I

1.1 Sistemas criptográficos

A criptografia é a base de inúmeros mecanismos de segurança, por este motivo esta seção apresenta inicialmente os dois principais modelos criptografia existentes (TERADA; 2000): criptografia Convencional ou Simétrica; criptografia de chave pública ou assimétrica. Em seguida são apresentados alguns conceitos fundamentais para a utilização de serviços de criptografia: funções espalhamento; assinatura digital; certificados digitais; infra-estrutura de chaves públicas.

1.1.1 Criptografia simétrica

A criptografia simétrica, também conhecida como criptografia convencional ou criptografia de chave secreta, é muito utilizada em quase todos os tipos de criptossistemas, contando com características de robustez, em relação à segurança, e de eficiência, no que tange ao consumo de processamento computacional (TERADA, 2000) (STALLINGS, 1998).

A Figura 1 ilustra o processo de comunicação sigilosa com a utilização da criptografia simétrica, onde uma mensagem legível X é criptografada com a utilização de uma chave K, transformando-se numa mensagem ilegível Y. O texto Y é então transmitido para o destinatário que, somente se possuir a chave K, decriptografa a mensagem, obtendo novamente o texto X.

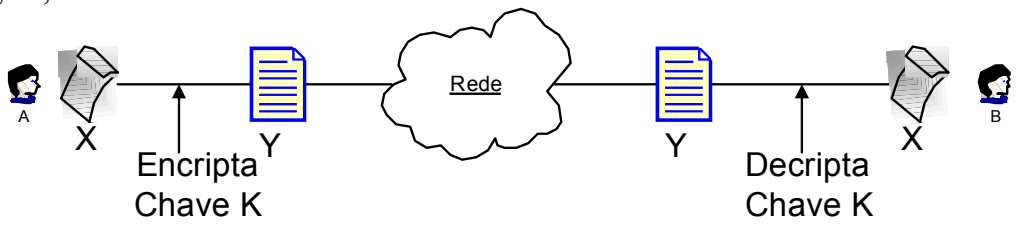


Figura 1 Privacidade com criptografia simétrica

Este modelo, quando comparado com a criptografia de chave pública, mostra-se

extremamente eficiente e leve, consumindo poucos recursos computacionais. Porém, em relação a sua operabilidade, apresenta alguns problemas, tais como:

- **Escalabilidade:** a segurança do modelo baseia-se em segredo compartilhado da chave criptográfica. Assim, é necessário que uma entidade armazene uma chave para cada parceiro de comunicação.
- **Confiabilidade da chave secreta:** caso o parceiro divulgue a chave, a confiabilidade não estará garantida.

Os diversos tipos de ataques aos algoritmos de criptografia simétrica exploram tanto as possíveis vulnerabilidades na arquitetura, quanto a utilização de chaves criptográficas pequenas mais vulneráveis a tentativas de "adivinhação". Tais ataques, cujo objetivo é a revelação do texto legível, perseguem a descoberta da chave criptográfica ou a decifração de padrões dos códigos. Entre todos os tipos de ataques, o mais comum é o de força bruta que tenta adivinhar o valor da chave por meio de sucessivas tentativas. A tabela 1 apresenta uma estimativa do tempo gasto pelo ataque de força bruta, para a descoberta da chave secreta de diferentes tamanhos:

Tabela 1 Estimativa de tempo para quebra de chave por força bruta

Tamanho da chave(bit)	Número de chaves possíveis	Tempo requerido quebra com 1 encriptação por μs	Tempo requerido para quebra com 10^6 encriptações por μs
32	$4{,}3\ 10^9$	19 horas	7,1 milisegundos
56	$7{,}2\ 10^{16}$	$5{,}3x10^4$ anos	13 dias
128	$3{,}4\ 10^{38}$	$2{,}5x10^{26}$ anos	$2{,}5\ 10^{20}$ anos

O tempo requerido para uma encriptação depende diretamente do equipamento e algoritmo utilizados. O trabalho (RICHMOND, 2000) apresenta uma estimativa onde, uma máquina Intel Pentium 4 1.5GHz utilizando o algoritmo RC5-64bits, realiza $1{,}95.10^6$ encriptações por segundos.

