualized devices such as servers, networks and storage; – termination procedures for cloud service usage; – backup and restoration. The document should specify that a supervisor should monitor these operations.	The cloud service provider should provide documentation about the critical operations and procedures to cloud service customers who require it.

Other information for cloud services

Cloud computing has the benefit of rapid provisioning and administration, and on-demand self-service. These operations are often carried out by administrators from the cloud service customer and the cloud service provider. Because human intervention in these critical operations can cause serious information security incidents, mechanisms to safeguard the operations should be considered and, if needed, be defined and implemented. Examples of serious incidents include erasing or shutting down a large number of virtual servers or destroying virtual assets.

CLD.12.4 Logging and monitoring

The objective specified in clause 12.4 of ISO/IEC 27002 applies.

CLD.12.4.5 Monitoring of Cloud Services

Control

The cloud service customer should have the capability to monitor specified aspects of the operation of the cloud services that the cloud service customer uses.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
The cloud service customer should request information from the cloud service provider of the service monitoring capabilities available for each cloud service.	The cloud service provider should provide capabilities that enable the cloud service customer to monitor specified aspects, relevant to the cloud service customer, of the operation of the cloud services. For example, to monitor and detect if the cloud service is being used as a platform to attack others, or if sensitive data is being leaked from the cloud service. Appropriate access controls should secure the use of the monitoring capabilities. The capabilities should provide access only to information about the cloud service customer's own cloud service instances. The cloud service provider should provide documentation of the service monitoring capabilities to the cloud service customer. Monitoring should provide data consistent with the event logs described in clause 12.4.1 and assist with SLA terms.

CLD.13.1 Network security management

The objective specified in clause 13.1 of ISO/IEC 27002 applies.

CLD.13.1.4 Alignment of security management for virtual and physical networks

Control

Upon configuration of virtual networks, consistency of configurations between virtual and physical networks should be verified based on the cloud service provider's network security policy.

Implementation guidance for cloud services

Cloud service customer	Cloud service provider
(no additional implementation guidance)	The cloud service provider should define and document an information security policy for the configuration of the virtual network consistent with the information security policy for the physical network. The cloud service provider should ensure that the virtual network configuration matches the information security policy regardless of the means used to create the configuration.

Other information for cloud services

In a cloud computing environment built on virtualization technology, a virtual network is configured on virtual infrastructure on a physical network. In such environments, inconsistency of network policies can cause system outages or defective access control.

NOTE – Depending on the type of cloud service, the responsibilities for configuring a virtual network can vary between a cloud service customer and a cloud service provider.

Annex B

References on information security risk related to cloud computing

(This annex does not form an integral part of this Recommendation | International Standard.)

Proper use of the information security controls provided by this Recommendation | International Standard relies on the organization's information security risk assessment and treatment. Although these are important subjects, the focus of this Recommendation | International Standard is not on the approach to information security risk assessment and treatment. Following is a list of references that include descriptions of the risk sources and risks in the provision and use of cloud services. It should be noted that risk sources and risks vary according to the type and nature of the service and the emerging technologies of cloud computing. Users of this Recommendation | International Standard are recommended to refer to the current versions of the documents as necessary.

Recommendation ITU-T X.1601 (2014), *Security framework for cloud computing*.

Australian Government Information Management Office 2013, *Summary of Checkpoints* in: *Privacy and Cloud Computing for Australian Government Agencies, Better Practice Guide,* Version 1.1, February, *pg. 8*.http://www.finance.gov.au/files/2013/02/privacy-and-cloud-computing-for-australian-government-agencies-v1.1.pdf

Australian Government Cyber Security Centre 2015, *Cloud Computing Security for Tenants* – April. http://www.asd.gov.au/publications/protect/Cloud_Computing_Security_for_Tenants.pdf

Australian Government Cyber Security Centre 2015, *Cloud Computing Security for Cloud Service Providers* – April. http://www.asd.gov.au/publications/protect/Cloud_Computing_Security_for_Cloud_Service_Providers.pdf

Cloud Security Alliance 2014, *Cloud Controls Matrix* – January.

ENISA 2009, *Cloud Computing Security Risk Assessment* – November.

ENISA 2009, *Cloud Computing Information Assurance Framework* – November.

Hong Kong OGCIO 2013, *Security & Privacy Checklist for Cloud Service Providers in Handling Personal Identifiable Information in Cloud Platforms* – April.

Hong Kong OGCIO 2013, *Security Checklists for Cloud Service Consumers* – January.

ISACA 2012, *Security Considerations for Cloud Computing* – July.

NIST, SP 800-144 2011, *Guidelines on Security and Privacy in Public Cloud Computing* – December.

NIST, SP 800-146 2012, *Cloud Computing Synopsis and Recommendations* – May.

SPRING Singapore 2012, *Annex A: Virtualisation Security Risk Assessment* of Singapore Technical Reference 30:2012 Technical Reference for virtualisation security for servers – March.

SPRING Singapore 2012, *Annex A: Checklist of security and service level considerations when reviewing SaaS* of Singapore Technical Reference 31:2012 Technical Reference for security and service level guidelines for the usage of public cloud computing services – March.

SPRING Singapore 2013, *Annex A: Cloud Service Provider Disclosure* of Singapore Standard SS 584:2013 Specification for Multi-Tiered Cloud Computing Security – August.

SPRING Singapore 2012, *Annex B: Checklist of security and service level considerations when reviewing IaaS* of Singapore Technical Reference 31:2012 Technical Reference for security and service level guidelines for the usage of public cloud computing services – March.

SPRING Singapore 2013, Singapore Standard SS 584:2013 *Specification for Multi-Tiered Cloud Computing Security* – August.

SPRING Singapore 2012, Singapore Technical Reference 30:2012 *Technical Reference for virtualisation security for servers* – March.

SPRING Singapore 2012, Singapore Technical Reference 31:2012 *Technical Reference for security and service level guidelines for the usage of public cloud computing services* – March.

US Government FedRAMP PMO 2014, *FedRAMP Security Controls Baseline Version 2.0* – June.

Bibliography

– Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.
– ISO/IEC 17203:2011, *Information technology – Open Virtualization Format (OVF) specification*.
– ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*.
– ISO/IEC 27005:2011, *Information technology – Security techniques – Information security risk management*.
– ISO/IEC 27018:2014, *Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*.
– ISO/IEC 27036-1:2014, *Information technology – Security techniques – Information security for supplier relationships – Part 1: Overview and concepts*.
– ISO/IEC 27036-2:2014, *Information technology – Security techniques – Information security for supplier relationships – Part 2: Requirements*.
– ISO/IEC 27036-3:2013, *Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security*.
– ISO/IEC CD 27036-4, *Information technology – Security techniques – Information security for supplier relationships – Part 4: Guidelines for security of cloud services* – (Under development).
– ISO/IEC 27040:2015, *Information technology – Security techniques – Storage security*.
– ISO 19440:2007, *Enterprise integration – Constructs for enterprise modelling*.
– ISO 31000:2009, *Risk management – Principles and guidelines*.
– NIST, SP 800-145 2011, *The NIST Definition of Cloud Computing*.
– NIST 2009, *Effectively and Securely Using the Cloud Computing Paradigm*.
– ENISA 2009, *Cloud Computing Benefits, risks and recommendations for information security*.
– Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing V3.0*.
– Cloud Security Alliance, *Top Threats to Cloud Computing V1.0*.
– Cloud Security Alliance, *Domain 12: Guidance for Identity & Access Management V2.1.*
– ISACA, *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives*.
– ISACA, *Cloud Computing Management Audit/Assurance Program*.

ITU Technology Watch Report

ITU Technology Watch report (March 2012): Privacy in cloud computing https://www.itu.int/oth/T2301000016/en


WE CA
HELP YO
DATABASE
INTERNET LAPTOP MOBILE MOBILITY NETWORK
DATA
DESIGN
DATABASE
PROJECT
MANAGER
SYSTEM
CUSTOMER
MANAG
COMPUTER
INFORMATION
WORKSTATION
STATION
EMAIL
INTERNET LAPTOP MOBILE
BUSINESS
DESIGN
COMPUTER
INTERNET LAPTOP MOBILE MOBILITY NETWORK
PROFESSIONAL CLIENT
INFORMATION
DATABASE
COMPUTER
CLIENT
STRATEGY
ANALYSIS
KNOWLEDGE
PLANNING
INTERNET LAPTOP MOBILE MOBILITY NETWORK
INFORMATION
PROJECT
MANAGEMEN
ANA
PRO
RESEARC
TE
MANAGE
ACCESS
MANAGER
CLIENT
INTERNET LAPTOP MOBILE MOBILITY
SYSTEM
ACCESS
DATA
MENT
INFORMATION
SECURITY
PRODUCTS
KTOP
STRATEGY
FORMATION
ANAGER
ANALYSIS
PROCESS
QUALITY
TECHNOLOGY
MANAGEMENT
PROFESSIONAL
INTERNET LAPTOP MOBILE MOBILITY NETWORK
DATA
DESKTOP
MANAGEMENT
KNOWLEDGE
DATA
MANAGER
STRATEGY
ACCESS
CLIENT
INTERNET LAPTOP MOBILE MOBILITY NETWORK
PLANNING
KNOWLEDGE
INFORMATION

8.

Assisting developing countries

Requirements and challenges regarding provision and consumption of cloud computing services in developing countries

Supplement 46 to ITU-T Y.3500-series Recommendations

(11/2017)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Summary

Supplement 46 to the ITU-T Y-series Recommendations applies to the ITU-T Y.3500 series Recommendations. Cloud computing has the potential to alleviate some of the socio-economic challenges being faced in developing countries such as lack of resilient electrical power, lack of information and communication technology (ICT) infrastructure and can also improve service delivery to mention but a few.

Emanating from a survey conducted on the status of cloud computing in developing countries, this Supplement highlights the requirements and challenges of cloud computing provision and consumption in developing countries with regards but not limited to standards implementation, data connectivity and infrastructure deployment.

Keywords

Broadband, challenges, cloud computing, cloud service customer, cloud service provider, information and communications technology, Internet, quality of service, service level agreement, standards.

Table of Contents

Introduction

The global trends in sectors such as health, agriculture, commerce, education, banking and finance have demonstrated that a significant amount of data will be delivered and accessed online. Most enterprises are looking for ways to improve operational efficiency and cut costs through least-cost operator strategies and outsourcing. Cloud computing is among the prominent technologies that are making this process viable. Governments are also beginning to leverage some of the characteristics of cloud computing such as on demand access and cost effectiveness to deliver improved citizen services and increase Government operational efficiencies.

In developing countries, cloud computing has the potential to:

i) improve energy efficiency in every sector of the economy by consolidating IT services especially in government and banking sector;

ii) improve service delivery and operational efficiency in various sectors such as health, tourism and transport;

iii) create new business models;

iv) build new skills in application and content development;

v) promote environmental sustainability;

vi) make significant savings in set up cost of IT solutions;

vii) contribute significantly to the gross domestic product (GDP) and

viii) create new job opportunities.

Despite the prospects outlined above, cloud computing adoption in developing countries is still low and several developing countries encounter many challenges to effectively contribute to the cloud economy. Various efforts are being made by numerous stakeholders to support accelerated implementation of cloud computing in developing countries and to build trust in the use of this emerging technology. However, there are many barriers affecting cloud computing adoption in these countries which need to be addressed before it can become a reality. These barriers vary significantly depending on the country's level of development and business and communications environments.

As a step towards creating an impetus to the deployment and usage of cloud computing services in developing countries, an ITU-T survey was commissioned to assess the current profile of cloud computing deployment and consumption in developing countries. The survey allowed for the identification of bottlenecks and weaknesses that need to be addressed to effectively exploit the cloud computing platform in developing countries. The findings of this survey are presented and analysed in this supplement.

1 Scope

The scope of this Supplement to ITU-T Y.3500-series is to study and present the situation relating to the application of cloud computing services in developing countries, the obstacles encountered and the facets that would stimulate assimilation of cloud computing services based on experiences from these countries.

The Supplement also highlights the current requirements for provision and deployment of cloud computing services and to what extent cloud computing standards are applied in developing countries.

2 References

[ITU-T X.1258] Recommendation ITU-T X.1258 (2016), *Enhanced entity authentication based on aggregated attributes*.

[ITU-T L.1300] Recommendation ITU-T L.1300 (2014), *Best practices for green data centres*.

[ITU-T L.1301] Recommendation ITU-T L.1301 (2015), *Minimum data set and communication interface requirements for data centre energy management*.

[ITU-T L.1302] Recommendation ITU-T L.1302 (2015), *Assessment of energy efficiency on infrastructure in data centres and telecom centres*.

[ITU-T L.1320] Recommendation ITU-T L.1320 (2014), *Energy efficiency metrics and measurement for power and cooling equipment for telecommunications and data centres*.

[ITU-T X.1601] Recommendation ITU-T X.1601 (2015), *Security framework for cloud computing*.

[ITU-T X.1602] Recommendation ITU-T X.1602 (2016), *Security requirements for software as a service application environments*.

[ITU-T X.1631] Recommendation ITU-T X.1631 (2015), *Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services.*

[ITU-T X.1641] Recommendation ITU-T X.1641 (2016), *Guidelines for cloud service customer data security*.

[ITU-T X.1642] Recommendation ITU-T X.1642 (2016), *Guidelines of operational security for cloud computing*.

[ITU-T Y.3051] Recommendation ITU-T Y.3051 (2017), *The basic principles of trusted environment in information and communication technology infrastructure*.

[ITU-T Y.3052] Recommendation ITU-T Y.3052 (2017), *Overview of trust provisioning for information and communication technology infrastructures and services*.

[ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014), *Information technology – Cloud computing – Overview and vocabulary*.

[ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), *Information technology – Cloud computing – Reference architecture*.

[ITU-T Y.3503] Recommendation ITU-T Y.3503 (2014), *Requirements for desktop as a service*.

[ITU-T Y.3510] Recommendation ITU-T Y.3510 (2016), *Cloud computing infrastructure requirements*.

[ITU-T Y.3511] Recommendation ITU-T Y.3511 (2014), *Framework of inter-cloud computing*.

[ITU-T Y.3514] Recommendation ITU-T Y.3514 (2014), *Cloud computing – Trusted inter-cloud computing framework and requirements.*

[ITU-T Y.3520] Recommendation ITU-T Y.3520 (2015), *Cloud computing framework for end to end resource management*.

[ISO/IEC 27002] ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls*.

[TIA-942] TIA-942:2017, *Telecommunications Infrastructure Standard for Data Centers*.

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following terms defined elsewhere:

3.1.1 cloud computing [ITU-T Y.3500]: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.

3.1.2 cloud service [ITU-T Y.3500]: One or more capabilities offered via cloud computing invoked using a defined interface.

3.1.3 cloud service category [ITU-T Y.3500]: Group of cloud services that possess some common set of qualities.

3.1.4 cloud service customer [ITU-T Y.3500]: Party which is in a business relationship for the purpose of using cloud services.

NOTE – A business relationship does not necessarily imply financial agreements.

3.1.5 cloud service partner [ITU-T Y.3500]: Party which is engaged in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer, or both.

3.1.6 cloud service provider [ITU-T Y.3500]: Party which makes cloud services available.

3.1.7 cloud service user [ITU-T Y.3500]: Natural person, or entity acting on their behalf, associated with a cloud service customer that uses cloud services.

NOTE – Examples of such entities include devices and applications.

3.1.8 communications as a Service (CaaS) [ITU-T Y.3500]: Cloud service category in which the capability provided to the cloud service customer is real time interaction and collaboration.

NOTE – CaaS can provide both application capabilities type and platform capabilities type.

3.1.9 community cloud [ITU-T Y.3500]: Cloud deployment model where cloud services exclusively support and are shared by a specific collection of cloud service customers who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection.

3.1.10 compute as a service (CompaaS) [ITU-T Y.3500]: Cloud service category in which the capabilities provided to the cloud service customer are the provision and use of processing resources needed to deploy and run software.

NOTE – To run some software, capabilities other than processing resources may be needed.

3.1.11 data storage as a service (DSaaS) [ITU-T Y.3500]: Cloud service category in which the capability provided to the cloud service customer is the provision and use of data storage and related capabilities.

NOTE – DSaaS can provide any of the cloud capabilities types.

3.1.12 desktop as a service (DaaS) [ITU-T Y.3503]: A cloud service category in which the capabilities provided to the cloud service customer are the ability to build, configure, manage, store, execute and deliver users' desktop functions remotely.

3.1.13 hybrid cloud [ITU-T Y.3500]: Cloud deployment model using at least two different cloud deployment models.

3.1.14 infrastructure as a service (IaaS) [ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer is an infrastructure capabilities type.

NOTE – The cloud service customer does not manage or control the underlying physical and virtual resources, but does have control over operating systems, storage, and deployed applications that use the physical and virtual resources. The cloud service customer may also have limited ability to control certain networking components (e.g., host firewalls).

3.1.15 infrastructure capabilities type [ITU-T Y.3500]: Cloud capabilities type in which the cloud service customer can provision and use processing, storage or networking resources.

3.1.16 network as a service (NaaS) [ITU-T Y.3500]: Cloud service category in which the capability provided to the cloud service customer is transport connectivity and related network capabilities.

3.1.17 party [ITU-T Y.3500]: Natural person or legal person, whether or not incorporated, or a group of either.

3.1.18 platform as a service (PaaS) [ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer is a platform capabilities type.

3.1.19 private cloud [ITU-T Y.3500]: Cloud deployment model where cloud services are used exclusively by a single cloud service customer and resources are controlled by that cloud service customer.

3.1.20 public cloud [ITU-T Y.3500]: Cloud deployment model where cloud services are potentially available to any cloud service customer and resources are controlled by the cloud service provider.

