FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

4SEG – SEGURANÇA DE REDES
AULA 5

Assinatura e Certificado Digital

Profa. Maria Cláudia Roenick Guimarães
E-mail: maria.roenick@faeterj-rio.edu.br

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Contextualização

- Na aula anterior falamos de alguns princípios importantes sobre Criptografia: tipos de aplicação, modelo clássico e moderno, tipos chaves de criptografia, entre outras questões;

- Nessa aula, vamos abordar alguns tipos de soluções de mercado para implementar integridade de dados, assinatura e certificado digital (autenticidade);

- O conteúdo dessa aula foi retirado dos Capítulos 11, 12, 13 e 14 do Livro "Criptografia e Segurança de Redes – 6ª Edição – STALLING, W." e de sites sobre o assunto (disponíveis no Google Classroom).

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Funções de HASH

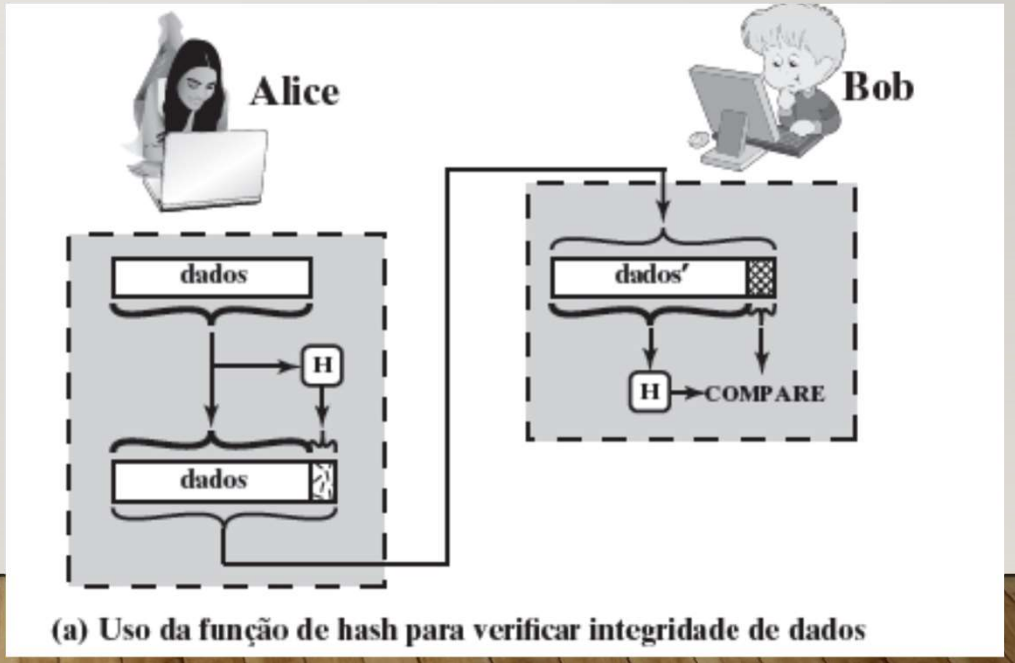
- Uma função de hash aceita uma mensagem de tamanho variável M como entrada e produz um valor de hash de tamanho fixo h = H(M);
- Uma "boa" função de hash tem a propriedade de que os resultados da aplicação da função a um grande conjunto de entradas produzirá saídas que são distribuídas por igual e aparentemente de modo aleatório. Em termos gerais, o objeto principal de uma função de hash é a integridade de dados. Uma mudança em qualquer bit ou bits em M resulta, com alta probabilidade, em uma mudança no código de hash;
- O tipo de função de hash necessária para aplicações de segurança é conhecido como função de hash criptográfica. Ela é um algoritmo para o qual é computacionalmente inviável (pois nenhum ataque é de maneira significativa mais eficiente do que a força bruta) descobrir ou (a) um objeto de dados que seja mapeado para um resultado de hash pré-especificado (a propriedade de mão única) ou (b) dois objetos de dados que sejam mapeados para o mesmo resultado de hash (a propriedade livre de colisão).