1.1.2 Criptografia de chave pública (assimétrica)

O surgimento da criptografia de chave pública gerou uma grande revolução na história da criptografia, mudando conceitos e mecanismos, trazendo profundas transformações para as áreas de privacidade, autenticação e distribuição de chaves. Se, até então, a criptografia baseava-se no uso de ferramentas de substituição e permutação; a criptografia de chave pública foi a pioneira em basear-se apenas em funções matemáticas (STALLINGS, 1998). Porém, a maior mudança alcançada ocorreu no âmbito de sua utilização, quando cada usuário passou a possuir um par de chaves (S, P), S privada e P pública, sendo as mesmas correlacionadas matematicamente de forma que, se x é um texto legível e S() e P() denotam a aplicação das chaves S e P para criptografia, temos:

$S(x) = y$ e $P(y) = x$ / $P(x) = z$ e $S(z) = x$, ou seja, o que uma chave criptografa, somente sua parceira decriptografa.
Nesse sistema, cada usuário possui seu par de chaves (S,P), sendo S armazenada secretamente e P distribuída publicamente, o que facilita o processo de distribuição de chaves e permite as seguintes funcionalidades :

1. Enviar mensagens de forma sigilosa;
2. Com o auxílio de funções espalhamento, evitar que mensagens sejam furtivamente modificadas;
3. Evitar que uma entidade envie mensagens utilizando outra identidade.

A Figura 2 ilustra um exemplo de dois parceiros (A e B) utilizando-se da criptografia de chave pública. Quando "A" deseja enviar uma mensagem sigilosa para "B", encripta a mensagem com a chave pública de B (P_B). Como somente "B" possui sua chave privada S_B , só ele poderá decriptografar e entender a mensagem. Outro caso "A" deseja enviar uma mensagem para "B" com garantias de autoria e integridade. A entidade "A" criptografa a mensagem X com sua chave privada S_A; nesse caso, tanto "B" como qualquer entidade podem possuir a chave pública de "A" (Pa) e assim decriptografar a mensagem. Porém, como somente "A" conhece S_A, garante-se que "A" é a única entidade capaz de produzir ou modificar a mensagem.

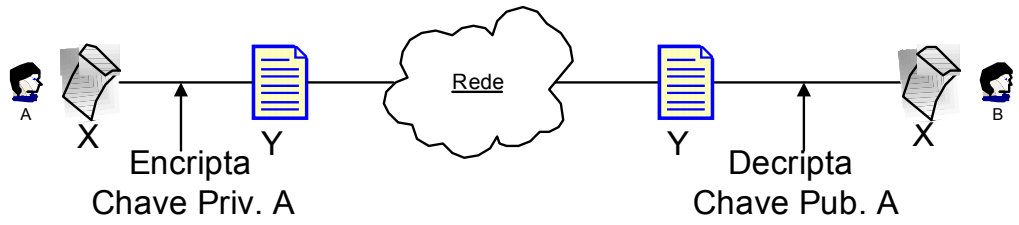


Figura 2 Privacidade e autenticação com criptografia de chave pública

Com tudo isso, os sistemas de criptografia de chave pública possibilitam funções de privacidade e autenticidade e não apresentam problemas como os atribuídos à criptografia convencional, de distribuição de chaves e/ou manutenção de segredos entre entidades. O armazenamento e o uso seguro da chave privada é o requisito básico para a correta utilização desse tipo de sistema. Porém, a criptografia de chave pública consome até mil vezes mais recursos computacionais do que a simétrica (HARBITTER; MENASCÉ, 2001), assim seu uso não é recomendado para todos os processos de comunicação.
Na prática, a criptografia de chave pública é utilizada para autenticação, assinatura de documentos digitais e troca de chaves simétricas, cabendo à criptografia simétrica as funcionalidades de privacidade.

1.1.3 Análise Comparativa entre Criptografia Convencional e de Chave Pública

A criptografia assimétrica surge aprimorando uma série de deficiências da criptografia convencional, principalmente nas áreas de assinatura digital e distribuição de chaves. Porém, em relação ao desempenho deixa muito a desejar, sendo até 1000 vezes mais ineficiente e em relação à segurança, apesar de apresentarem tamanhos de chaves com grandezas distintas, não existe nenhum estudo que identifique um tipo de algoritmo mais robusto que outro (HARBITTER; MENASCÉ, 2001). A tabela 2 apresenta uma comparação entre criptografia convencional e de chave pública.

Tabela 2 Tabela Comparativa entre os Modelos de Criptografia Convencional e de chave pública (STALLINGS, 1998).