3.1.21 resource management [ITU-T Y.3520]: The most efficient and effective way to access, control, manage, deploy, schedule and bind resources when they are provided by service providers and requested by customers.

3.1.22 role [ITU-T Y.3502]: A set of activities that serves a common purpose.

3.1.23 service level agreement (SLA) [ITU-T Y.3500]: Documented agreement between the service provider and customer that identifies services and service targets.

NOTE 1 – A service level agreement can also be established between the service provider and a supplier, an internal group or a customer acting as a supplier.

NOTE 2 – A service level agreement can be included in a contract or another type of documented agreement.

3.1.24 software as a service (SaaS) [ITU-T Y.3500]: Cloud service category in which the cloud capabilities type provided to the cloud service customer is an application capabilities type.

3.2 Terms defined in this Supplement

None.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

AC	Alternating Current
BaaS	Back-up as a Service
CaaS	Communications as a Service
CAPEX	Capital Expenditure
CompaaS	Compute as a Service
CSC	Cloud Service Customer
CSP	Cloud Service Provider
DaaS	Desktop as a Service
DC	Direct Current
DraaS	Disaster Recovery as a Service
DSaaS	Data Storage as a Service
IaaS	Infrastructure as a Service
ICT	Information and Communication Technology
IT	Information Technology
IXP	Internet Exchange Point

LAN	Local Area Network
M&E	Mechanical and Electrical
NaaS	Network as a Service
OPEX	Operational Expenditure
PaaS	Platform as a Service
PCI DSS	Payment Card Industry Data Security Standard
PUE	Power Usage Effectiveness
QoS	Quality of Service
SAN	Storage Area Network
SaaS	Software as a Service
SMB	Small and Medium Businesses
SDO	Standard Development Organization
SLA	Service Level Agreement
UI	Uptime Institute
UPS	Uninterruptible Power Supply
VAS	Value Added Services

5 Conventions

None.

6 Overview

According to [ITU-T Y.3500], cloud computing has been defined as *"A paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand."*

6.1 Key characteristics

Cloud computing is a dynamic concept that keeps evolving. According to [ITU-T Y.3500], the key characteristics of cloud computing include:

i) on demand access which allows cloud service customers (CSCs) to make use of the resources as and when required;

ii) cost effectiveness as it readily reduces the capital expenditure (CAPEX) of organizations allowing them to divert resources to operational expenditure (OPEX);

iii) high scalability as it offers little time to implementation enabling the CSCs to promptly customize and adjust the cloud computing capabilities according to their needs;

iv) energy saving as the same resources are being utilized by multiple tenants; and

v) increased level of convenience as only broadband internet access is required which can be accessed over a varied range of terminals such as tablets, laptops, workstations and mobile phones.

6.2 Deployment models

According to [ITU-T Y.3500], the cloud economy consists of various cloud service deployment models and service categorises. The cloud computing deployment models are described in the Table 6-1.

Table 6-1 – Cloud computing deployment models

Model	Description
Private cloud	Proprietary resources provided for a single organization (for example, a government or large enterprise), managed and hosted internally or by a third-party.
Public cloud	Open resources that offer services over a network that is open for public use. Many mass market services widely used by individuals, such as webmail, online storage and social media are public cloud services.
Hybrid cloud	A mix of the deployment models for example, public and private cloud provision.
Community cloud	Resources/services provided for and shared by defined CSCs who have similar requirements and a relationship with one another. This is managed and hosted internally or by a third-party or a combination of both.

6.3 Service categories

The representative services offered on the cloud platform are described below [ITU-T Y.3500]. As the sector evolves, other services will soon be offered on this platform.

Table 6-2 – Cloud platform service categories

Service category	Description
Communicate as a service	Audio/video communication services, collaborative services, unified communications, e-mail, instant messaging, data.
Compute as a service (CompaaS)	Cloud service category in which the capabilities provided to the cloud service customer are the provision and use of processing resources needed to deploy and run software.
Data storage as a service (DSaaS)	Cloud service category in which the capability provided to the cloud service customer is the provision and use of data storage and related capabilities.
Infrastructure as a service (NaaS)	Virtualized on-demand server, virtualized data centre, flexible on-demand storage space, flexible local area networks (LANs), firewalls, security services, etc.
Network as a service (NaaS)	Platform for cloud computing service provision, virtualized network (customer service management, billing, on-demand bandwidth etc.)
Platform as a service (PaaS)	Applications built on top of cloud service provider's infrastructure. Developers can derive benefit from PaaS.
Software as service (SaaS)	Business applications, customer relations and support (CRM), HR, finance (ERP), online payments, electronic marketplace.

6.4 Benefits of cloud computing

According to the report by [b-ITU-D Q3/1], "Access to Cloud Computing: Challenges and opportunities for developing countries", Cloud computing adoption offers tangible benefits in terms of cost reduction, flexibility, agility, scale, and innovation.

Cloud technologies enable businesses and governments to consolidate their investments, their servers and data centres to reduce their costs. For small and medium businesses (SMBs), cloud computing is an opportunity to get access, at a fraction of cost, to the latest technologies which were previously only accessible to large enterprises, and without having to worry about technical infrastructure that is not core to their business. This enables them to better compete with any other business on the globe. Cloud computing

allows businesses and governments to become more flexible and agile by allowing them to build new products and services much faster. This also gives an opportunity to small start-ups to participate in the industry with their innovations.

7 Questionnaire findings

An ITU-T survey was commissioned to assess the current profile of cloud computing deployment in developing countries. To this effect two questionnaires on cloud computing status in developing countries were formulated. The first questionnaire was designed for cloud service customers (CSC) and the second one for cloud service providers (CSP). The questionnaires were made available in word document format and online to facilitate a wide range of feedback methods for the respondents. In May 2016 they were disseminated to ITU members from developing countries with a request to share the questionnaires with the CSCs and CSPs in their countries, including entities which were not ITU-T members.

Eight (8) responses were received for the CSC questionnaire and eighteen (18) for the CSP questionnaire from seventeen (17) countries. The majority of responses were from Africa as highlighted in the appendices and Table 7-1.

Table 7-1 – List of countries and responses obtained

No.	Country	Number of CSP respondents	Number of CSC respondents	Total
1	Afghanistan	1	0	1
2	Algeria	1	0	1
3	Bosnia and Herzegovina	1	0	1
4	Botswana	1	0	1
5	Burkina Faso	1	0	1
6	Cote d'Ivoire	1	0	1
7	Gambia	1	0	1
8	Ghana	1	1	2
9	Malawi	1	1	2
10	Nigeria	1	0	1
11	Senegal	1	0	1
12	Sudan	1	1	2
13	Trinidad and Tobago	0	1	1
14	Tunisia	1	0	1
15	Uganda	0	1	1
16	Zambia	2	1	3
17	Zimbabwe	3	2	5
	Total	**18**	**8**	**26**

The questionnaires covered the following main axes:

a) availability of reliable internet services over which the cloud services may be accessed;

b) deployment and usage of cloud based services;

c) degree of implementation of standards and service level agreements;

d) degree of infrastructure deployment;

e) levels of data privacy and cloud security;

f) cloud computing training requirements;

g) factors that affect the deployment and usage of cloud computing services; and

h) factors that may motivate the uptake of cloud computing services in developing countries.

7.1 Questionnaire respondents

Of the respondents under CSCs:

- seventy five per cent (75%) were government institutions;
- thirteen per cent (13%) were corporate intuitions; and
- thirteen per cent (13%) were multinational companies.

On the other hand respondents under CSPs:

- thirty three per cent (33%) of CSP respondents also provided mobile services and fixed services; and
- twenty eight per cent (28%) also provided Internet services.

7.2 Deployment of cloud computing in developing countries

The main motivation for most CSCs to migrate to the cloud is the increase in operational efficiency. Furthermore, cloud computing services free them from the need to acquire expensive hardware and to deploy information technology (IT) infrastructure ultimately ensuring cost optimization.

The deployment requirements for customers to access cloud services from the CSPs are relatively simple as customers are only required to pay for licence fees, where applicable, as well as to have a reliable internet connection. It is also imperative that customers have a resilient power supply for the cloud computing services to be provided with minimum disruption.

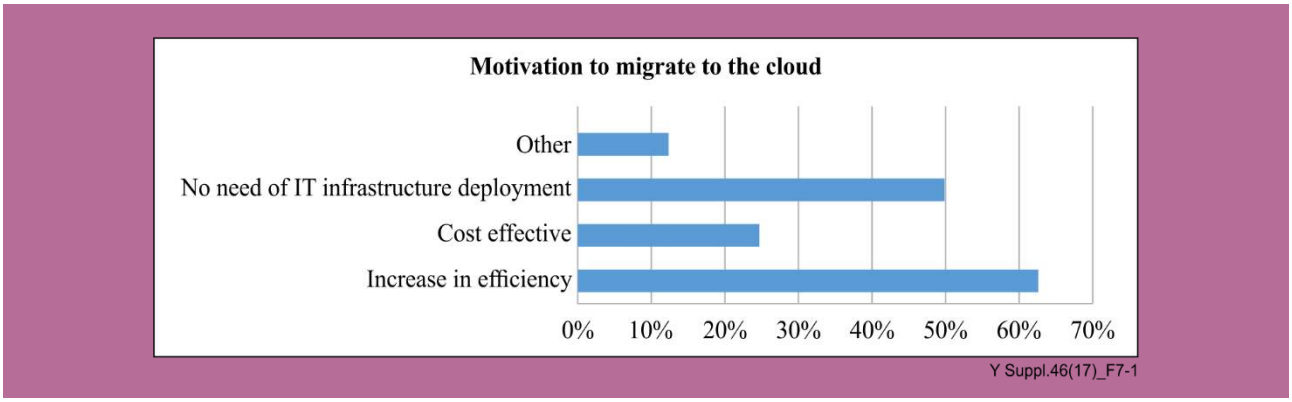


Figure 7-1 – Motivation to migrate to the cloud

In addition to the aforementioned motivations, respondents indicated the following motivations for migrating to the cloud:

- scalability in an instance;
- flexibility to switch vendors and platforms with minimal notice without cost overruns;
- resilience and an overwhelming degree of reliability;

- resource conservation owing to workforce redundancy;
- absence of wasted capacity, routine server maintenance or daily backup issues;
- data security and protection from denial of service attacks and spam;
- statutory compliance when housing and processing medical or government data;
- guaranteed uptime and SLA; and
- access to the latest licensed software and infrastructure without having to pay for it entirely.

Most CSPs have engaged in cloud service provision in order to provide their customers with an affordable solution that minimizes their infrastructure investment costs and has faster time to market. At the same time, the CSPs have been motivated to provide customer on-demand services in order to meet the needs of their customers who want to access these services at their convenience.

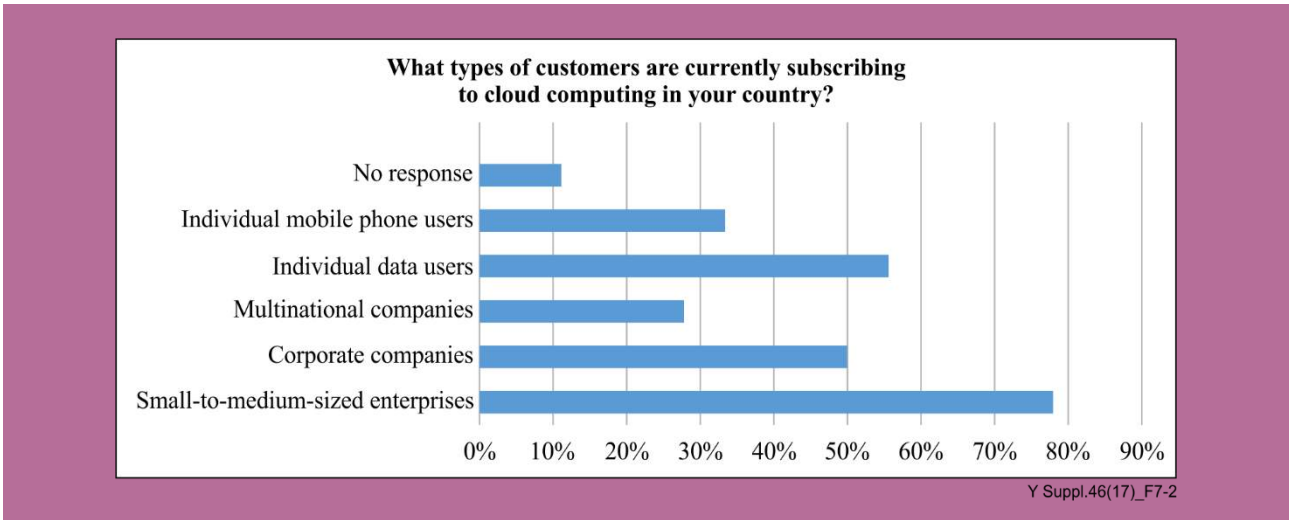


Figure 7-2 – Types of customers subscribing to cloud computing

The target market for most providers is skewed towards providing solutions to small-to-medium sized enterprises that want to minimize their infrastructure cost or completely outsource the data management services. Some relatively bigger corporate companies and organizations that include private and government institutions also use the cloud services motivated by the need to have some cost effective and efficient way of deployment of IT services.

The services mainly being offered by the CSPs include:

- online customer support;
- data storage through virtual private servers;
- mail hosting;
- communication and collaboration services;
- software as a service relating to business application such as accounting and human resource management; and
- infrastructure as a service.

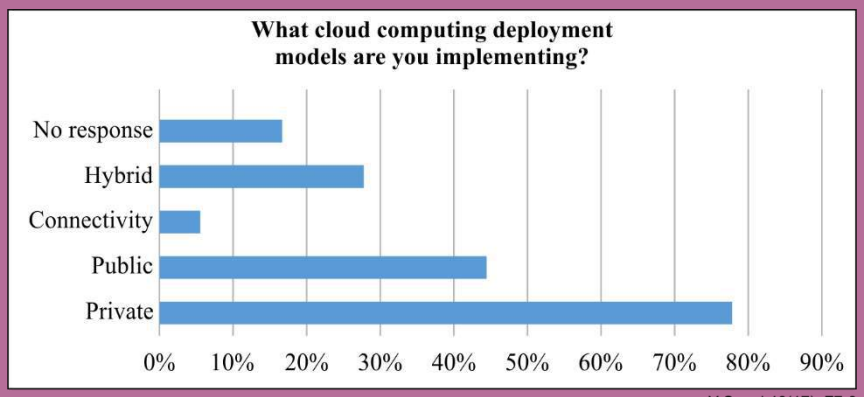


Figure 7-3 – Implemented cloud computing models

Case study: Senegal

Senegal is at the stage where information is being gathered by various experts to try and guide developments in cloud computing in the country. Specifically, some of the country's ICT operators have begun to implement or are already using cloud computing. At present, the application of cloud computing is mostly by big corporate organizations like banks. Many operational and regulatory issues such as policy implementation, licensing and security still remain unclear. Senegal would want to holistically provide an environment which promotes the availability of this service to many users.

Case Study: Zambia

In Zambia, there are about seven (7) cloud service providers already providing or in the process of offering cloud computing services to the public. Only one (1) of these providers has cloud computing as its core business. The other providers offer cloud computing services as value added services (VAS) to which they obtain a license from the ICT regulator, ZICTA.

7.3 Applications and services

The common cloud computing applications and services in use include:

- data storage;
- platform as a service; and
- software as a services.

The most salient service is infrastructure as a service (IaaS) which has demonstrated to be the most promising cloud computing solution. Other promising applications are:

- SaaS
- PaaS
- CaaS
- NaaS
- Data Storage

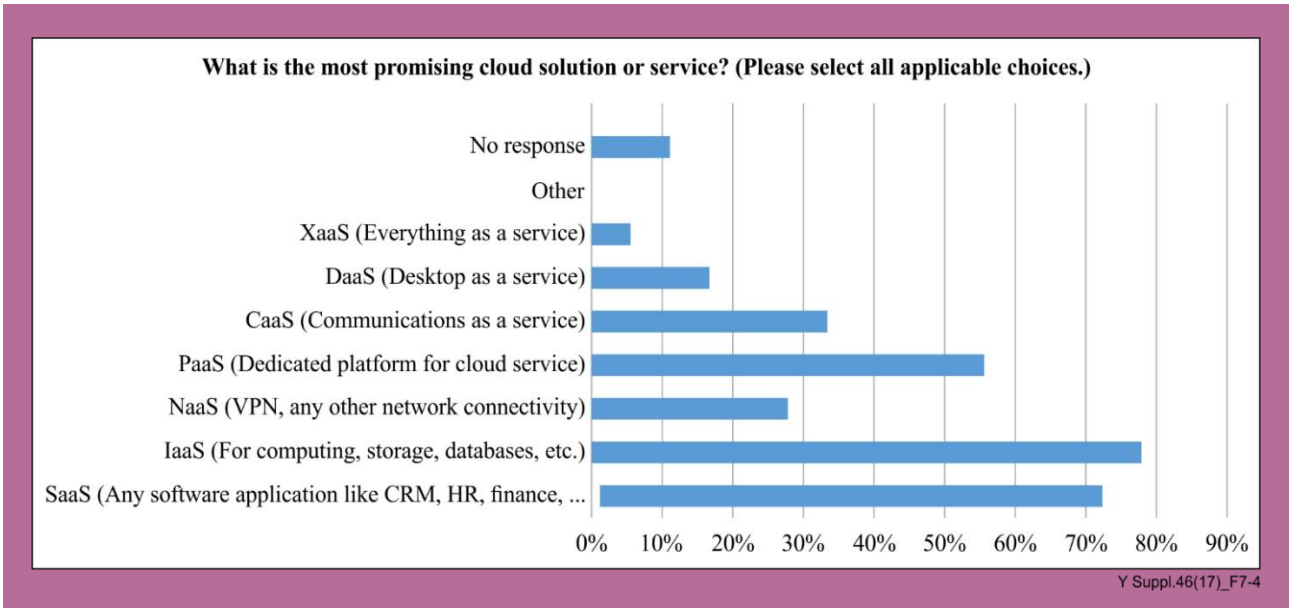


Figure 7-4 – Popular cloud computing services

7.4 Infrastructure requirements

Cloud related infrastructure that facilitate the access to or the transmission of cloud data include broadband infrastructure, internet exchange points (IXPs) and reliable electricity supply. Broadband connectivity is the prominent requirement that will enable access to cloud computing services.