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Funções de HASH

- Para entender melhor alguns dos requisitos e implicações de segurança para as funções de hash criptográficas, é útil examinar a faixa de aplicações em que elas são empregadas:
  - Autenticação de mensagem é um mecanismo ou serviço usado para verificar a integridade de uma mensagem. Ela garante que os dados recebidos estão exatamente como foram enviados (ou seja, não contêm modificação, inserção, exclusão ou repetição).

A função de hash precisa ser transmitida de forma segura. Ou seja, precisa ser protegida de modo que, se um adversário alterar ou substituir a mensagem, não será viável para ele alterar também o valor de hash para enganar o receptor.



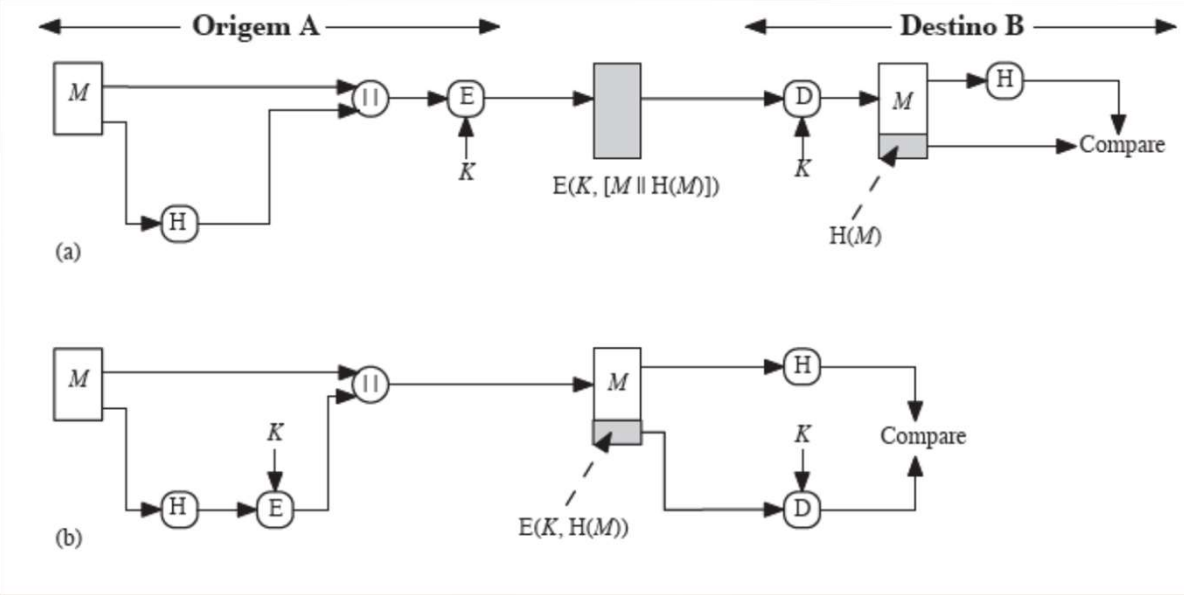
(a) Uso da função de hash para verificar integridade de dados