	Criptografia Convencional	**Criptografia de Chave Pública**
Desempenho	Rápida	Lenta
Número de Chaves	1	2
Distribuição de Chaves	Complexa	Simples
Administração de Chaves	Complexa	Simples
Tamanho de Chave	56 – 256 bits	512 - 2048 bits
Quantidade de Algoritmos Disponíveis	Muitos	Poucos

Em suma, os dois modelos apresentam vantagens de uso. Com efeito, a existência de diferentes tipos de criptografia permite a indicação adequada para situações distintas, sendo o caso mais comum a utilização da criptografia assimétrica para autenticação, troca de chaves e assinatura digital e a simétrica para autenticação e privacidade.

1.1.4 Funções espalhamento, Assinatura digital e Certificados Digitais

Em decorrência da evolução das aplicações sobre redes computacionais, surgiu a necessidade de se criar mecanismos que, por meio de provas irrefutáveis, oferecem garantias sobre a autoria de documentos digitais que, análogo ao conceito de assinatura de documentos em papéis, permitissem a comprovação dos seguintes quesitos:

1. Verificar a autoria, a data e a hora da assinatura;
2. Comprovar a existência de mudanças na mensagem, a partir do momento da assinatura;
3. Possibilitar que uma entidade terceira possa verificar a mensagem e assinatura em caso de disputas.

A criptografia de chave pública atende a todos esses requisitos. Uma mensagem criptografada com a chave privada de uma determinada entidade pode ser decriptografada e entendida publicamente, por meio de sua chave de conhecimento público. Porém, só pode ser gerada pela própria entidade (única conhecedora da chave privada) e qualquer alteração posterior à criptografia acarretará em deformações na mensagem decriptografada. Portanto, a criptografia de chave pública é amplamente utilizada para a geração de assinaturas digitais.

Entretanto, devido ao excessivo consumo de recursos computacionais para processar mensagens longas com criptografia assimétrica, os modelos para assinaturas digitais utilizam-se também de funções de espalhamento. Estas recebem como parâmetro, documentos de tamanho variável e retornam blocos de bits com tamanho fixo, denominados MACs (*Message Authentication Code* - código identificador de mensagem). É certo que diferentes entradas podem gerar MACs iguais, porém, em uma boa função espalhamento a probabilidade de que isso ocorra é tão baixa que, na prática o código MAC é utilizado como identificador da mensagem que o gerou.

Como os códigos MAC são geralmente bem menores que as mensagens que os geraram, sua utilização como identificador de documentos acarreta uma economia de representação. No caso específico de assinaturas digitais, a criptografia assimétrica é aplicada somente no código MAC ao invés de toda mensagem, o que gera uma economia de recursos computacionais.

A

Figura 3 ilustra o processo de assinatura digital de uma mensagem M pela entidade A, onde se adiciona à mensagem original seu código MAC gerada pela função espalhamento $F_e()$ e criptografado $S_a()$ com a chave privada de A (S_a).

No processo de verificação da assinatura da mensagem, também ilustrado pela **Figura 3** , compara-se o código MAC obtido por meio da função espalhamento $F_e()$, com o obtido por meio da decriptografia $P_a()$ da assinatura coma chave pública de A (P_a).