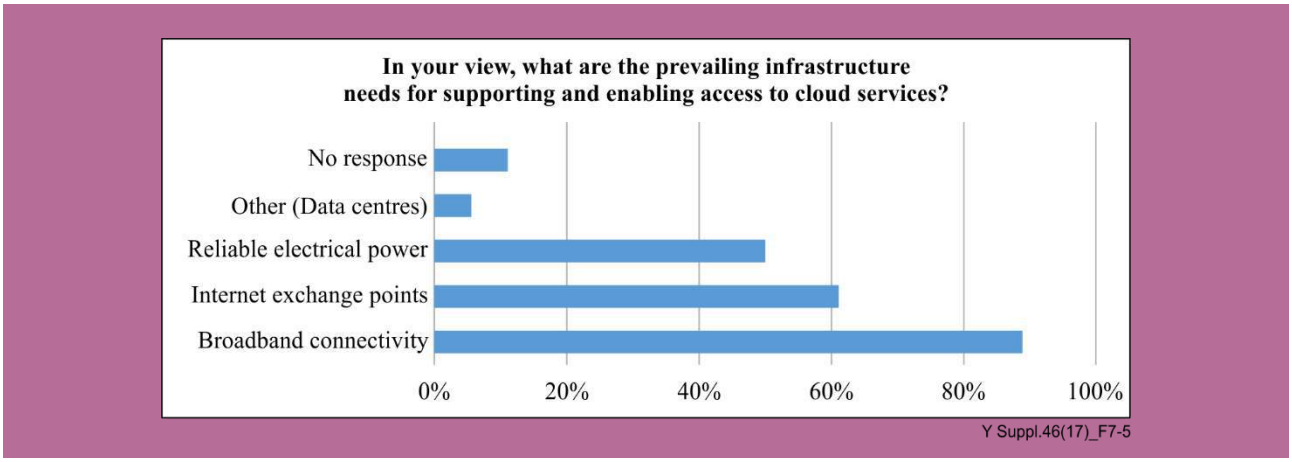


Figure 7-5 – Infrastructure requirements

7.5 Costs associated with cloud computing adoption

Cloud computing enables access to a multitude of services on the Internet. Thus, costs associated with cloud computing adoption depend on the context such as the deployment model, the service category and many others parameters including:

- licence fees;
- training on how to access cloud services;
- set up configurations; and
- Internet connection.

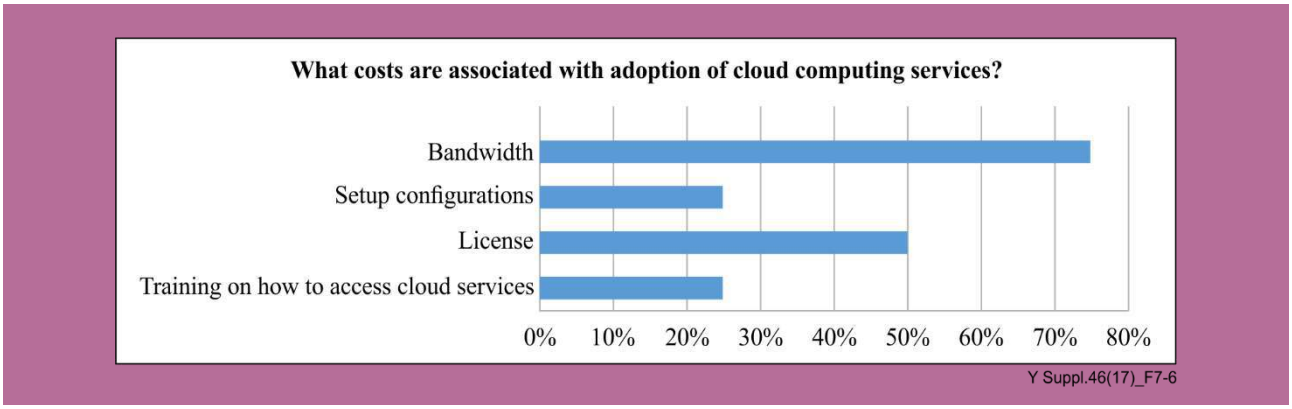


Figure 7-6 – Cost for adoption of cloud computing

8 Cloud computing requirements in developing countries

8.1 Standardization requirements

Several efforts are being made by various standards developing organizations (SDOs) to develop cloud computing standards that will foster the adoption of cloud computing services. Standards will set a benchmark that will be used to assess and select the most apt cloud computing solution for a given requirement.

There is need for fervent standardization of cloud computing in developing countries to enable the ease and flexible adoption of cloud computing and to optimize the use of this technology in these countries. Standards will also help to circumvent the possible vendor or operator lock-in of CSCs. The different aspects of the standards that need to be considered are as highlighted.

8.1.1 Cybersecurity

ITU has developed several recommendations on security in the cloud. The recommendations developed hitherto include:

- Security framework for cloud computing [ITU-T X.1601] which analyses security threats and challenges in the cloud computing environment and describes security capabilities that could mitigate these threats and address security challenges.
- Recommendation [ITU-T X.1602] on security requirements for software as a service application environments which analyses the maturity levels of SaaS application and proposes security requirements to provide a consistent and secure service execution environment for SaaS applications.
- Information technology – Security techniques ([ITU-T X.1631]) – Code of practice for information security controls based on [ISO/IEC 27002] for cloud services. This recommendation provides guidelines for information security controls applicable to the provision and use of cloud services for both CSPs and CSCs.
- Generic security guidelines for the cloud service customer (CSC) data in cloud computing are provide in [ITU-T X.1641]. This Recommendation also analyses the CSC data security lifecycle and proposes security requirements at each stage of the data lifecycle. Furthermore, it provides guidelines on when each control should be used for best security practice.
- Recommendation [ITU-T X.1642] on guidelines of operational security for cloud computing provides generic operational security guidelines for cloud computing from the perspective of cloud service providers (CSPs). A set of security measures and detailed security activities for the daily operation and maintenance are provided to help CSPs mitigate security risks and address security challenges for the operation of cloud computing.

8.1.2 Interoperability and portability

Cloud computing offers a diverse range of products and services such as IaaS, DaaS and SaaS as well as varied range of platforms on which these products and services are delivered and accessed. In order for these applications and services to work in tandem, there will be need for a prescribed set of rules that will ensure the synergistic application of these services and to also prevent vendor lock-in. Interoperability and portability standards will ensure that customers make the best use of the various cloud computing services and platforms that are available and that these products and services are able to cooperate and inter-work.

8.1.3 Service level agreements (SLA)

Most CSCs have signed service level agreements with their cloud service providers. The following are some of the benchmarks of the cloud computing applied in SLAs.

- Security and privacy of data
- Data ownership
- Accountability
- Flexibility
- Cost
- Performance
- Confidentiality
- Usability
- Support
- Service availability
- Quality of service
- Contract management
- Provisioning time
- Dispute process
- Applicable law

The multiple aspects of SLAs exemplify the need to have them standardized and this has also been generally expressed by most CSCs and CSPs. The relevant aspects that need to be standardised in SLAs include quality of service (QoS), data security and privacy, confidentiality and service availability.

8.1.4 Green standards

There is a global paradigm shift towards enabling environmental sustainability in all sectors of the economy. This is being achieved through a number of initiatives and technological innovations and advancements. Cloud computing is one such innovation that is envisaged to contribute significantly towards achieving environmental sustainability through resource pooling. However, the increasing demand for cloud services has drastically increased the energy consumption of data centres, subsequently challenging the energy efficiency of these data centres.

Many strides are being made to ensure that the deployment of cloud computing infrastructure such as data centres does not negate the benefits of the cloud computing technology and exacerbate the negative impact of cloud services on the environment. ITU has developed a number of recommendations that will support energy optimization in data centres. These include:

- [ITU-T L.1300] which describes best practices aimed at reducing the negative impact of data centres on the climate. The application of the best practices defined in this Recommendation can help owners and managers to build future data centres, or improve existing ones, and to operate in an environmentally responsible manner. Such considerations will strongly contribute to a reduction of the impact of the information and communication technology (ICT) sector on climate change.

- [ITU-T L.1301] which establishes a minimum data set necessary to manage data centres and telecommunication rooms in an environmentally responsible manner. The Recommendation specifies the communication interface and defines the parameters to be communicated depending on the type of equipment used in data centres, such as power systems (alternating current (AC)/direct current (DC) and uninterruptible power supply (UPS) and energy distribution), cooling systems and ICT equipment.
- [ITU-T L.1302] which specifies an energy efficiency assessment methodology for data centres and telecom centres, test equipment accuracy requirements, assessment period, assessment conditions and calculation methods.
- [ITU-T L.1320] which contains the general definition of metrics, test procedures, methodologies and measurement profiles required to assess the energy efficiency of power and cooling equipment for telecommunications and data centres.

8.1.5 Other standards

Other standards would be developed as the need arises.

8.2 Human resources

Inadequate human resources to fully implement and utilise cloud computing services in developing countries has been identified as a constraint. In order to make cloud computing services a reality in developing countries, there is need to build human capacity and to develop the relevant skills in the following areas:

- standards development;
- auditing of cloud service provision to ensure compliance with the relevant regulations;
- management of the cloud infrastructure and service provision to enable a smooth migration and integration of cloud services as well as the execution of other legal and business processes;
- regulation of the various facets of cloud service provision such as infrastructure installation and management;
- cyber-security, service delivery and data protection; and
- cloud applications development to create new opportunities for new services.

8.3 Data centres

Data centres are considered as one of the infrastructure requirements for supporting and enabling access to cloud services. For this purpose, the establishment of data centres in developing countries should take into account some pillars, including the following:

- **high availability**: Service continuity and high availability of data centres infrastructure, based on Tier III specifications of the [TIA-942 Standard], should be ensured;
- **security**: Data centres should be aligned with international data Centre security standards (physical and environmental safety, technical security, …);
- **energy efficiency**: Ensuring the energy efficiency of data centres by increasing cooling efficiency and reducing power consumption is essential. Redundancy of power and cooling supplies should also be guaranteed;
- **cloud readiness**: In addition to the usual data centre services (such as dedicated private area, dedicated rack or colocation, dedicated server,…), data centres would be scalable and ready to support a wide range of cloud services such as virtual private server, virtual private cloud, cloud back-up, virtual load-balancer, virtual firewall, web hosting and elastic storage. For this reason, data Centres should ensure higher connectivity to LANs and storage area networks (SANs) and use virtualization for multi-tenancy; and

- **service operation centre**: The management of processes and functions of data centres should be controlled by a dedicated service operation centre, which will mainly take in charge the management of access, events, requests, incidents, service desk 24x7, technical components, applications and IT operations.

As adoption increases, cloud services will continue to drive the evolution of several aspects of data centres in developing countries, from architecture to software and control processes.

8.3.1 Data centres – Case studies

Case study 1: National data Centres in Zambia

Zambia has established a government owned cloud service provider, the Zambia National Data Centre Limited (ZNDC). This is a company limited by guarantee through the ICT regulator, Zambia Information and Communications Technology Authority (ZICTA). The establishment of the ZNDC with three geo-located data centres will provide a platform for both government and private sector to consume secure, highly reliable and available cloud Services from the Tier III Uptime certified data centre.

The data centres are not just traditional data centres offering reliable power and cooling services only. They are modular data centres built on cloud architecture with virtualization as the bedrock. The three data centres provide on demand cloud services such as e-mail as a service, infrastructure as a service (IaaS), back-up as a service (BaaS), disaster recovery as a service (DraaS) and platform as a service (PaaS).

The high level topology of the data centres is shown in Figure 8-1:

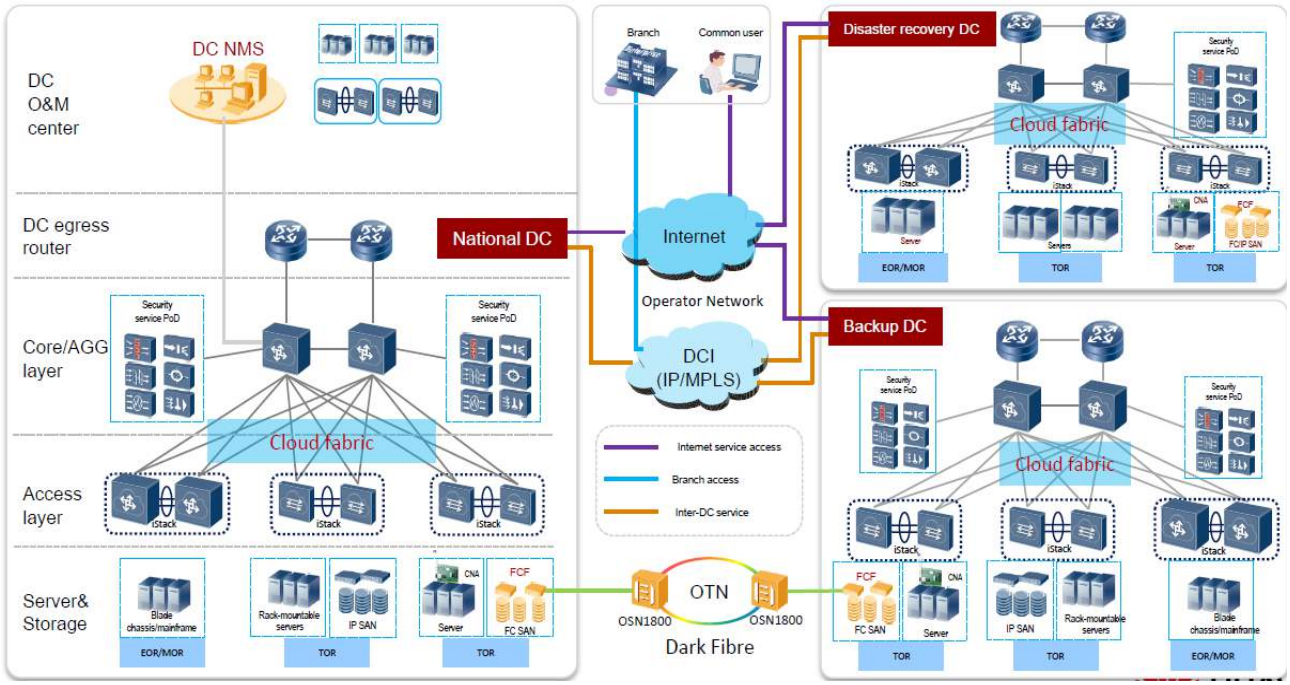


Figure 8-1 – High-level topology of data Centres

The national data centre has three sites that are located in geographically spread areas with a combined floor space of 1,600 square metres. The sites were chosen based on the country spread so that one site in the northern part of the country can serve the northern region of the country while the other two will serve the central and southern part of the country.

The data centres are designed for an average power usage effectiveness (PUE) of 1.3. The facility has a combined rack count of 206 with 24/7 network operation centre technicians and mechanical and electrical (M&E) staff.

The data centres are built to Tier III standard with multiple dark fibre and MPLS links, multiple DWDM and dual full stack IPv4 and IPv6 support.

The Zambia National Data Centre is cognisant of the challenges affecting cloud computing uptake in the country. Among the challenges is connectivity. The data centres have been declared as carrier neutral data centres allowing all ISPs and carriers in the country to form a local traffic fabric loop at the data centres. With this, data centre clients have a choice of Internet service providers to choose from as and when service level agreements (SLAs) are not met.

In cognizance of security challenges, measures have been taken to mitigate these challenges by adopting best practices from regional data centres in Kenya and South Africa. The data centres have adopted ISO 27001 and is in the process of undergoing the payment card industry data security standard (PCI DSS) to optimise security as the centre will handle financial data.

In order to increase client confidence and trust, the ZNDC facilities are undergoing Tier III certification with the Uptime Institute (UI) to guarantee availability and operational and sustainability of the facility.

Case study 2: Tunisie Télécom

Tunisie Télécom, the incumbent telecom operator in Tunisia, considers data Centres as an extension of its infrastructure to support the convergence of communication and information technologies. In this regard, Tunisie Télécom has built, to date, three data centres, as follows:

a) Primary data center: Carthage Data Centre

Located in the northern suburb of the capital Tunis, and inaugurated in October 2013, this data centre, is the largest data centre of Tunisie Télécom (space of the data centre: 2 700 m^2, hosting space: 660 m^2) and it has the largest capacities among Tunisie Télécom's data Centres in terms of hosting (200 racks), energy and connectivity.

This data Centre is ISO 27001-certified (*Information Security Management System*) since May 2016 and it is compliant with the specifications of ISO 14001 (*Environmental Management System*) and Tier III certifications (the process of request of these two certifications is ongoing). Carthage Data Centre is currently hosting the cloud computing platform of Tunisie Télécom as well as data for many clients from Tunisia.

b) Secondary data centre: Kasba Data Centre

This data centre is located in the capital Tunis, around 20 km from the primary data Centre. It was the first data centre established by Tunisie Télécom over an area of 280 m^2. This data centre is hosting the SaaS platform of Tunisie Télécom.

c) Disaster recovery data centre: Kairouan Data Centre

This data centre was recently established and it is located in the western region of the country, around 160 km from the primary data centre. It is used for disaster recovery and it guarantees a physical and geographical redundancy.