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Funções de HASH

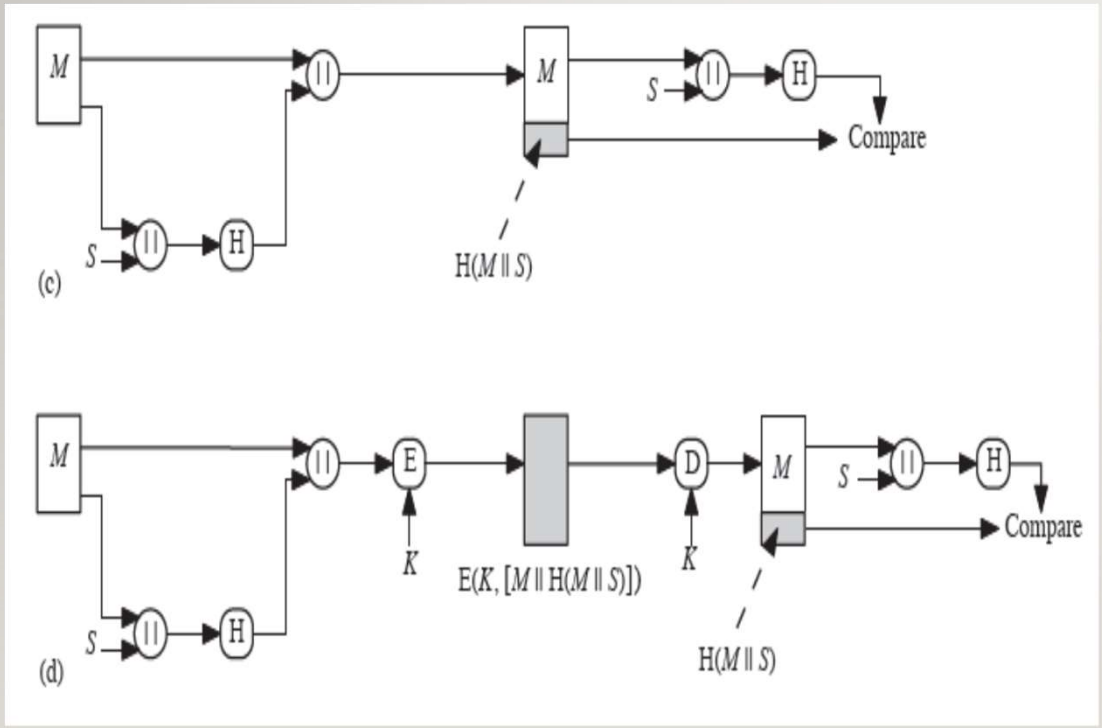
a. A mensagem mais o código de hash concatenado são encriptados usando a encriptação simétrica. Como somente A e B compartilham a chave secreta, a mensagem deverá ter vindo de A e sem alteração. O código de hash oferece a estrutura ou redundância exigida para conseguir a autenticação. Como a encriptação é aplicada à mensagem inteira mais o código de hash, a confidencialidade também é fornecida.

b. Somente o código de hash é encriptado, usando a encriptação simétrica. Isso reduz o peso do processamento para as aplicações que não exigem confidencialidade.



FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Funções de HASH



c. É possível usar uma função de hash, mas não a encriptação para autenticação de mensagem. A técnica considera que as duas partes se comunicando compartilham um valor secreto comum, S. A calcula o valor de hash sobre a concatenação de M e S, e anexa o valor de hash resultante a M. Como B possui S, ele pode recalcular o valor de hash para verificar. Como o valor secreto em si não é enviado, um oponente não pode modificar uma mensagem interceptada e não pode gerar uma mensagem falsa.

d. A confidencialidade pode ser acrescentada à abordagem do método (c) encriptando a mensagem inteira mais o código de hash.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Funções de HASH

- Normalmente, a autenticação de mensagem e alcançada usando um código de autenticação de mensagem (MAC, do acrônimo em inglês para *message authentication code*), também conhecido como função de hash chaveada. Normalmente, MACs são usados entre duas partes que compartilham uma chave secreta para autenticar informações trocadas entre elas.
- Uma função MAC toma como entrada uma chave secreta e um bloco de dados e produz um valor de hash, conhecido como MAC, que e associado a mensagem protegida. Se a integridade da mensagem tiver que ser verificada, a função MAC pode ser aplicada a mensagem e o resultado comparado com o valor MAC associado.
- Um invasor que altera a mensagem não poderá alterar o valor MAC associado sem conhecer a chave secreta. Observe que a parte que esta verificando também sabe quem é a parte emissora, pois ninguém mais conhece a chave secreta.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Funções de HASH

- Outra aplicação importante, similar à aplicação de autenticação de mensagem, é a Assinatura Digital. A operação da assinatura digital é similar à do MAC. No caso da assinatura digital, o valor de hash da mensagem é encriptado com a chave privada do usuário. Qualquer um que conhecer a chave pública do usuário pode verificar a integridade da mensagem que está associada à assinatura digital. Nesse caso, um invasor que quisesse alterar a mensagem precisaria conhecer a chave privada do usuário.