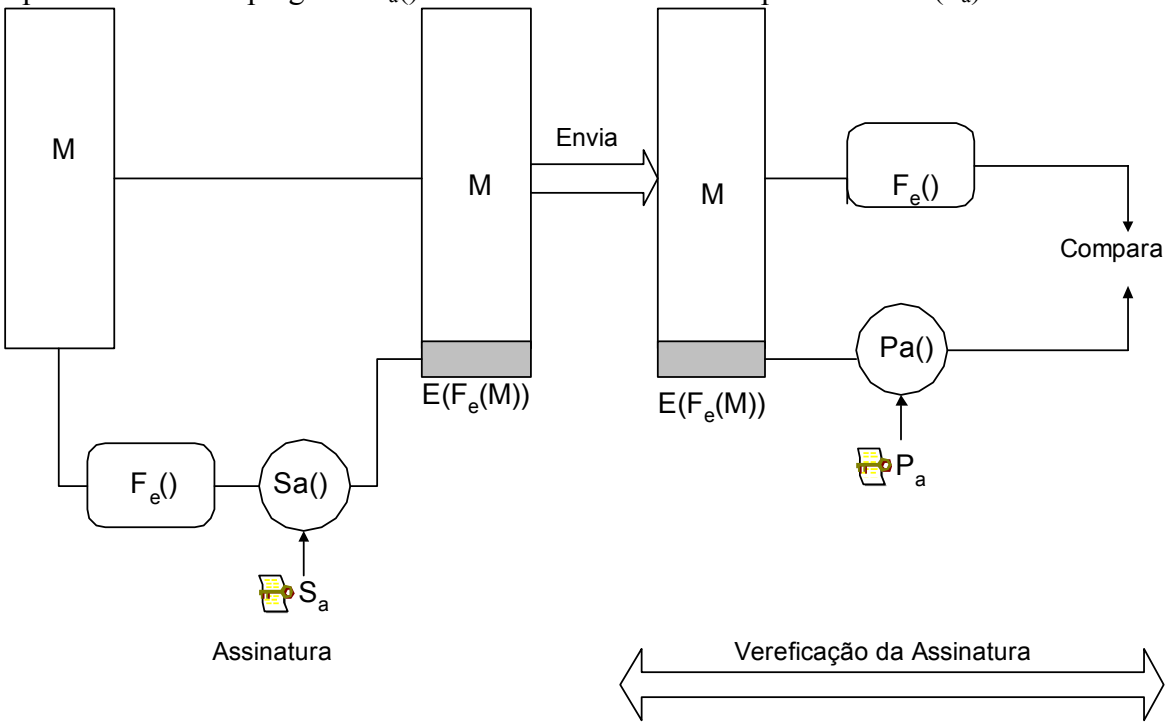


Figura 3 Processo de Assinatura digital.

1.1.5 Infra-estrutura de Chaves públicas (ICP)

Para a utilização coerente dos serviços de criptografia de chave pública, deve-se relacionar de forma precisa, chaves públicas como pertencentes às entidades parceiras de comunicação (STEVE; CARLISLE, 2002). A assinatura digital de um documento serve para ilustrar tal necessidade, onde, por meio da chave pública correspondente se obtém a garantia sobre o uso de uma determinada chave privada para gerar tal assinatura, porém para determinar de forma segura a identidade do assinante é necessário relacionar a chave pública ou privada como pertencente a tal entidade. A ICP fornece uma base para que relações de confiança possam ser estabelecidas, fornecendo uma forte ligação entre uma entidade e seu par de chaves criptográficas.

Uma ICP consiste em políticas e procedimentos que oferecem base para a utilização de serviços de criptografia de chave pública, o que incluem: como as chaves devem ser controladas; como os usuários têm suas identidades verificadas, como uma chave pública de usuário é disponível para outros usuários. Para melhor compreender o funcionamento de uma ICP, se faz necessário descrever os seguintes componentes presentes na mesma:

Certificados digitais: o certificado digital é a base para se possa relacionar de forma segura entidades com suas respectivas chave públicas, consiste em um documento contendo sua data de validade, dados de uma entidade como identidade e chave pública. Para atribuir credibilidade os certificados são assinados pala Autoridade Certificadora;

Política de segurança: a política da segurança contém as regras operacionais de uma ICP, regulamentando as operações de todos os componentes assim como procedimentos adotados para a geração, a emissão, o armazenamento, e a revogação chaves;

Autoridade Certificadora (AC): a AC é uma entidade que possui sua chave publica conhecida e confiada por um domínio de usuários para emitir certificados digitais. Uma AC pode autorizar outras ACs a produzir certificados válidos em seu domínio, criando assim uma rede hierárquica de confiança, onde a AC no topo da hierarquia é chamada de AC raiz;

Autoridade do Registradora (AR): Para que a partir de uma requisição, a AC possa emitir certificados digitais para uma entidade de forma coerente, deve verificar corretamente a identidade do requerente, a AR tem como papel realizar tal verificação, onde o grau de rigor aplicado pela AR durante esse processo afeta no grau de confiança do certificado digital;

Lista de Certificados Revogados (LCR): Quando o proprietário de um certificado digital tem sua chave privada comprometida ou é excluído de seu domínio, seu certificado é revogado. Assim para que possa verificar a validade de um certificado se faz saber se o mesmo não foi revogado. A LCR é um documento assinado pela AC e publicado periodicamente que, informando os certificados revogados de um domínio;

Repositório de Certificados (RC): A RC tem o objetivo de disponibilizar certificados e LCR de um domínio.