Each data centre is compliant with [TIA-942 standards], and each of them is connected with at least two different fibre links to Tunisie Télécom's MPLS Backbone to ensure redundancy (10 Gbit/s fibre links for Carthage and Kairouan Data Centres and 1 Gbit/s fibre links for Kasba Data Centre).

8.4 Electricity supply

Over 50 per cent of the CSP questionnaire respondents indicated that electricity supply is one of the main challenges for the provision of cloud computing services.

The problems of electricity supply in most developing countries are similar and are usually three fold:

i) **limited access**: Vast areas of many developing countries have limited access to electricity.

ii) **costly**: Where electricity is available, it is usually expensive.

iii) **poor quality**: Electricity in most developing countries is of poor quality and intermittent.

Power may raise the operational cost for CSP while on other hand it may contribute to poor quality of service if it is not reliable. These issues must be resolved if developing countries are to enjoy the benefits of cloud computing services.

8.5 Network infrastructure

According to the findings of the questionnaires, broadband connectivity was identified by CSPs as the most prevailing infrastructure requirement to support and enable access to cloud services.

In fact, cloud computing performance depends on consumer's Internet connection, used to access cloud services. With a huge amount of data stored in the cloud, connections need to be high-speed and reliable in order to allow cloud computing resources to be easily distributed, and without enough bandwidth, the delivery of cloud computing services would not be feasible. Unfortunately, consumers' access to affordable broadband Internet is still not satisfactory in many developing countries, especially in the least developed countries. Most of these countries rely on mobile broadband networks which are in many cases characterized by low speed and high latency and consequently are not suitable for cloud service delivery especially for applications such as video-steaming and real-time computing.

Moreover, cloud performance closely depends on network performance. For this reason, and in order to provide a real added value for cloud services, the network components for cloud services composition and delivery should meet a number of requirements in terms of flexibility, scalability, and on-demand resource provisioning, and offer the necessary advanced network functions to guarantee performance, security and availability of cloud services.

According to [ITU-T Y.3510], there are several types of networks involved in cloud computing services delivery and composition, such as:

i) **intra-datacentre network**, which is the network connecting local cloud infrastructures, such as the data centre local area network use to connect servers, storage arrays and L4-L7 devices (e.g., firewalls, load balancers, application acceleration devices);

ii) **access and core transport network**, which is the network used by CSCs to access and consume cloud services deployed by the CSP; and

iii) **inter-datacentre network**, which is the network interconnecting remote cloud infrastructures, taking into account that these infrastructures may be owned by the same or different CSPs.

[ITU-T Y.3510] listed a number of requirements for the networking resources of each of the access and core transport networks, intra-datacentre networks and inter-datacentre networks. However, some general requirements are applicable on the three types of networks where networking resources should be scalable, ensure services' performance and availability in order to meet SLA objectives, be able to adapt dynamically to the traffic generated by cloud services, support IPv4 and IPv6 and support policy based control on flow by flow basis in a fine-grained manner.

Case study: Network connectivity at Tunisie Télécom's Carthage Data Centre

In order to ensure performance, security and availability of cloud services, Carthage Data Centre is connected with two different high-speed fibre links to Tunisie Télécom's IP MPLS Backbone (10 Gbits/link). The two links are completely different in order to guarantee redundancy and access continuity without any interruption (different access points at the data centre level, different paths to the IP MPLS Backbone, different PoP's locations, etc.).

Carthage Data Centre is also interconnected with the two other data centres of Tunisie Télécom (Kairouan Data Centre for disaster recovery, and Kasba Data Centre).

Besides, Tunisie Telecom has deployed all means (VRF, VLAN, Firewalls, anti-DDos protection, etc.) and procedures to prohibit any fraudulent connection on the private networks of customers.

8.6 Trust

One of the issues affecting the implementation of cloud computing services in developing countries relates to the mistrust of cloud computing services, which in its nature generally puts a curtain wall between the CSP and the CSC. Potential users of cloud computing services will accept the "curtain wall" if there is strong evidence that the CSP on the other side of the "curtain" can be trusted. For that to happen there should be conditions which must be agreed upon and met by the CSP to assure the CSC that they can be trusted.

The development of those conditions and the framework of meeting them can be complicated if left up to the CSP and CSC to handle. However, if the efforts of international standardization organizations such as ITU produces recommendations on trust, both the CSP and CSC are more likely to feel comfortable to work with such recommendations.

The current cloud computing trust and security issues are closely related. In fact the uptake of cloud computing services in developing countries can suddenly increase by merely making stakeholders aware that issues of trust are different from those to do with security and show them how they are handled without confusing the two.

The ITU has already developed Recommendations such as [ITU-T Y.3514], "Cloud Computing – Trusted inter-cloud computing framework and requirements". This Recommendation specifies a framework of trusted inter-cloud computing and relevant use cases. It provides general requirements for trusted inter-cloud and specific ones related to governance, management, resiliency, security and confidentiality of trusted inter-clouds on security in the cloud. It is based on the framework of inter-cloud computing [ITU-T Y.3511].

The scope of this Recommendation includes:

– overview of trusted inter-cloud computing;
– general requirements for trusted inter-cloud;
– requirements for governance of trusted inter-cloud;
– requirements for management of trusted inter-cloud;
– requirements for resiliency of trusted inter-cloud; and
– requirements for security and confidentiality of trusted inter-cloud.

There are other closely related recommendations that ITU-T has developed which are very relevant to issues of trust of the cloud. These include:

- [ITU-T Y-3051] "The basic principles of trusted environment in information and communication technology infrastructure" which is devoted to the issue of creating trusted environment in ICT infrastructure providing information and communication services. The Recommendation provides the definition, common requirements and the basic principles of creating trusted environment.
- [ITU-T Y.3052] "Overview of trust provisioning for information and communication technology infrastructures and services" which provides an overview of trust provisioning in ICT infrastructures and services. It introduces the necessity of trust to cope with potential risks due to lack of trust.

- [ITU-T X.1258] "Enhanced entity authentication based on aggregated attributes"; aggregating attributes from multiple attribute authorities may be needed in order to enable a relying party to enhance its trust in the identity of a party. The aggregation can be regarded as having to deal with a collection of globally unique identifiers, which is common across all attribute authorities.

All ICT stakeholders have a role to play in making cloud computing services more trusted in developing countries. There could be some aspects that may differ from country to country but a common framework could be provided to make it easier for stakeholders to accept them.

It is believed that the more trust issues are handled, the more CSCs will take up cloud computing services.

9 Challenges of cloud computing adoption

The regulation of cloud computing services is not properly defined in most developing countries which greatly inhibits the adoption of cloud services in these countries. The main challenges that have affected the adoption of cloud computing in developing countries include:

9.1 Lack of regulatory framework for cloud computing services

Developing counties lack the regulatory framework to govern the provision and consumption of cloud computing services.

9.2 Security and privacy concerns

Data security and privacy are the most salient challenges associated with the adoption of cloud computing services in developing countries. CSCs tend to be sceptical about handing over their data to a third party. There are concerns of confidentiality of company information, the likelihood of corruption of data and the fate of CSC's data when there is a switch over to another service provider or after termination of the contract. CSPs have a responsibility to demonstrate their credibility as well as to improve awareness on the safety of cloud computing services.

A lot of speculation has been raised on the geographical location of the data centres. CSCs feel they lose control of their data once it is in a location outside their jurisdiction. The local authorities may also not have control over such data. CSCs get concerned regarding how they could be protected in such instances or indeed what each country's strategy could be in this regard.

9.3 Infrastructure needs

Some CSPs highlighted the need to invest more in infrastructure that could provide a broader diversity of cloud computing services as well as increase the capacity of providers to serve more users. This includes the need to deploy data centres, Internet exchange points (IXP) and robust electricity infrastructure sources.

9.4 Capacity building

CSPs highlighted the need for capacity building initiatives on the use, regulation and implementation of cloud computing services as well as the development of cloud computing applications that will create new opportunities for cloud services. The capacity building interventions could be targeted at corporate organizations as well as embedded in the curriculum for schools and tertiary institutions.

9.5 Quality of service

The provision of cloud computing services relies on good quality and reliable Internet services. There has been a general concern from the CSPs and CSCs about the unreliable and low internet connection speed over which cloud services are provided. The lack of IXPs has also resulted in users paying high international bandwidth prices thereby negatively affecting cloud service provision and uptake of cloud services in most developing countries.

9.6 Compliance limitations

Currently, there are no clear policies or regulatory frameworks on the provision of cloud computing services in most developing countries. Equally, there is a lack of standards adoption that will ensure adherence to international best practices for which CSPs could be held accountable. This has had adverse implications on the speedy uptake of cloud computing services.

9.7 High cost of broadband Internet

In its report of September 2017 [b-ITU/UNESCO] "The State of Broadband: broadband catalysing sustainable development", the Broadband Commission projected Internet penetration in developing world to reach 41.3per cent by the end 2017. Affordability, lack of skills and infrastructure are the reasons among the large gaps in connectivity around the world.

Internet is still not affordable in developing countries and cloud computing can be very expensive, especially in terms of bandwidth consumption, according to 75 per cent of the questionnaire respondents.

Besides the obvious factors, migration to cloud computing could lead to unexpected additional costs according to the [b-ITU-D report] in April 2012 entitled "Cloud Computing in Africa: Situation and Perspectives". Indeed, some operations can be very costly especially if they are not well planned in the timeline. For example, moving large volumes of data to or from the cloud can be very expensive. The same is true of data storage on the cloud for very long periods. Such an operation can be very expensive without the service user realizing it in the short term.

10 General recommendations on adoption of cloud computing by developing countries

General recommendations on cloud computing adoption in developing countries are listed and described as follows:

10.1 Regulatory framework

The provision and uptake of cloud services require an enabling environment respectively for CSPs and CSCs. A number of issues such as cyber security, privacy, data centre location and quality of service have to be looked into to make this possible.

International standardization organizations should participate in developing a model regulatory framework which developing countries can easily adopt.

10.2 Standards adoption

Developing countries are encouraged to adopt/adapt international standards relating to security and trust to stimulate the uptake of cloud computing services.

10.3 Basic broadband infrastructure

Broadband is the main infrastructure requirement to access cloud computing services. As such, it is necessary to ensure that broadband infrastructure is developed as the bedrock for cloud services to thrive.

Policy makers and regulators should put in place policies and regulations that support the development of broadband infrastructure.

10.4 Internet exchange points

IXP can reduce the exchange of data between CSPs.

It is recommended that developing countries consider the establishment of national and regional IXP.

10.5 Reliable electricity

Electricity is one of the main challenges for the provision of cloud computing services.

To benefit from cloud computing services, developing countries have to resolve the problems of inaccessibility, unaffordability and poor quality of electricity.

10.6 Data centres

It is generally recommended that data centres should be of an appropriate tier-level in order to offer the necessary redundancy and resilience to the cloud computing services.

The end result would be a win-win scenario where CSPs will have enough customers to sustain their businesses and CSCs would lower their OPEX and have the reduced burden of maintaining own computing resources.

Appendix I

Presentation of the results of the questionnaires for cloud service customers

I.1 List of responders

Eight responses were received from seven different countries.

Table I.1 – List of respondents

	Organization	Country	Submission
1	NCA	Ghana	By e-mail
2	Bank of Zambia	Zambia	By e-mail
3	Telecommunications Authority of Trinidad and Tobago	Trinidad and Tobago	By e-mail
4	Liquid Telecom	Zimbabwe	By e-mail
5	Telecel Zimbabwe	Zimbabwe	By e-mail
6	National Telecommunications Corporation Sudan	Sudan	Online
7	Uganda Communications Commission	Uganda	Online
8	MACRA	Malawi	Online

I.2 Responses to the questionnaire

1 General questions

1.1 What is your main line of business?

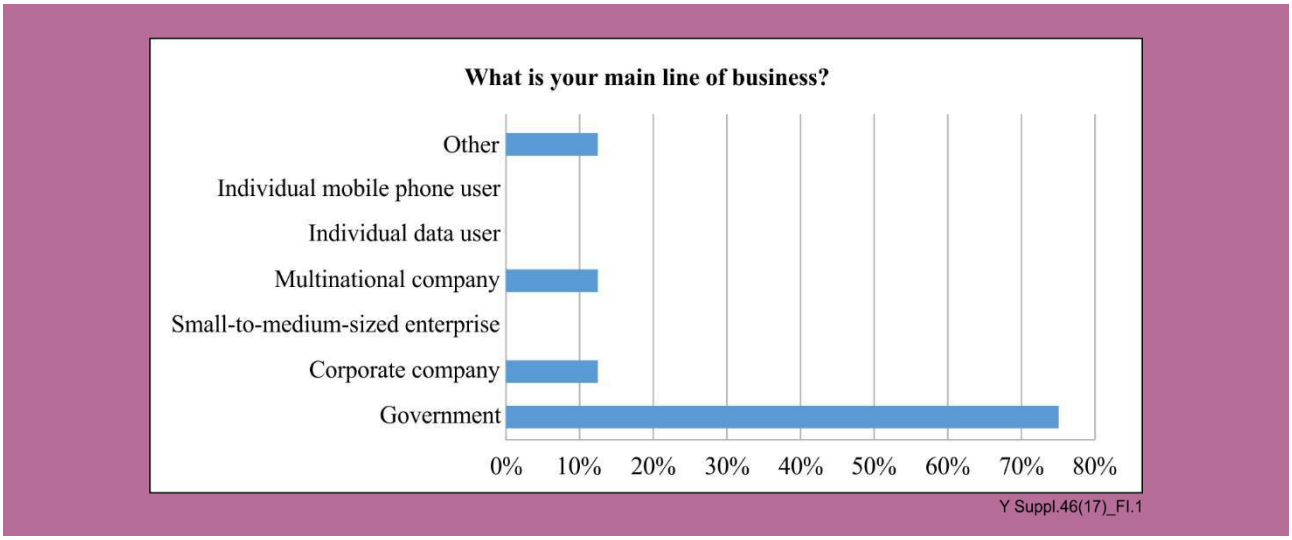


Figure I.1 – Respondent's main line of business

The majority or responders represent the government. There were also responders from a corporate company, a multinational company and an ICT regulator.