  - Se, além da assinatura digital, o que se procura é confidencialidade, então a mensagem mais o código hash encriptado com a chave privada pode ser encriptado usando uma chave secreta simétrica. Essa é uma técnica comum.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Funções de HASH

- Outras aplicações de funções de hash:
  - Criação de um arquivo de senha de mão única: por exemplo, um esquema no qual um hash de uma senha e armazenado por um sistema operacional em vez da senha em si. Desse modo, a senha real não pode ser recuperada pelo hacker que conseguir acesso ao arquivo de senhas;
  - Detecção de intrusão e detecção de vírus: por exemplo, Armazene H(F) para cada arquivo em um sistema e guarde de forma segura os valores de hash (por exemplo, em um CD-R mantido em segurança). Posteriormente, será possível determinar se um arquivo foi modificado, recalculando H(F). Um intruso precisaria alterar F sem alterar H(F);
  - Construção de uma função pseudoaleatória (PRF) ou gerador de número pseudoaleatório (PRNG): uma aplicação comum para um PRF baseado em hash é a geração de chaves simétricas.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Autenticação de Mensagens

- No contexto das comunicações por uma rede, os seguintes ataques podem ser identificados:

1. Divulgação: liberação do conteúdo da mensagem a qualquer pessoa ou processo que não possui a chave criptográfica apropriada.

2. Análise de tráfego: descoberta do padrão de tráfego entre as partes. Em uma aplicação orientada a conexão, a frequência e a duração das conexões poderiam ser determinadas. Em um ambiente orientado a conexão ou sem conexão, o número e a extensão das mensagens entre as partes poderiam ser determinados.

3. Máscara: inserção de mensagens na rede a partir de uma origem fraudulenta. Isso inclui a criação de mensagens por um oponente, que fingem ter vindo de uma entidade autorizada. Também se incluem as confirmações fraudulentas de recebimento ou não de mensagem por alguém que não seja o destinatário dela.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Autenticação de Mensagens

- .. os seguintes ataques podem ser identificados (continuação):

4. Modificação de conteúdo: mudanças no conteúdo de uma mensagem, incluindo inserção, exclusão, transposição e modificação.

5. Modificação de sequência: qualquer modificação em uma sequência de mensagens entre as partes, incluindo inserção, exclusão e reordenação.

6. Modificação de tempo: atraso ou repetição de mensagens. Em uma aplicação orientada a conexão, uma sessão inteira ou uma sequência de mensagens poderia ser uma repetição de alguma sessão anterior válida, ou mensagens individuais na sequência poderiam ser adiadas ou repetidas. Em uma aplicação sem conexão, uma mensagem individual (por exemplo, datagrama) poderia ser adiada ou replicada.

7. Não reconhecimento na origem: negação de transmissão de mensagem pela origem.

8. Não reconhecimento no destino: negação do recebimento da mensagem pelo destino.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Autenticação de Mensagens

- Medidas para lidar com os dois primeiros ataques estão no âmbito da confidencialidade da mensagem. As medidas para lidar com os itens de 3 a 6 na lista anterior geralmente são consideradas como autenticação de mensagem. Os mecanismos para tratar especificamente do item 7 vêm sob o título de assinaturas digitais. O tratamento do item 8 pode exigir uma combinação do uso de assinaturas digitais e um protocolo projetado para impedir esse ataque;