A

Figura 4 de mostra como numa ICP uma entidade “A” obtém a chave pública de “B” de forma segura, este processo ocorre conforme os seguintes passos:

1. A recebe de “B” seu certificado(CerB);
2. “A” confere a assinatura a da AC, a data de validade do certificado e verifica na LCR recebida de RC se o certificado foi revogado;

3. Caso essas etapas sejam cumpridas com sucesso, “A” assume a chave publica do certificado como pertencente a “B”.

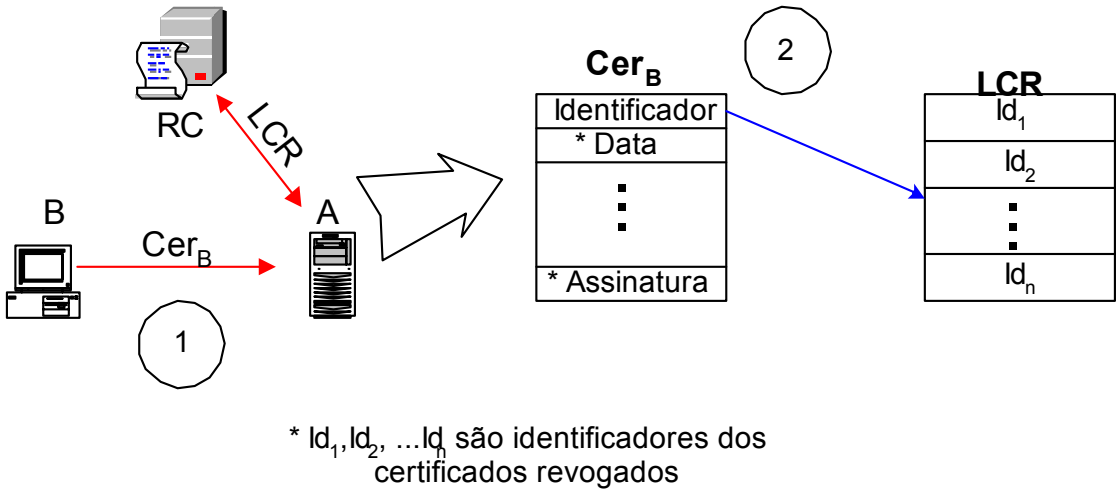


Figura 4 Processo para obter chave pública de um parceiro numa ICP

1.2 Mecanismos de Autenticação baseados em criptografia

Uma vez que os sistemas computacionais distribuídos passaram a fornecer serviços a diversos usuários, surgiu a necessidade de se utilizar mecanismos que os identificassem. Nos sistemas tradicionais, o processo de autenticação consiste no fornecimento de uma senha secreta, no início de uma seção. Entretanto, senhas transmitidas pela rede podem ser interceptadas e, posteriormente, usadas por um atacante para reivindicar falsa identidade.Já os protocolos de autenticação, baseados em criptografia, são considerados mais seguros por protegerem o conteúdo das senhas quando trafegam pela rede. A seguir, se tem uma analise de dois protocolos de autenticação: Kerberos e o diretório de autenticação x.509

1.2.1 Kerberos

O Kerberos (KEBEROS) (NEUMAN; THEODORE, 1994) é um serviço distribuído de autenticação que, por meio do uso de série de mensagens criptografadas, possibilita aos usuários provarem sua identidade a um verificador, sem transmitir pela rede dados confidenciais que possibilitem a atacantes ou verificadores reivindicarem a identidade do usuário.

A metodologia Kerberos conta com uma central de autenticação responsável em emitir bilhetes criptografados para os usuários obterem acesso. No processo de criptografia, o usuário comprova sua identidade quando se mostra capaz de ler bilhetes a

ele endereçados, pois as chaves secretas utilizadas para criptografia são derivadas das senhas dos usuários.
As mensagens 1, 2, 3 e 4 na Figura 5 mostram o pedido da aplicação e a resposta, quando determinada entidade Cliente (C) deseja comunicar-se com o Servidor (s), por meio do Servidor de Autenticação (SA) . É nesse processo que um cliente e o verificador autenticam-se mutuamente, ao provarem que conhecem a chave da sessão encapsulada no bilhete do Kerberos. Os seguintes campos são presentes nas mensagens da figura 7:

- id_C - identificador do cliente;
- id_s - identificador do servidor;
- K_C - Chave secreta entre SA e C (derivada da senha);
- K_C - Chave secreta entre SA e S (derivada da senha);
- K_{Cs} - Chave de sessão gerada por AS para a troca de chave entre as entidades C e V.
- K_{sub} - Chave de sessão gerada por C para o estabelecimento de um canal seguro com V;
- T - tempo de emissão do bilhete, utilizado para limitar a validade do bilhete por um período;
- N - número randômico gerado pelo usuário, utilizado para evitar ataques em que uma outra entidade tente se passar pela AS distribuindo bilhetes capturados na rede .