1.2 Do you use Internet to carry out day-to-day business transactions?

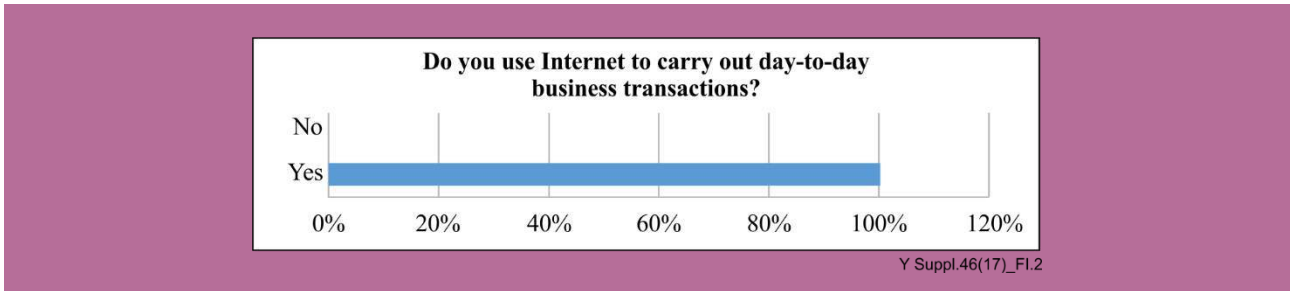


Figure I.2 – Day-today use of Internet

1.3 What main type of Internet connection do you use?

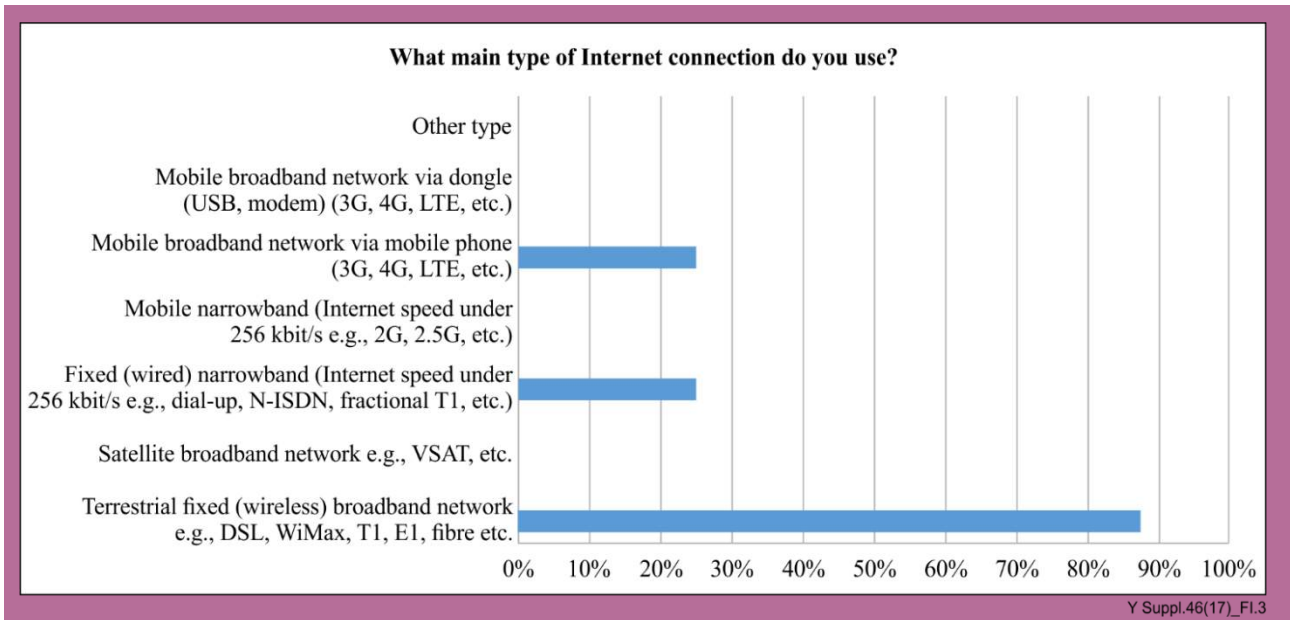


Figure I.3 – Type of Internet Connection

1.4 What was your motivation to migrate to the cloud?

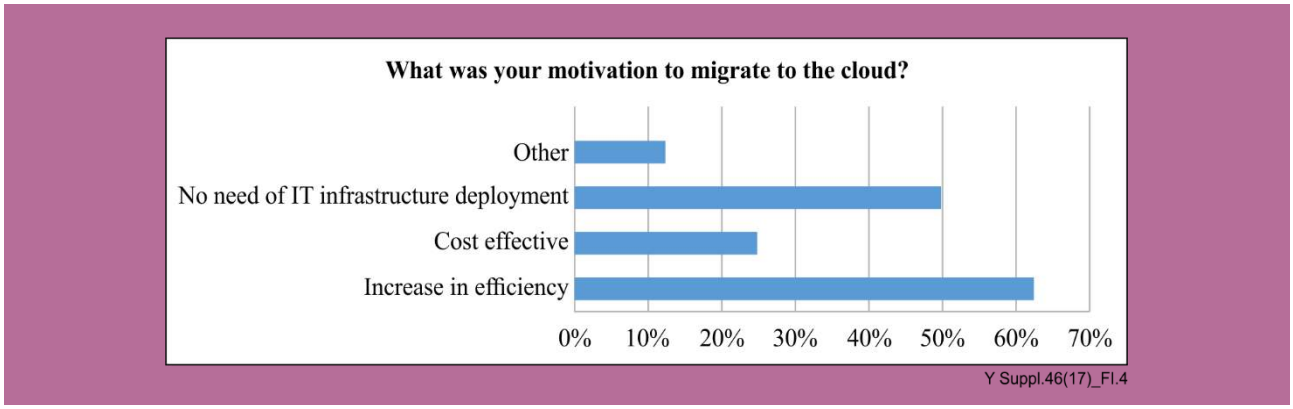


Figure I.4 – Motivation to migrate to the Cloud

In addition to the three proposed options (increase in efficiency, cost effectiveness and no need of IT infrastructure deployment), responders mention the following motivations to migrate to the cloud:

- scalability in an instance;
- flexibility to switch vendors and platforms with minimal notice without cost overruns;
- resilience and an overwhelming degree of reliability;
- resource conservation owing to workforce redundancy;
- absence of wasted capacity, routine server maintenance or daily backup issues;
- data security and protection from denial of service attacks and spam;
- statutory compliance when housing and processing medical or government data;
- guaranteed uptime and SLA;
- access to the latest licensed software and infrastructure without having to pay for it entirely.

2 Cloud computing usage

2.1 What were the criteria for selecting your current cloud provider?

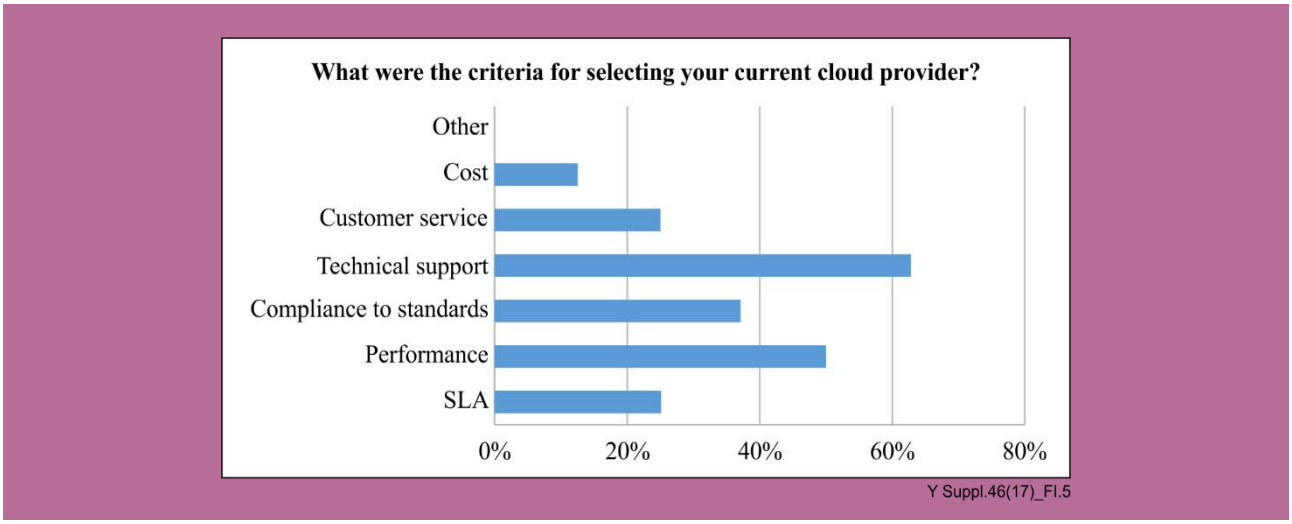


Figure I.5 – Criteria for selecting CSP

2.2 Which cloud computing service do you use?

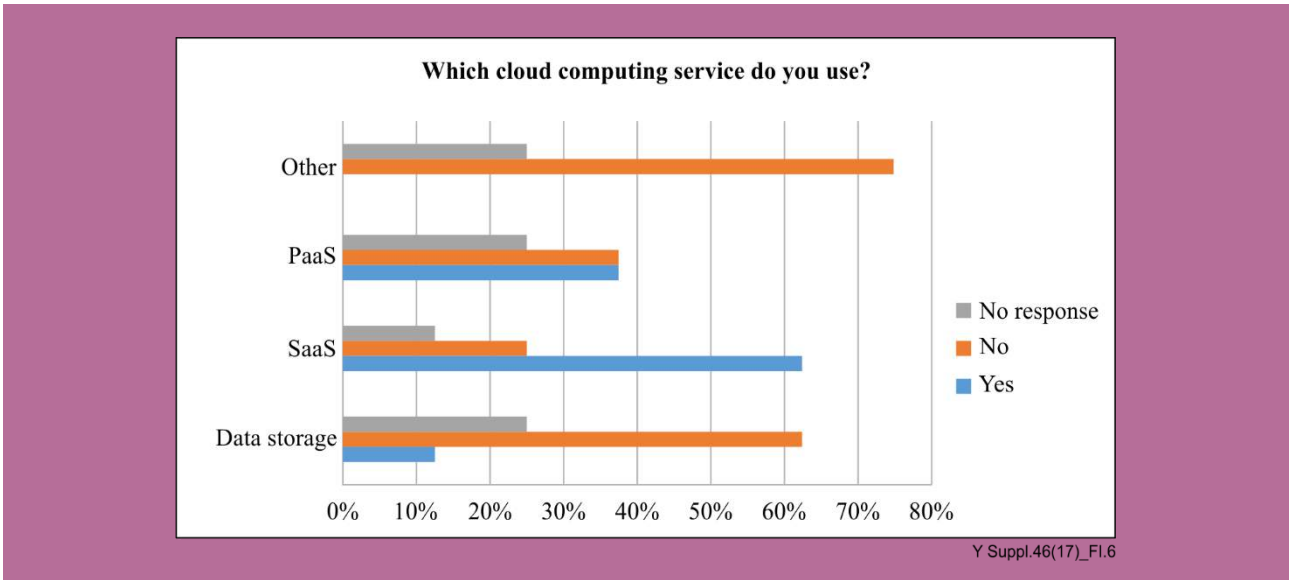


Figure I.6 – Popular cloud computing service

2.3 *What costs are associated with adoption of cloud computing services?*

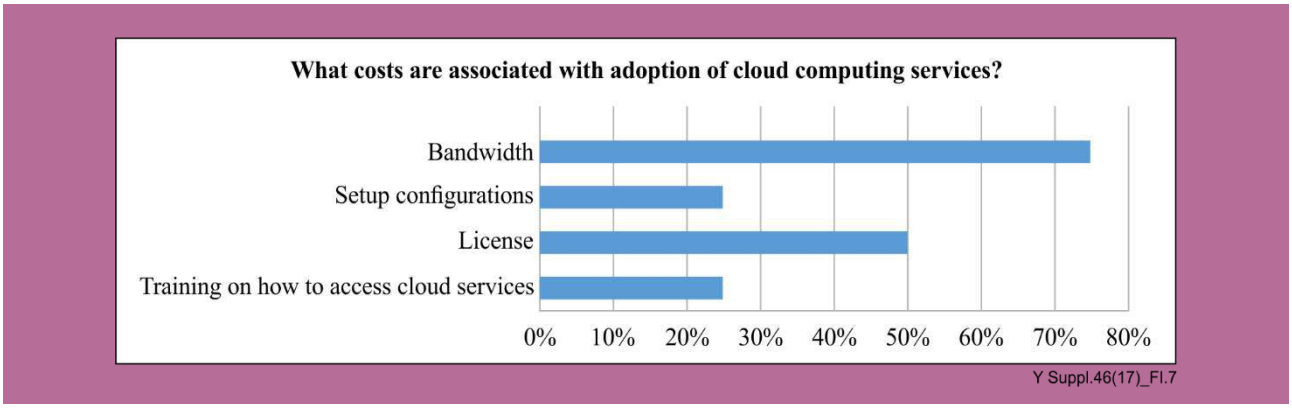


Figure I.7 – Cost for deployment of cloud computing services

3 Standardization requirements

3.1 *Have you signed any service level agreements (SLAs) to enhance customer protection?*

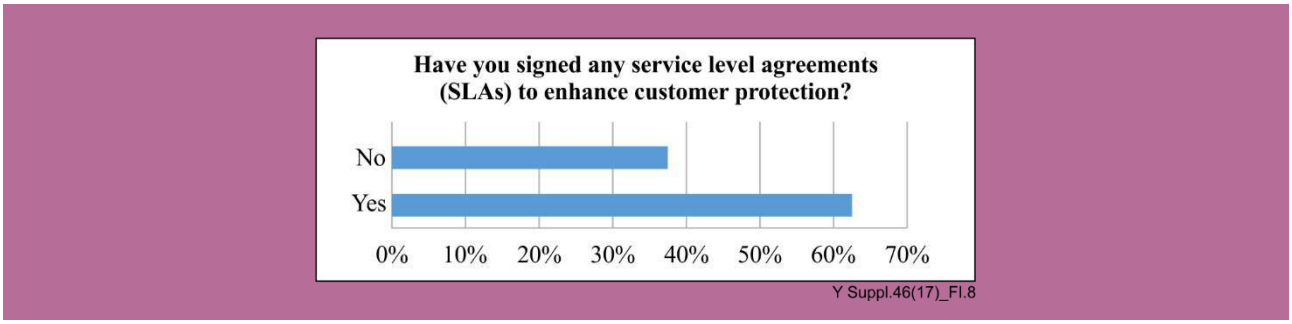


Figure I.8 – Service level agreements

3.2 *What are the service level agreement benchmarks for cloud computing?*

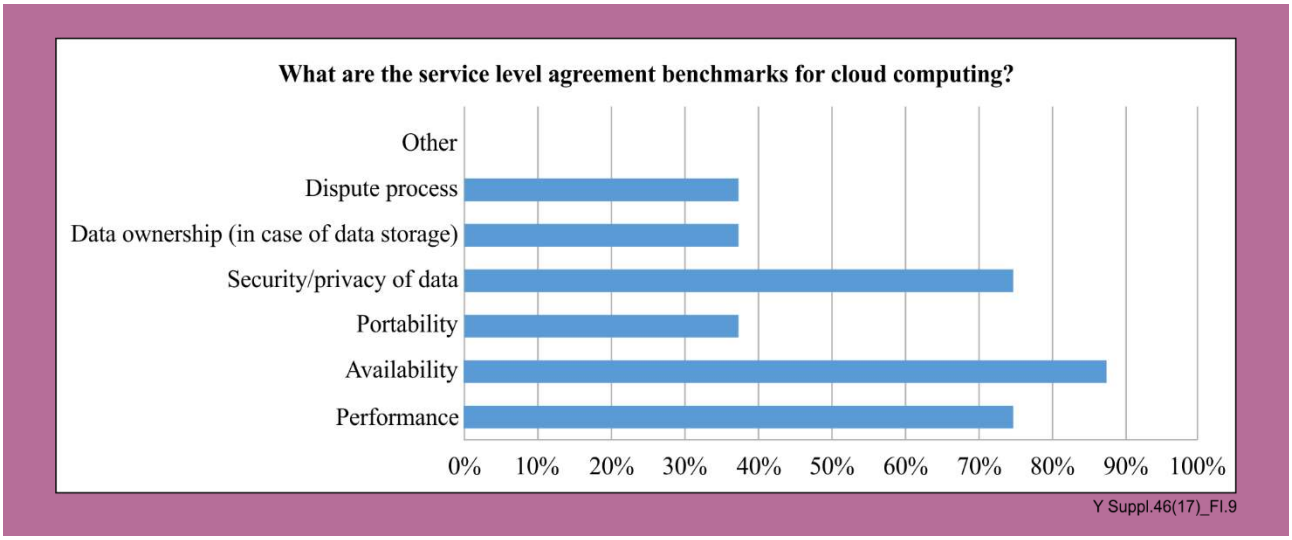


Figure I.9 – Popular SLA benchmarks

3.3 Do you think SLAs should be standardised?

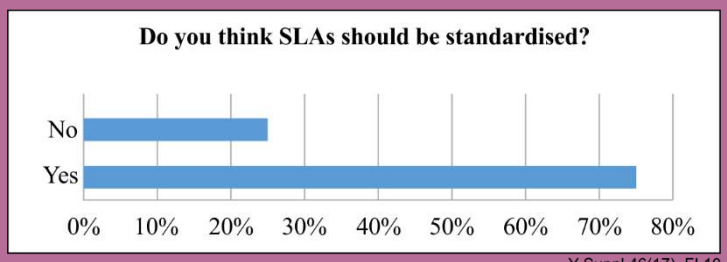


Figure I.10 – Standardization of SLAs

3.4 Can you identify some of the issues that are associated with cloud adoption that can be addressed with standards?

Received responses are the following:

- Speed
- Availability
- Data size limit
- Performance
- Portability
- Security/privacy of data
- Data ownership (in case of data storage)
- Dispute process
- Provision of general guidelines so that there is control and uniformity.
- Interoperability

4 Opportunities and challenges for cloud computing deployment

4.1 What do you think are bottlenecks and weakness that need to be addressed for an effective use of cloud services?

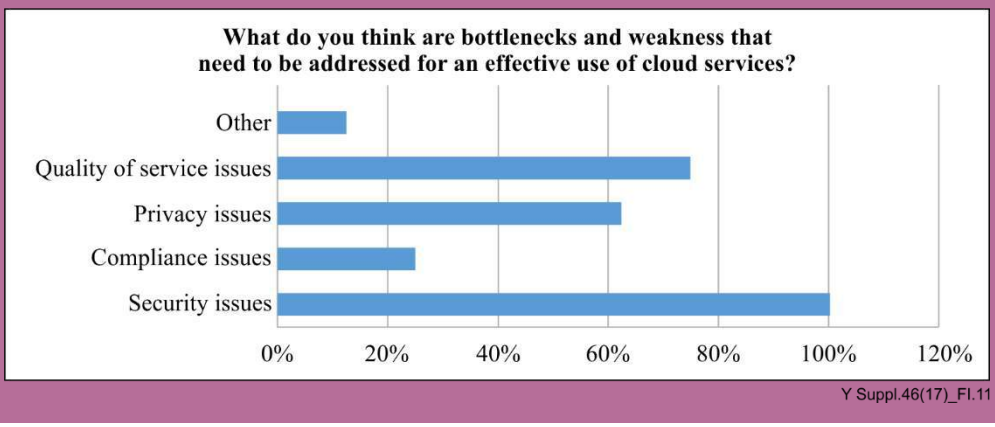


Figure I.11 – Cloud computing bottlenecks

In addition to the provided options, bandwidth availability and affordability were mentioned as bottlenecks and weaknesses that need to be addressed for an effective use of cloud services.

4.2 What do you think are some of the scenarios that can spur the use of cloud services in your country?

Received responses are the following:

- The pass of the right to information bill by parliament
- Overall cost savings
- Scalability in an instance
- Flexibility to switch vendors and platforms with minimal notice without cost overruns
- Resilience and an overwhelming degree of reliability
- Resource conservation owing to workforce redundancy
- Increased operational efficiency
- Absence of wasted capacity, routine server maintenance or daily backup issues
- Data security and protection from denial of service attacks and spam
- Statutory compliance when housing and processing medical or government data
- Guaranteed uptime and SLA
- Access to the latest licensed software and infrastructure without having to pay for it entirely
- Reduced cost of Internet service
- Increased privacy and security
- Cost of bandwidth
- The cost of investment in terms of infrastructure versus the use of cloud services
- The fact that services can be accessed and used from anywhere
- For SMEs, this cuts on costs of running the business
- No need to have premises to accommodate all staff
- Efficiency and cost reduction issues can spur the use of cloud services

Appendix II

Results of the questionnaire for cloud service providers (CSPs) on cloud computing status in developing countries

II.1 List of responders

Eighteen (18) responses were received from 15 different countries, 13 from Africa, one from Europe and one from Asia.