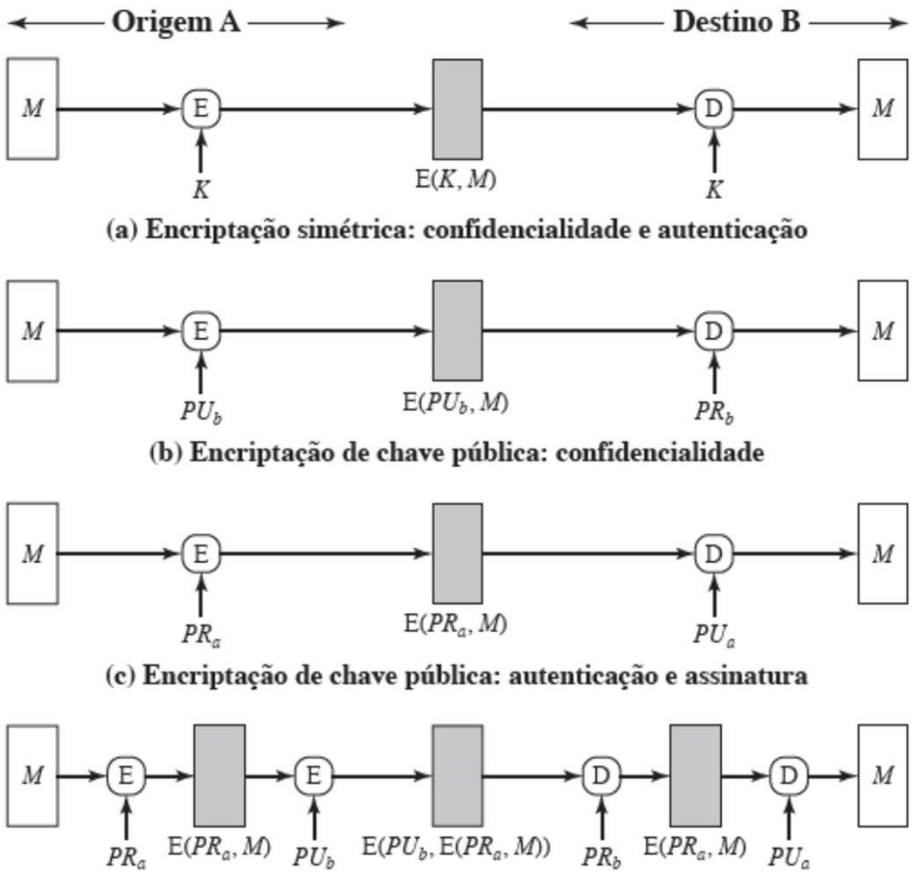
- A autenticação de mensagem é um procedimento para verificar se as mensagens recebidas vêm da origem afirmada e se não foram alteradas. A autenticação da mensagem também pode verificar sequência e tempo. Uma assinatura digital é uma técnica de autenticação que também inclui medidas para impedir o não reconhecimento por parte da origem;

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Aplicação de Chaves de Criptografia

- Como havíamos discutido anteriormente, dependendo da forma como as chaves são aplicadas, é possível obter resultados diferentes:

Figura 12.1 Usos básicos da encriptação de mensagem.



(a) Encriptação simétrica: confidencialidade e autenticação

(b) Encriptação de chave pública: confidencialidade

(c) Encriptação de chave pública: autenticação e assinatura

(d) Encriptação de chave pública: confidencialidade, autenticação e assinatura

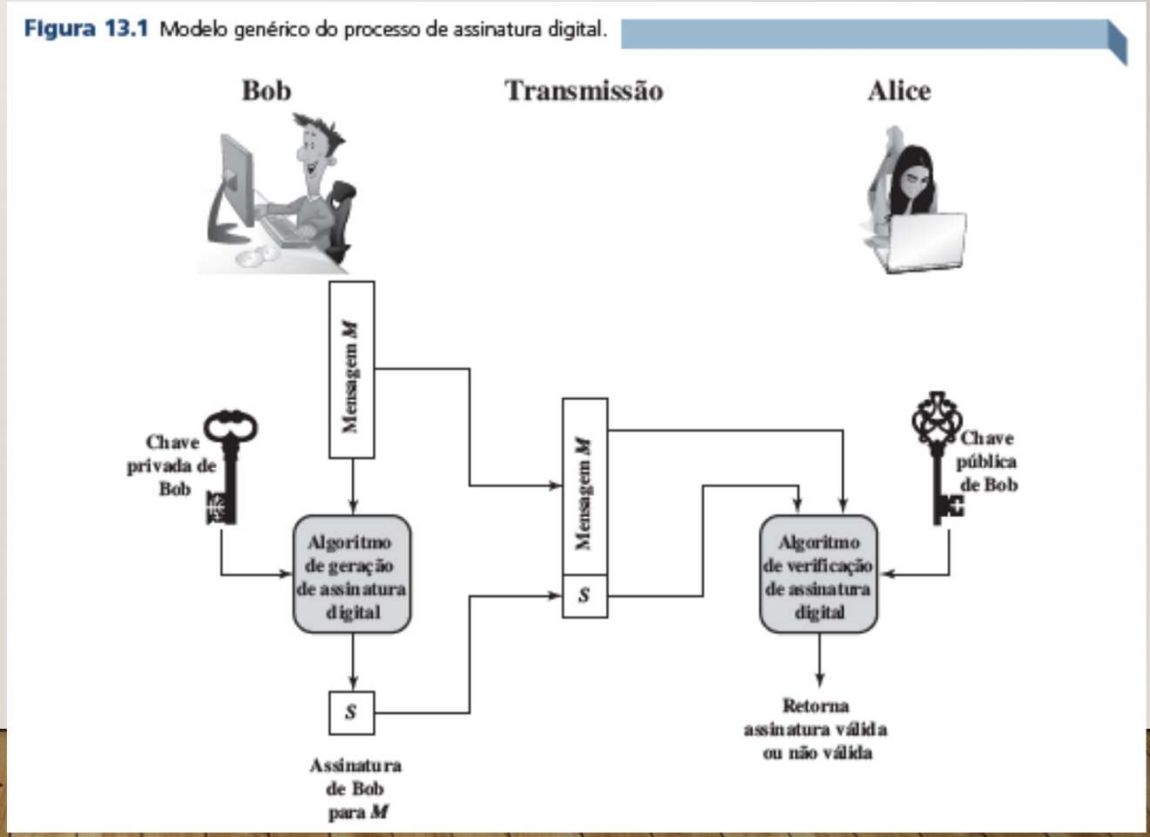
FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Assinatura Digital e Certificado Digital