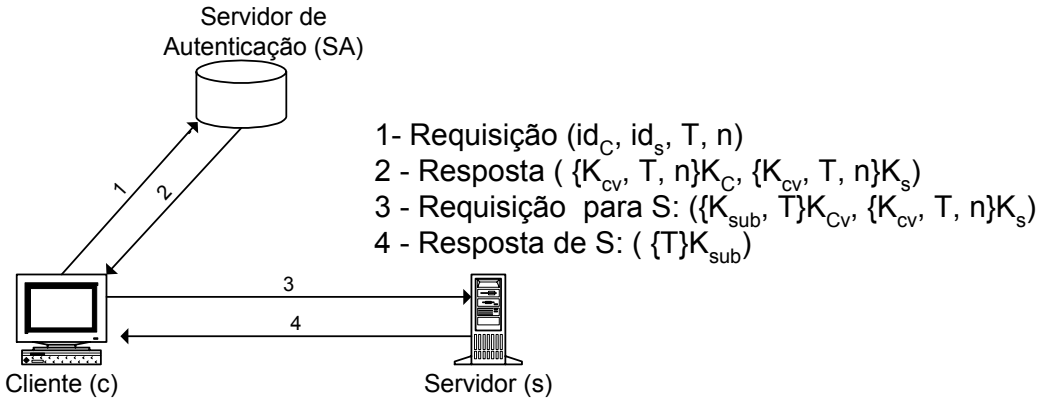


Figura 5 Protocolo básico de autenticação Kerberos

Por utilizar-se de criptografia simétrica, o Kerberos tem como pontos fortes a robustez e a eficiência. Entre suas limitações podemos citar a escalabilidade, já que a central de autenticação deve armazenar e gerenciar chaves de todos os usuários do domínio. Outro problema se dá em relação à segurança, pois o usuário divide o segredo de sua senha secreta com a central de autenticação, que pode assim realizar operações na rede em nome de seus usuários.

1.2.2 Variantes de chaves públicas do Kerberos

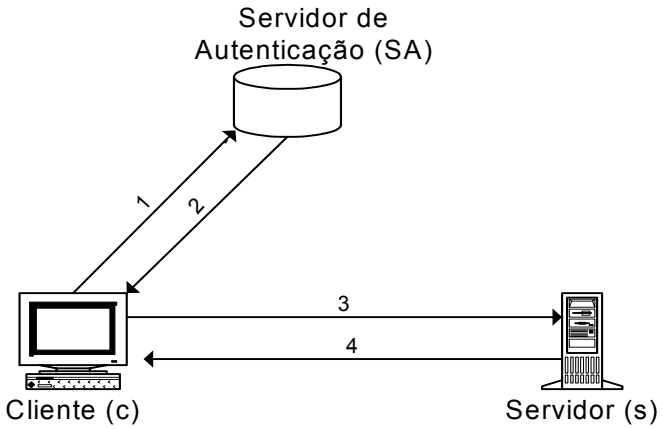
Conforme descrevemos acima, o serviço de autenticação Kerberos oferece os benefícios de robustez e eficiência, porém, apresenta limitações relacionadas a escalabilidade e à

vulnerabilidade do compartilhamento de segredo entre clientes e a central de autenticação. As duas variantes do Kerberos PKINIT (TUNG *et al*, 2001) e PKAPP (MEDVINSKY *et al*, 1999) apresentadas abaixo apontam como solução para essas limitações a utilização de criptografia de chave pública.

1.2.2.1 PKINIT

O PKINIT (*Public Key Cryptography for Initial Authentication in Kerberos* - Criptografia de chave pública para autenticação inicial do Kerberos) é uma proposta de utilização de criptografia de chave pública e certificados digitais no processo inicial de autenticação na central de autenticação do Kerberos, sendo os demais processos de requisição de bilhetes e estabelecimento de conexão com os servidores, similares ao Kerberos tradicional. A Figura 6 demonstra o processo de autenticação PKIINT, que ocorre por meio dos seguintes passos:

- ✓ 1, o usuário emite uma requisição para conexão mensagem igual ao padrão tradicional Figura 5, exceto que como o usuário deve usar criptografia de chave pública. Nessa etapa envia também seu certificado Cerc e assina a requisição Sc;
- ✓ 2, a central de autenticação verifica o certificado emite um bilhete concedendo igual ao tradicional, a não ser que, para a criptografia, ao invés das chaves compartilhadas K_c e K_k da Figura 5, passa a utilizar as chaves públicas das entidades C e K (K_{pc} e K_{pk}), além de anexar a assinatura da mensagem S_{as}*;*
- ✓ *3 e 4* os outros passos são iguais aos descritos acima para o Kerberos tradicional.