Table II.1 – List of respondents

	Organization	Country	Submission
1	Ministry for Digital Economy Development and Post	Burkina Faso	By e-mail
2	Operator	Senegal	By e-mail
3	Complete Enterprise Solutions	Zambia	By e-mail
4	BH Telecom	Bosnia and Herzegovina	By e-mail
5	Microsoft Cote d'Ivoire	Cote d'Ivoire	By e-mail
6	Altostrat Global LTD	Zambia	By e-mail
7	Liquid Telecom	Zimbabwe	By e-mail
8	Telecel Zimbabwe	Zimbabwe	By e-mail
9	CDTA	Algeria	Online
10	National Telecommunication Corporation Sudan	Sudan	Online
11	Ministry of Communications	Nigeria	Online
12	Tunisie Telecom	Tunisia	Online
13	MACRA	Malawi	Online
14	POTRAZ	Zimbabwe	Online
15	PURA	Gambia	Online
16	NCA	Ghana	Online
17	Botswana Communications Regulatory Authority	Botswana	By e-mail
18	Ministry of Communication and Information Technology (MCIT)	Afghanistan	By e-mail

II.2 Responses to the questionnaire

1 General questions

1.1 What is your main line of business?

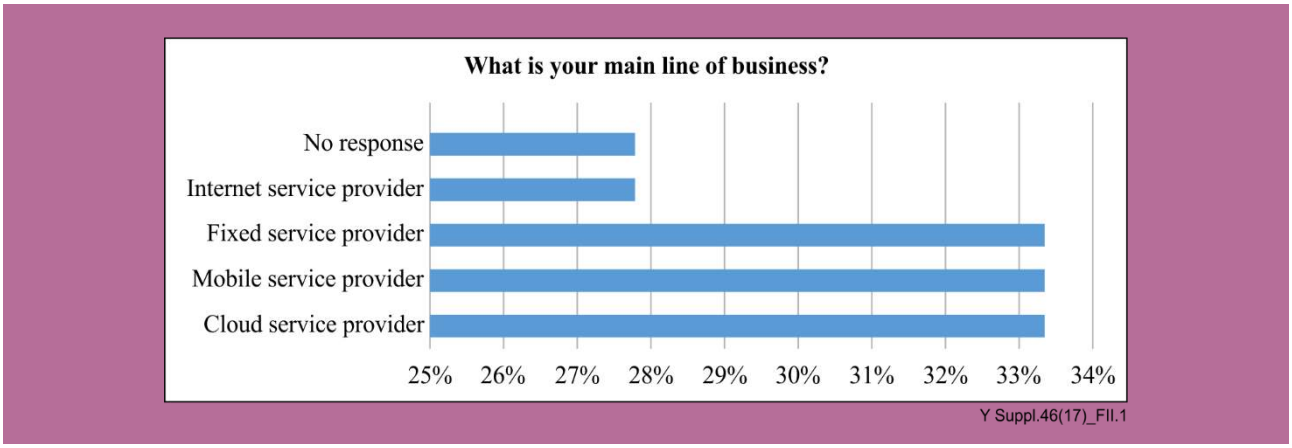


Figure II.1 – Respondent's main line of business

1.2 What means of connections are used in your country?

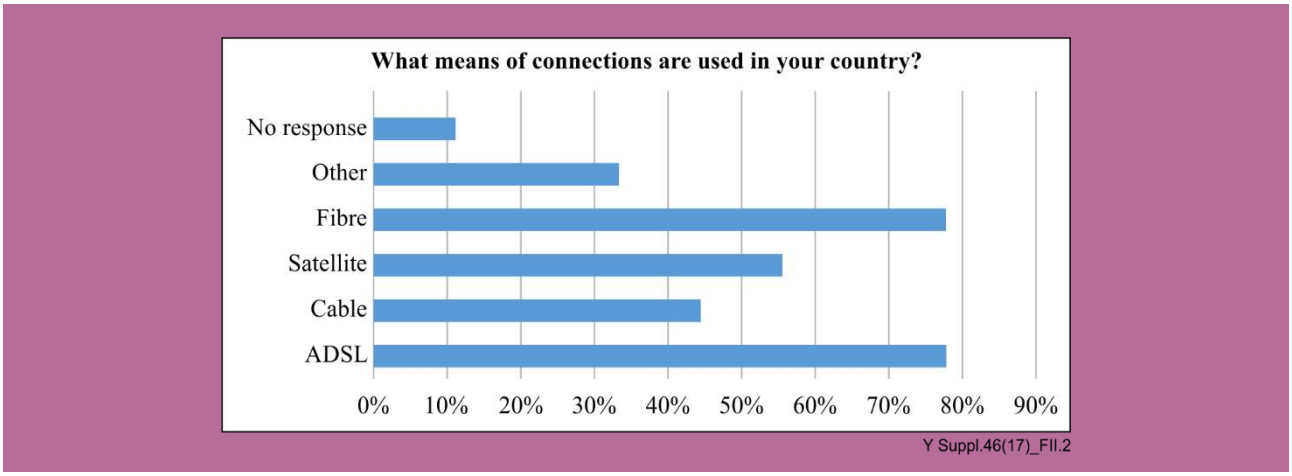


Figure II.2 – Network connectivity method

In addition to the provided options, responders mentioned "Wireless Radio Communication", "WIMAX", "Local network for the CDTA" and "Microwave" as means of connections used in their countries.

1.3 What types of customers are currently subscribing to cloud computing in your country?

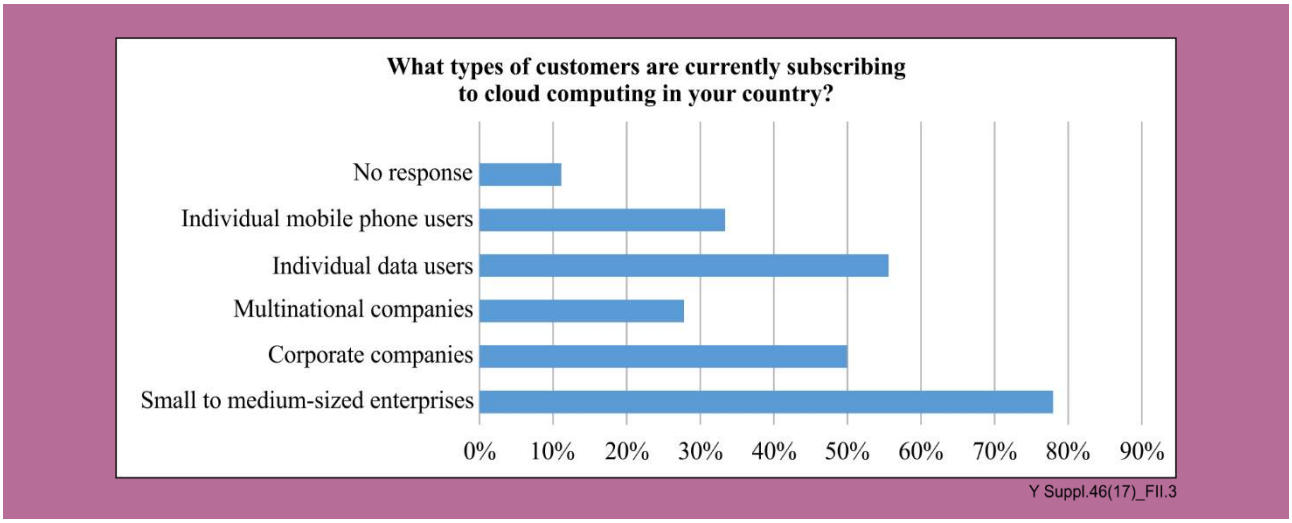


Figure II.3 – Cloud computing customer segments

1.4 How many enterprises in your country have migrated to the cloud till 2015?

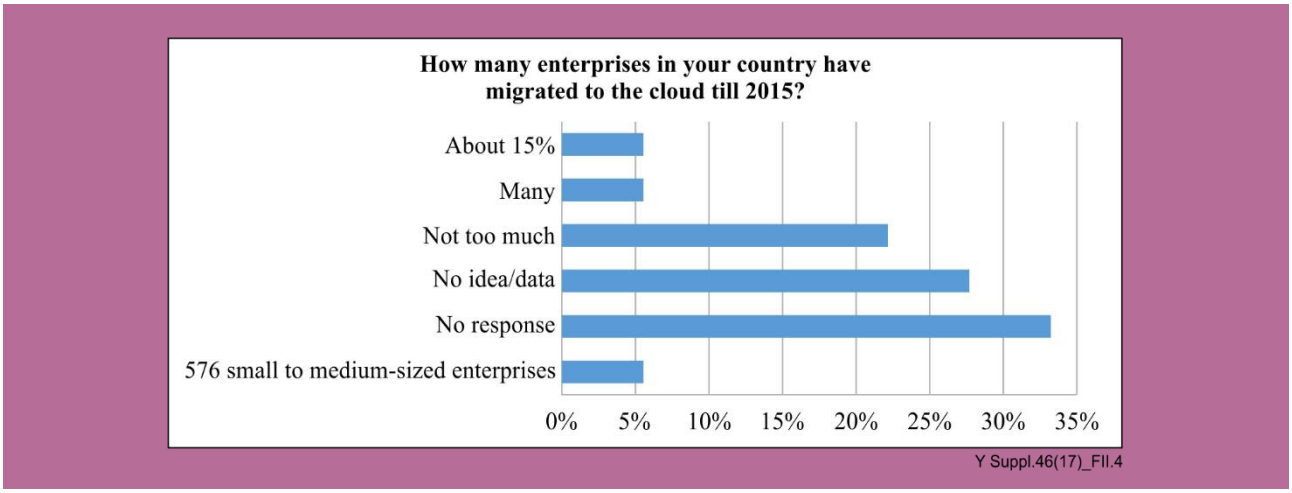


Figure II.4 – Cloud computing uptake

1.5 What are the reasons behind your engagement in the cloud computing area?

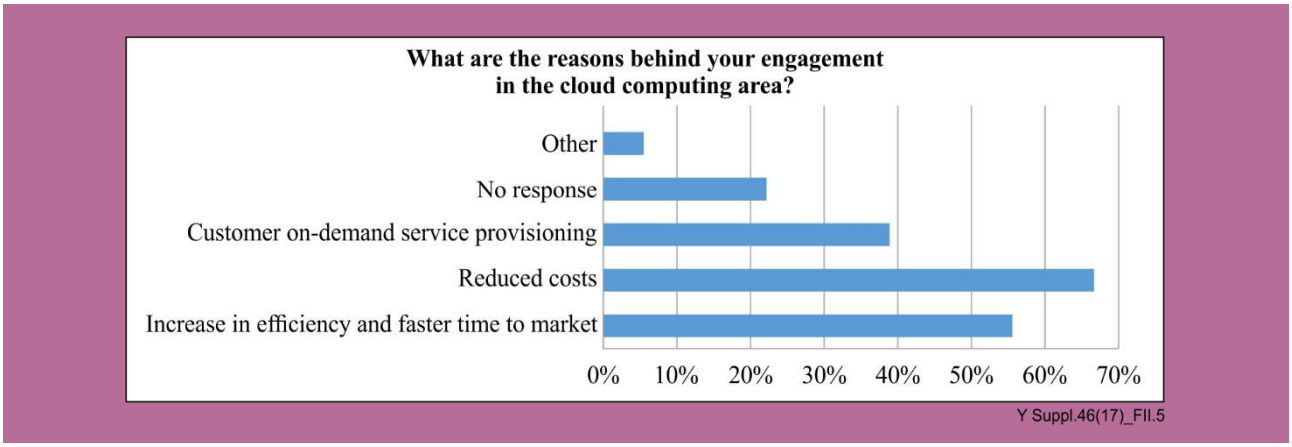


Figure II.5 – Drivers for cloud computing service provision

In addition to the proposed options, the developing of the sales of growth drivers was mentioned as a reason behind the engagement in the cloud computing area.

1.6 What kind of cloud service support are you more likely to use?

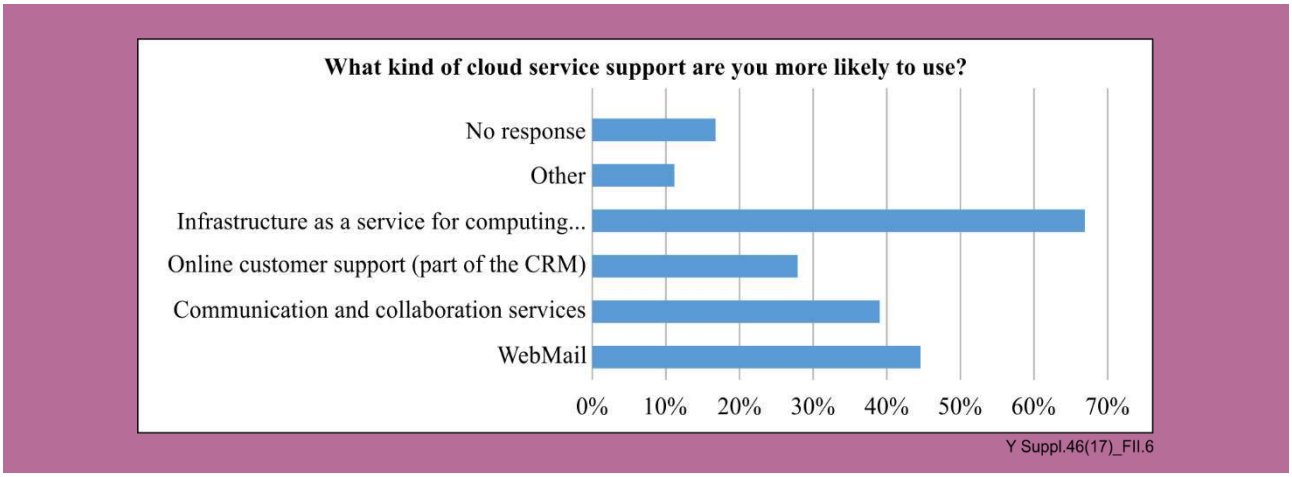


Figure II.6 – Popular cloud computing services

In addition to the proposed options, the following two responses were mentioned:

- SaaS business application (accounting, human resources management…) website management tool
- HPC for CDTA's researchers

2 Cloud computing deployment

2.1 What cloud computing deployment models are you implementing?

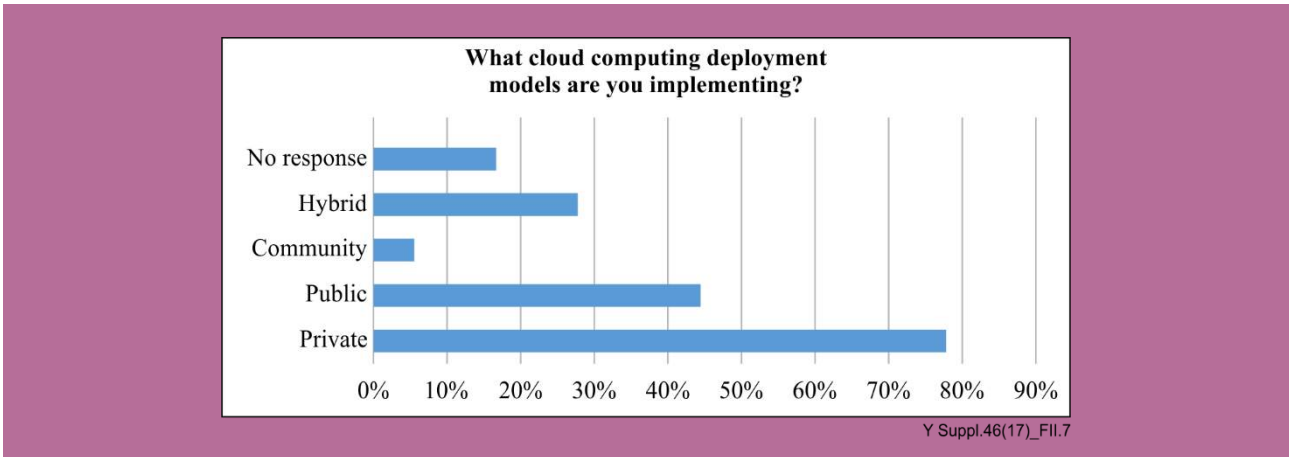


Figure II.7 – Popular cloud computing models

2.2 *What is the most promising cloud solution or service? (Please select all applicable choices)*