1- Requisição (id_C, id_s, T, n, Cer_c)
2 - Resposta ($\{K_{cv}, T, n\}K_{pc}$, $\{K_{cv}, T, n\}K_{ps}$, S_{as})
3 - Requisição para S: ($\{K_{sub}, T\}K_{Cv}$, $\{K_{cv}, T, n\}K_{ps}$)
4 - Resposta de S: ($\{T\}K_{sub}$)

Figura 6 Processo de autenticação no KDC segundo PKINIT

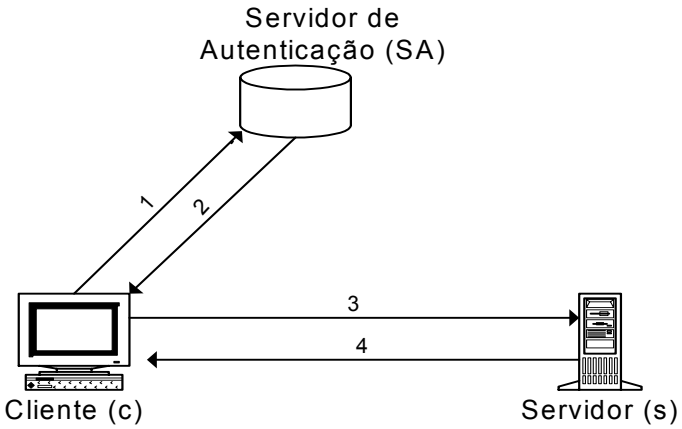
Em relação ao kerberos tradicional, o grande avanço da especificação PKINIT é permitir a autenticação inicial por criptografia assimétrica, dispensando a necessidade do compartilhamento de chaves privadas para a autenticação entre usuários e central de autenticação. Porém, o problema relacionado às questões de escalabilidade da central de autenticação, que necessita armazenar chaves de sessão para todas as entidades autenticadas, permanece sem resolução. Em relação a seu desempenho, outro ponto importante a ser ressaltado diz respeito ao acréscimo de processamento devido às operações de criptografia assimétrica. Tal acréscimo não é significativo quando se utiliza PCs comuns; porém, o uso de máquinas de baixo poder computacional como Palms, PocketPC e celulares podem inviabilizar o modelo (HARBITTER; MENASCÉ, 2001).

1.2.2.2 PKTAPP

No kerberos todos os bilhetes de acesso são emitidos e assegurados pelo KDC. Assim, todas as operações de autenticação da rede passam pela KDC, tornando-o um gargalo de performance.

O PKTAPP (*Public Key Tickets for Aplications Server* – Bilhetes de chave publica para servidores de aplicação) tem por objetivo aumentar a privacidade dos clientes Kerberos e a escalabilidade de sua plataforma por meio da utilização de criptografia de chave pública. Um nível maior de segurança é alcançado uma vez que os clientes não mais dividem o conhecimento da chave secreta com o SA e a escalabilidade do SA aumenta por não mais intermediar todos os processos de autenticação, que passam a ser realizados diretamente entre usuários e servidores. A Figura 7 demonstra o processo de autenticação PKTAPP, que ocorre por meio dos seguintes passos, informando sua identidade id_c:

1. O usuário requisita a chave pública do servidor;
2. O servidor responde com seu certificado $Cerc_c$;
3. O cliente requisita um bilhete de sessão para acessar o servidor. Essa mensagem é assinada pela chave privada do cliente S_c e criptografada pela chave pública do servidor K_{ps};
4. Da mesma forma que no tradicional Figura 5 , o servidor retorna o bilhete de serviço, criptografado com a chave de seção K_{sub}.



1. **Requisição para SA: id_C**
2. **Resposta de SA: $Cerc_c$**
3. **Requisição para S: $\{T, K_{sub}\}K_{ps}$, S_c**
4. **Resposta de S: $\{T\}K_{sub}$**

Figura 7 Processo de autenticação no KDC segundo PKAPP

Apesar de solucionar os problemas de privacidade e escalabilidade do KDC, o PKTAPP criou outros: a utilização de criptografia assimétrica em todos os processos de autenticação pode comprometer o desempenho das máquinas clientes e servidoras (HARBITTER; MENASCÉ, 2001).

1.2.3 Diretório x.509 Servidor de autenticação

O padrão X.509 (OPPLIGER, 1996) é integrante do padrão de serviços de diretório x.500 e define uma plataforma para serviços de autenticação baseados em certificados digitais. O servidor de diretório funciona como repositório de certificados digitais com informações de usuários, como sua chave pública, nome, data de validade e outros.

O servidor de autenticação x.509 permite processos de autenticação em uma e duas vias. Abaixo, segue uma breve descrição de cada uma, onde se admite que todas as entidades possuem as chaves públicas das demais envolvidas, ou as buscam previamente no repositório de certificados.

- ✓ **Autenticação simples**

O processo de autenticação consiste no envio de uma mensagem da entidade A para outra B, onde se certifica das seguintes premissas:

1. A identidade de A e a autoria da mensagem por A.
2. A mensagem é destinada para B.
3. A mensagem está íntegra.

A mensagem deve conter hora de criação(t_a), um desafio(r_a) e a identidade de B(I_B), sendo criptografada com a chave pública A. A hora de criação e o desafio são utilizados para impedir ataques em que o atacante capture a mensagem e a utilize na

tentativa de autenticar-se passando-se pela entidade A. Processo representado pala Figura 8, onde S_a, P_a, S_b e P_b correspondem respectivamente as chaves privadas e públicas de A e B, já ES_a representa o processo de criptografia utilizando S_a.

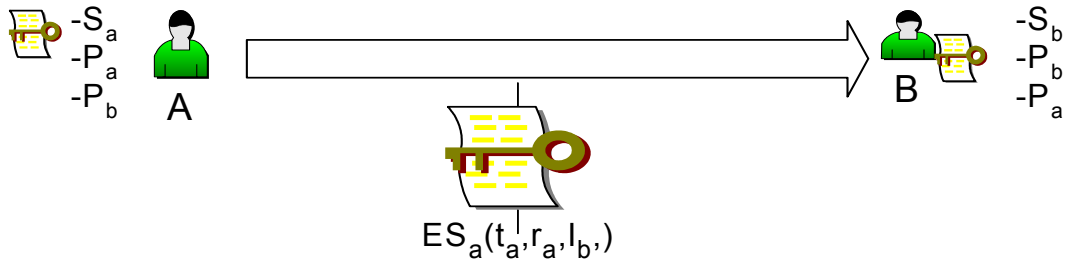


Figura 8 Processo de autenticação em uma via.

- ✓ **Dupla autenticação**

O processo de autenticação em duas vias, além da mensagem descrita acima, a entidade B envia uma resposta para A, com as seguintes garantias:

4. Identidade de B no envio da resposta.
5. A mensagem é destinada para A.
6. A mensagem está íntegra em relação à origem da resposta

Nesse modelo, ambas as entidades são autenticadas, de acordo com a Figura 9.

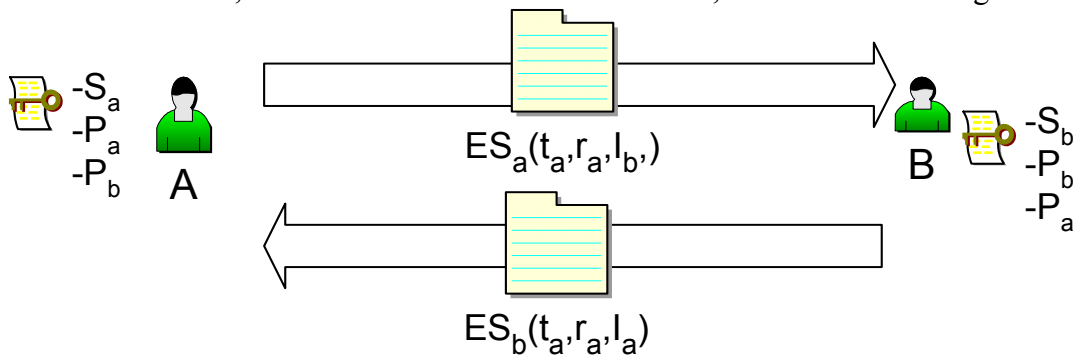


Figura 9 Processo de autenticação em duas vias.