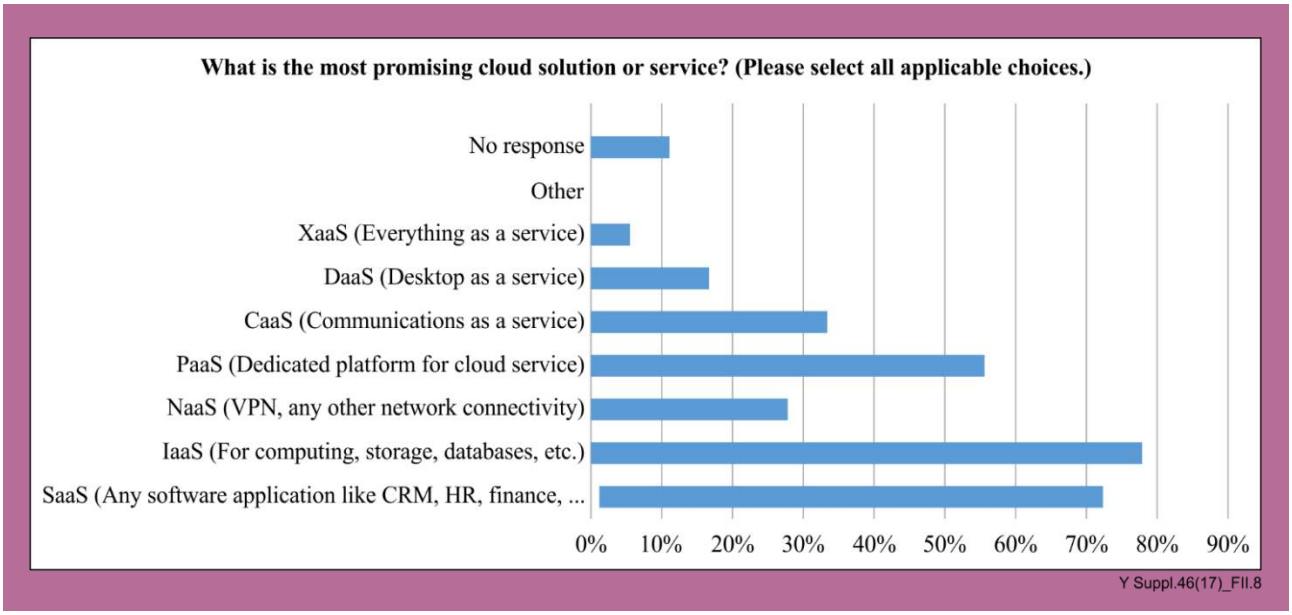


Figure II.8 – Popular cloud computing services

2.3 *Do you think that integration with your applications' demands in the cloud make it complex?*

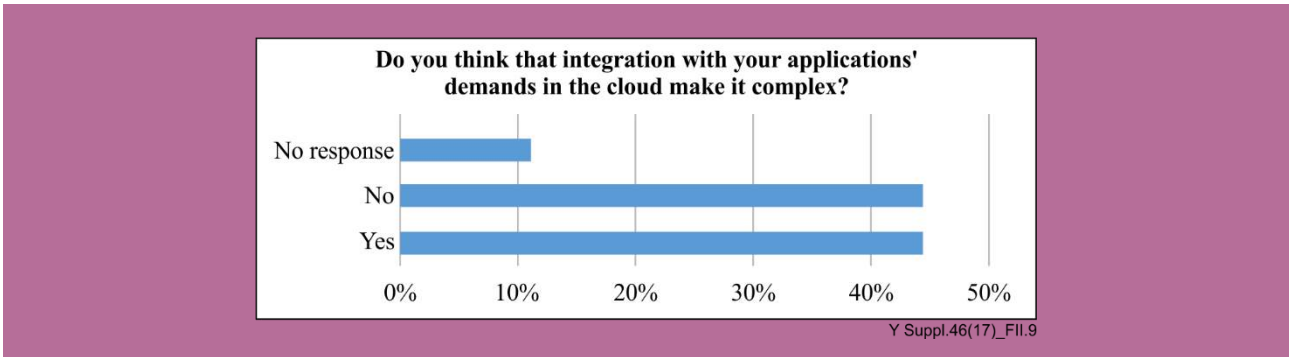


Figure II.9 – Complexity of application demand

2.4 *In your view, which technology scope should the CSP focus on?*

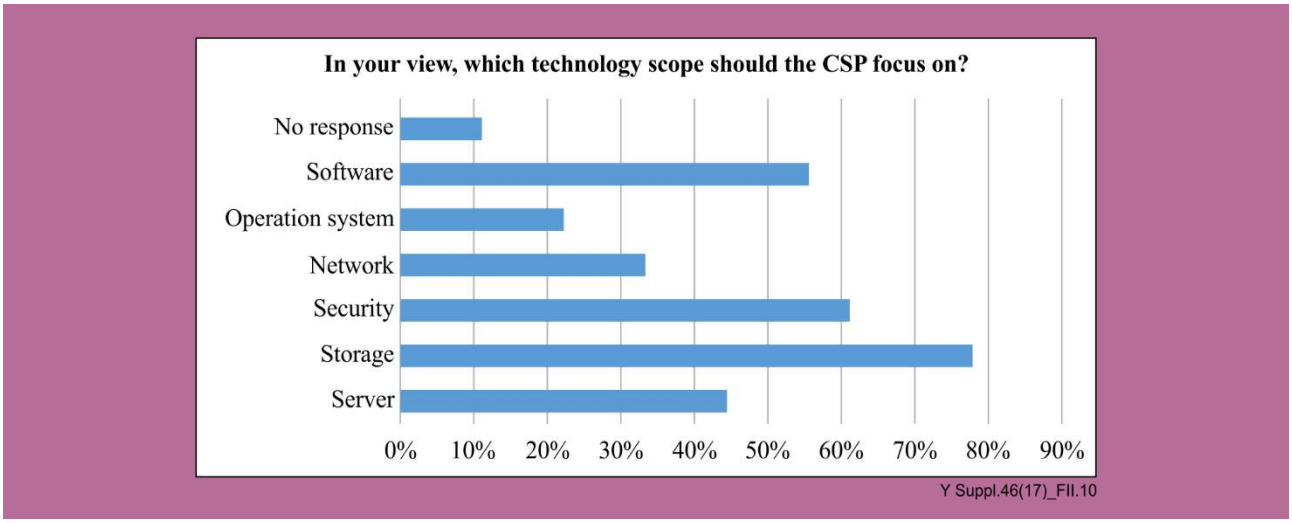


Figure II.10 – CSP Focus Technology

2.5 Do you consider important the rapid provisioning of cloud computing services?

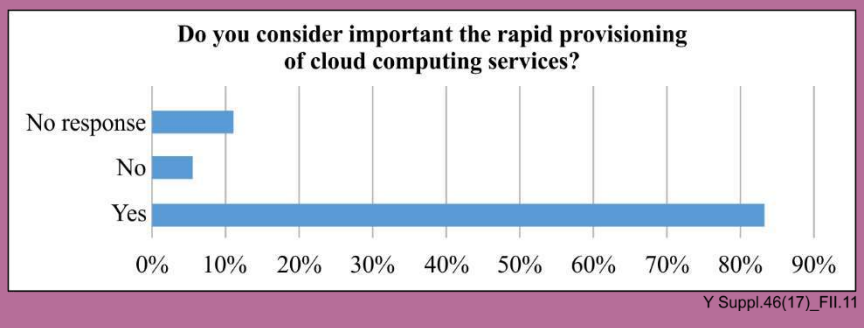


Figure II.11 – Importance of rapid cloud service provisioning

2.6 Do you consider important the dynamic provisioning of cloud computing services?

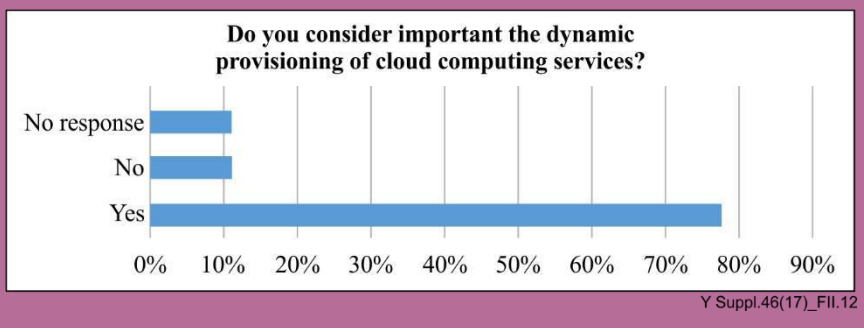


Figure II.12 – Importance of dynamic cloud service provisioning

2.7 Do you consider important data sharing through centralized consolidation at data centre level?

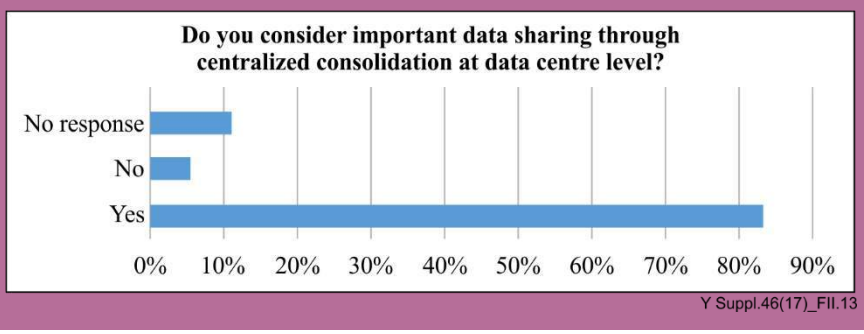


Figure II.13 – Importance of data centre sharing

2.8 In your view, what are the prevailing infrastructure needs for supporting and enabling access to cloud services?

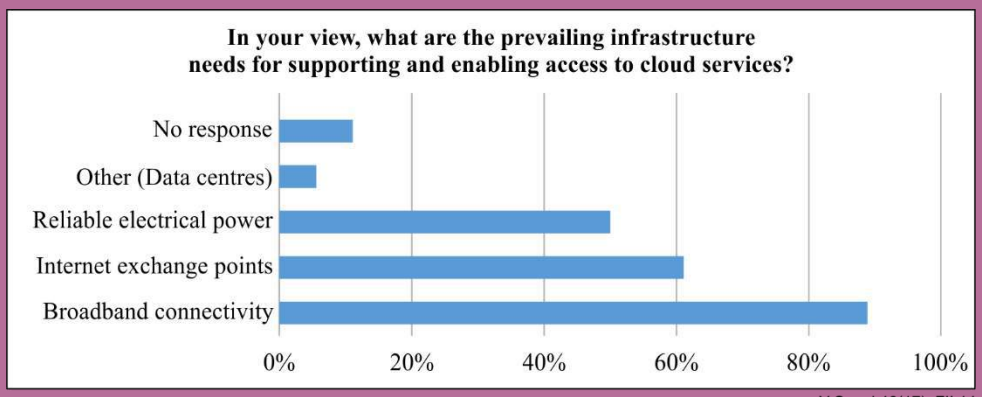


Figure II.14 – Infrastructure requirements

3 Standardization requirements

3.1 In your view, is there need for standardization of cloud computing services in your country?

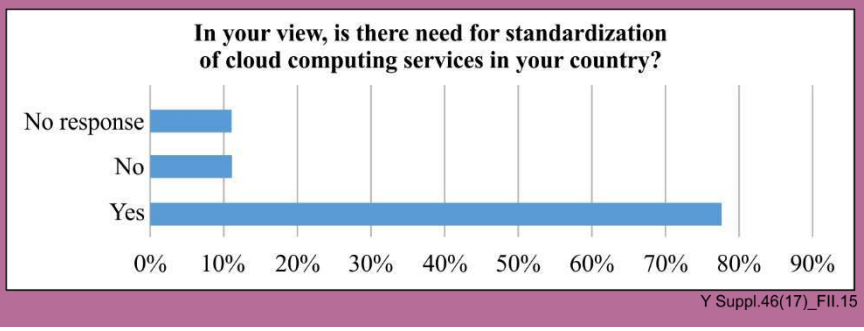


Figure II.15 – Standardization requirements

3.2 In your view, what areas of standardization do you consider important for cloud computing?

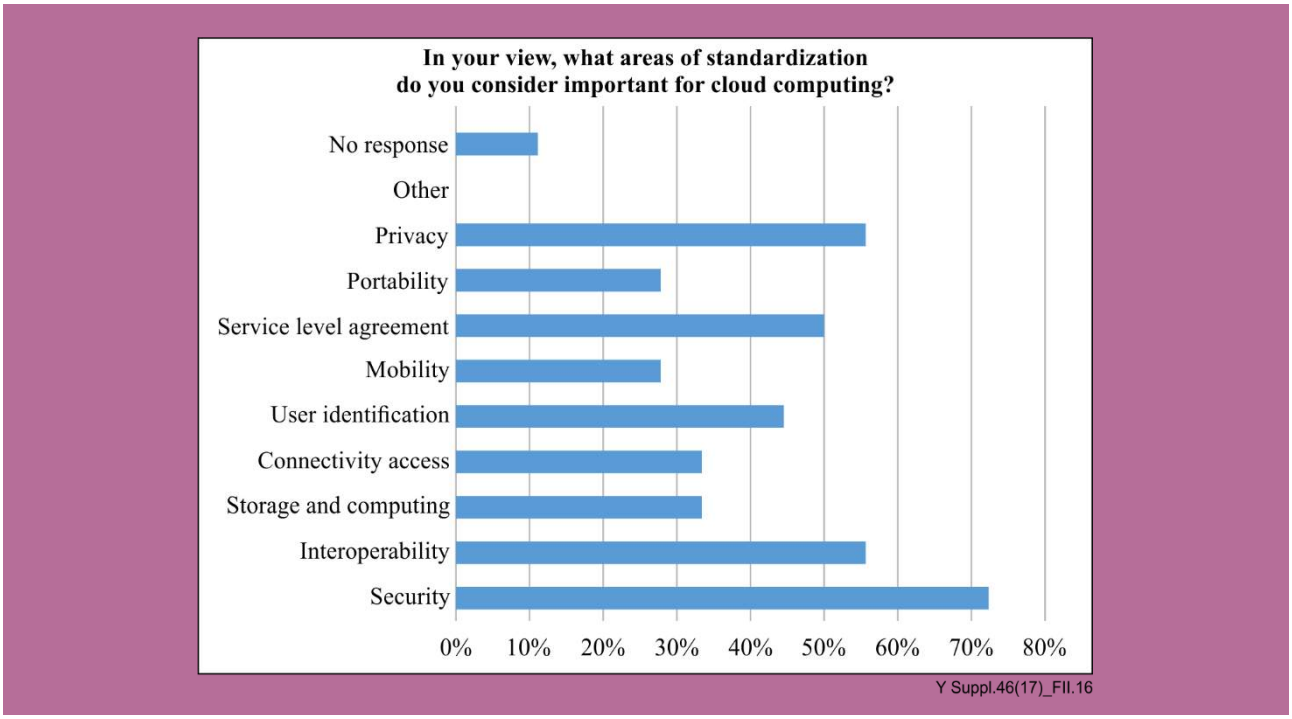


Figure II.16 – Priority areas of standardization

3.3 Do you think standardization makes the adoption of the cloud easier and more flexible?

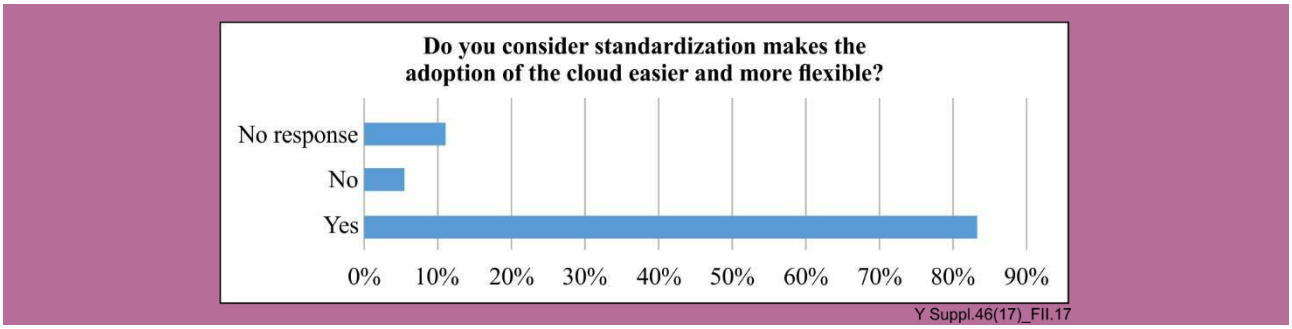


Figure II.17 – Importance of standardization to cloud services uptake

3.4 Do you consider that cloud data loss or leakage countermeasures should be carefully standardized?

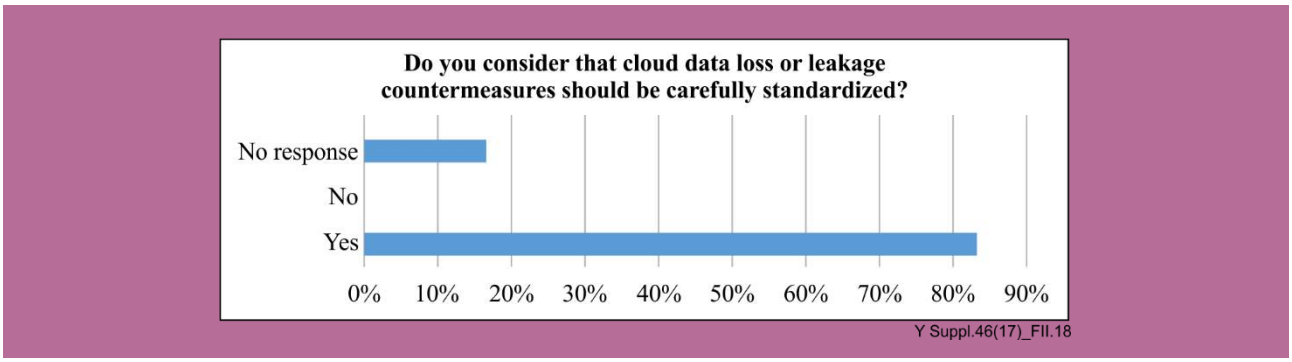


Figure II.18 – Importance of data loss standardization

3.5 Should standardization set up business continuity processes for the cloud?

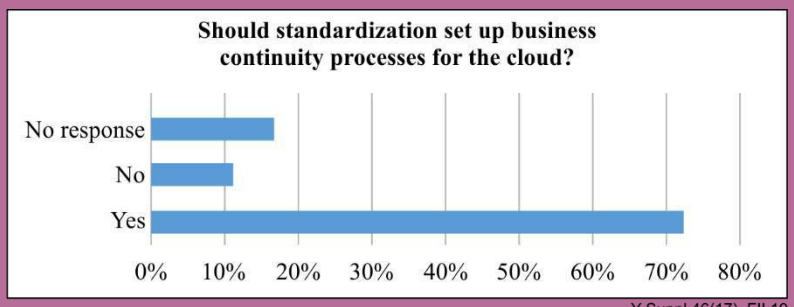


Figure II.19 – Business continuity standards

3.6 Should service level agreements be standardized?

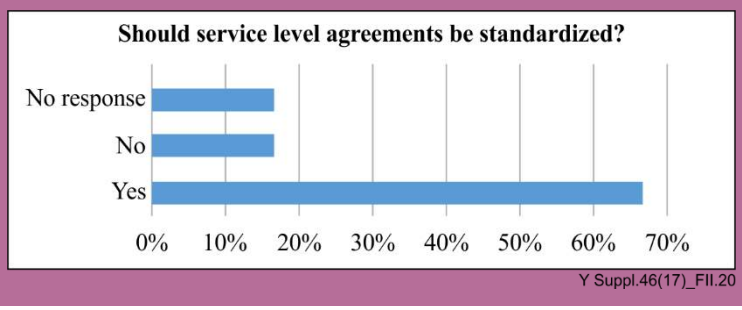


Figure II.20 – SLA standardization

3.7 If yes, what should be standardized in service level agreements?

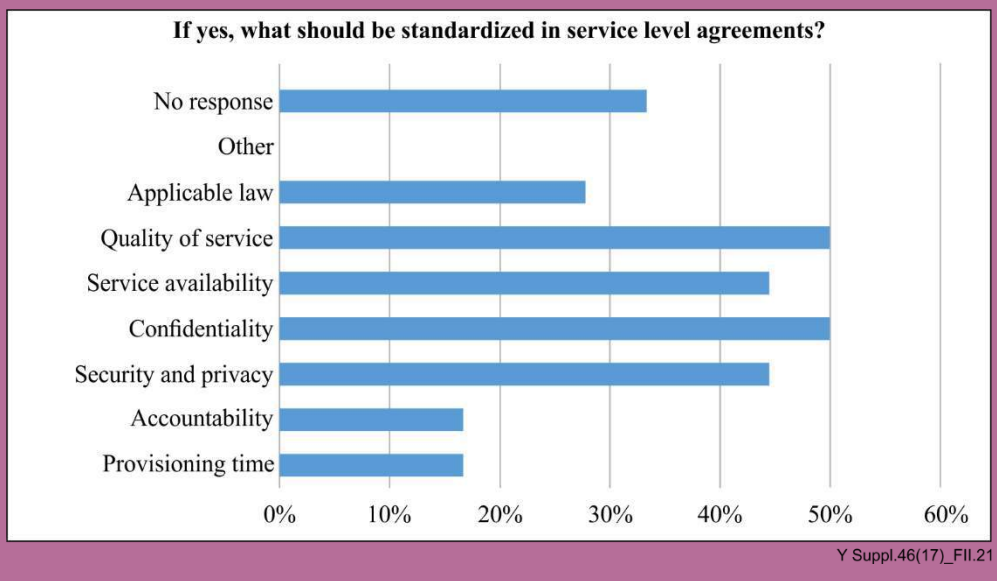


Figure II.21 – Components of SLA standardization

3.8 Should service management (like patch, incident and change) be standardized?

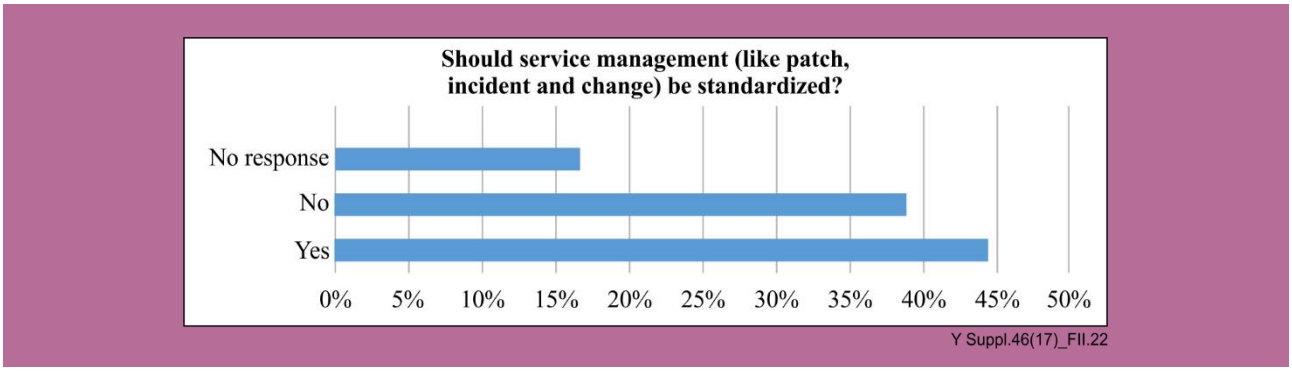


Figure II.22 – Service management standardization

3.9 Should cloud service contract management be standardized?

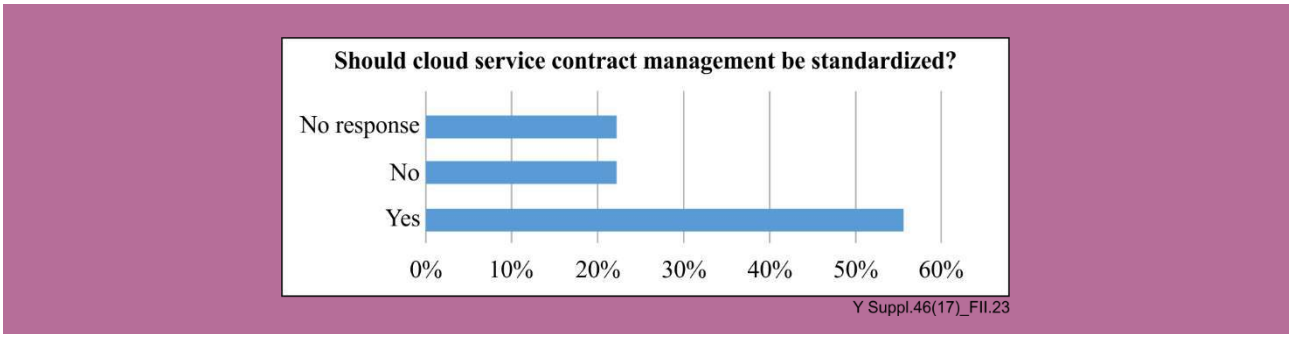


Figure II.23 – Contract management standardization

3.10 Can you identify some of the issues associated with cloud adoption that can be addressed with standards?

Received responses are the following:

- Security
- Data lost
- Storage
- Quality of service
- Internet access connectivity standardization (bandwidth speed)
- Bandwidth price models regulation and infrastructure sharing
- Interoperability
- Availability
- Data privacy and localization of data (inside or outside the country)
- SLA
- Quality and confidentiality

4 Opportunities and challenges for cloud computing deployment

4.1 What are the external barriers that you are encountering with cloud computing adoption?

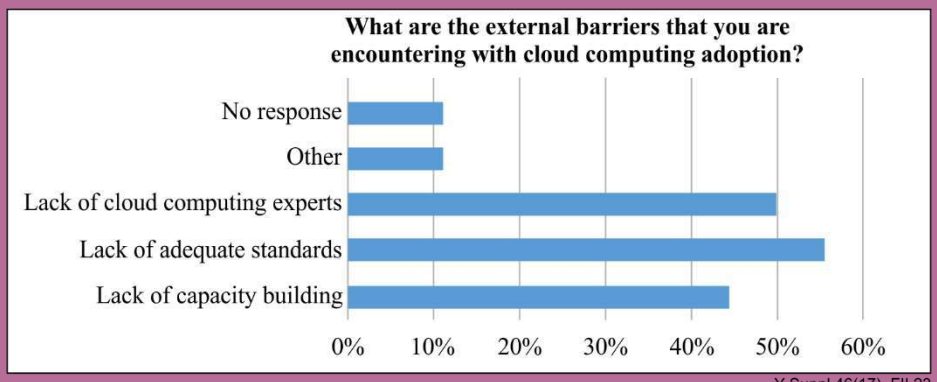


Figure II.24 – External barriers to adoption of cloud computing

The following two options were also mentioned by responders:

- the best international editor are not flexible for the adoption of their offer
- security concerns

4.2 What are the internal barriers that you are encountering with cloud computing adoption?

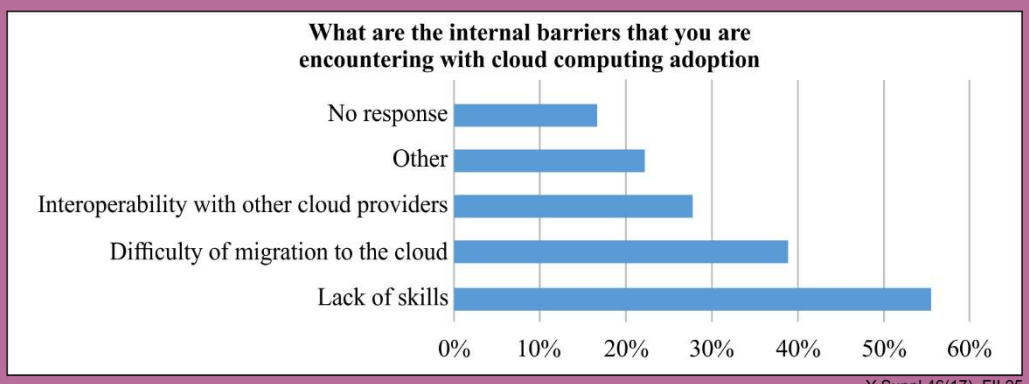


Figure II.25 – Internal barriers to adoption of cloud computing

Other options:

- Financing of infrastructure
- Lack of education in the benefits of cloud computing
- Lack of resources
- No need due to scale of operations

4.3 What do you think are bottlenecks and weakness that need to be addressed for an effective deployment of cloud services as perceived by cloud customers?

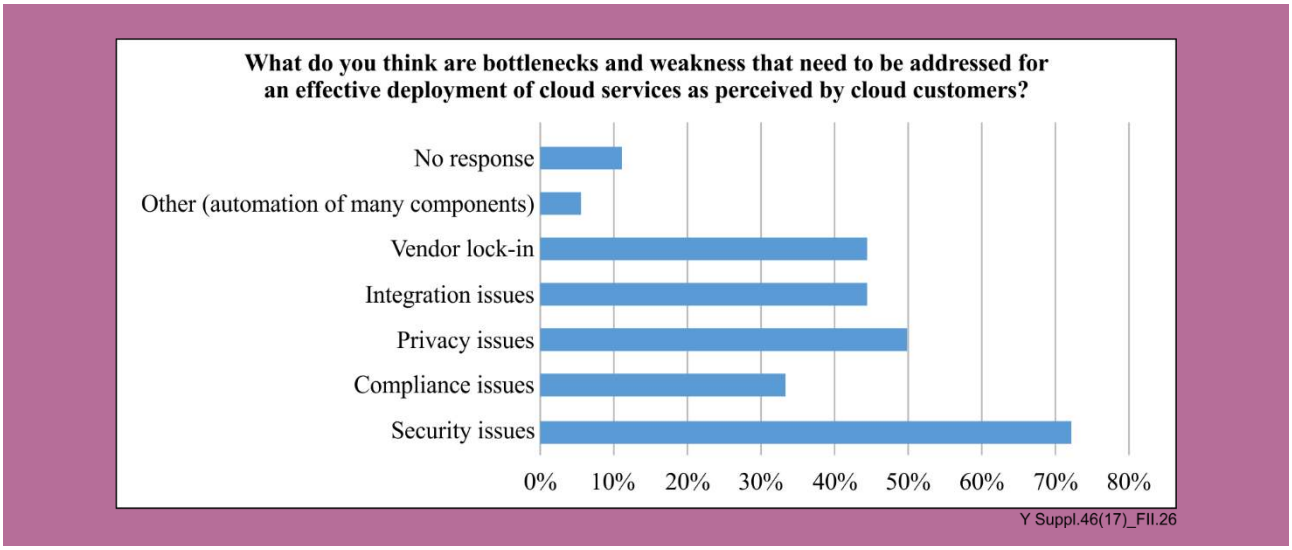


Figure II.26 – Bottlenecks to adoption of cloud computing

Automation of many components was also mentioned among bottlenecks that need to be addressed for an effective deployment of cloud services as perceived by cloud customers.

4.4 What are the scenarios that can spur the adoption of cloud services in the country and in developing countries?

Received responses are the following:

- Electricity supply, broadband connectivity, security and privacy issues
- Access to finances for CSPs, more capacity building and training for end users
- White labelled solutions
- Bandwidth cost
- Cloudification of infrastructures is not a matter of choice any more
- Government support and regulation, capacity and skilled manpower
- Providing cloud services by Telcos may increase the adoption of these services in the developing countries because Telcos are trusted parties in these countries
- Economies of scale (shared resources, cost savings, cost reduction)
- Centralised government services
- Local data centres for SME's
- Website hosting locally
- Cloud computing awareness workshops
- Developing countries are providing cloud services by telecom companies, but we do not have it by telecom company

Bibliography

[b-ITU-D Q3/1] ITU-D Q3/1 Report (2017), *Access to Cloud Computing: Challenges and opportunities for developing countries*.

[b-ITU-D report] ITU-D Report (April 2012), *Cloud Computing in Africa – Situation and Perspectives*.

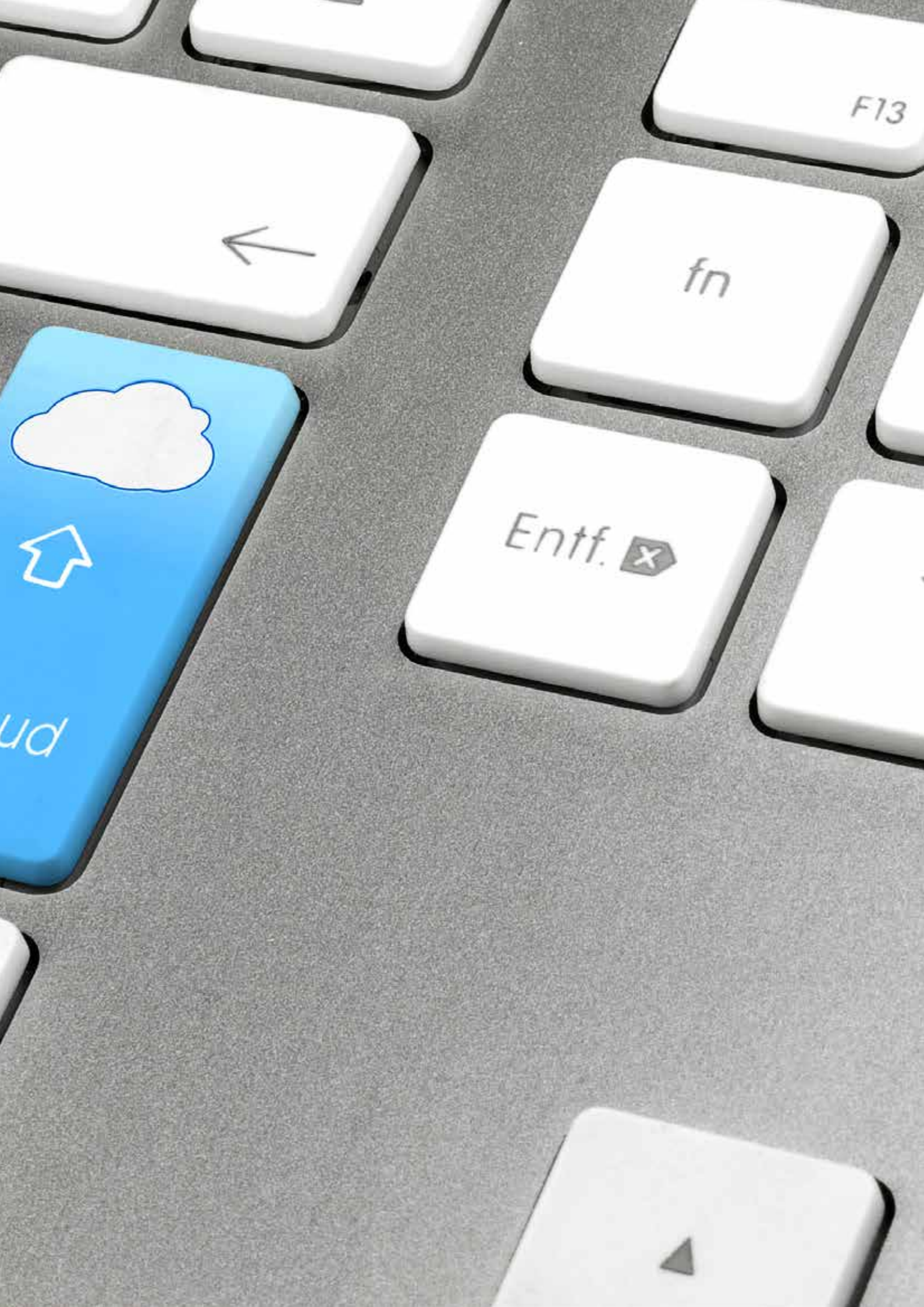
[b-ITU/UNESCO] Broadband Commission for Sustainable Development (September 2017), *The State of Broadband: Broadband catalysing Sustainable development*.

ITU Report

ITU Report (March 2012): Cloud Computing in Africa – Situation and Perspectives

http://www.itu-ilibrary.org/science-and-technology/cloud-computing-in-africa_pub/8097f580-en


connect to clo
alt


F13
fn
Entf.

International
Telecommunication
Union
Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN: 978-92-61-30401-0

9 789261 304010

Published in Switzerland
Geneva, 2019

Photo credits: Shutterstock