- O desenvolvimento mais importante a partir da criptografia de chave pública é a assinatura digital. Esta oferece um conjunto de capacidades de segurança que seria difícil de implementar de qualquer outra maneira;

A Figura 13.1 é um modelo genérico do processo de criação e uso de assinaturas digitais. Bob pode assinar uma mensagem usando um algoritmo de geração de assinatura digital. As entradas do algoritmo são a mensagem e a chave privada de Bob. Qualquer outro usuário pode verificar a assinatura usando um algoritmo de verificação, cujas entradas são a mensagem, a assinatura e a chave pública de Bob.

Figura 13.1 Modelo genérico do processo de assinatura digital.



FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Assinatura Digital e Certificado Digital

- A autenticação da mensagem protege duas partes que trocam mensagens contra um terceiro qualquer. Porém, ela não protege as duas partes uma da outra. Várias formas de disputa entre as duas são possíveis;
- Possíveis ataques e falsificações:
  - Ataque somente de chave: C só conhece a chave pública de A.
  - Ataque de mensagem conhecida: C recebe acesso a um conjunto de mensagens e suas assinaturas.
  - Ataque de mensagem escolhida genérica: C escolhe uma lista de mensagens antes de tentar quebrar o esquema de assinatura de A, independente da chave pública de A. C, então, obtém de A assinaturas válidas para as mensagens escolhidas. O ataque é genérico, pois não depende da chave pública de A; o mesmo ataque é usado contra todos.
  - Ataque de mensagem escolhida direcionada: semelhante ao ataque genérico, exceto que a lista de mensagens a serem assinadas é escolhida depois que C conhece a chave pública de A, mas antes que quaisquer assinaturas sejam vistas.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Assinatura Digital e Certificado Digital

- Possíveis ataques e falsificações (continuação):
  - Ataque de mensagem escolhida adaptativa: C tem permissão para usar A como um "oráculo". Isso significa que C pode solicitar de A assinaturas de mensagens que dependam de pares mensagem-assinatura previamente obtidos.

- Em situações nas quais não existe confiança completa entre emissor e receptor, é necessário algo mais do que a autenticação. A solução mais atraente para esse problema é a assinatura digital. A assinatura digital precisa ter as seguintes características:
  - verificar o autor e a data e hora da assinatura.
  - autenticar o conteúdo no momento da assinatura.
  - ser verificável por terceiros, para resolver disputas.

- Assim, a função de assinatura digital inclui a função de autenticação.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Assinatura Digital e Certificado Digital

- Requisitos de uma Assinatura Digital:

  - Precisa ser um padrão de bits que depende da mensagem sendo assinada;
  - Precisa usar alguma informação exclusiva do emissor, para impedir falsificação e negação;
  - É preciso ser relativamente fácil produzir a assinatura digital;
  - É preciso ser relativamente fácil reconhecer e verificar a assinatura digital;
  - É preciso ser computacionalmente inviável falsificar uma assinatura digital, seja construindo uma nova mensagem para uma assinatura digital existente ou uma assinatura digital fraudulenta para determinada mensagem;
  - É preciso ser prático reter uma cópia da assinatura digital em termos de armazenamento.

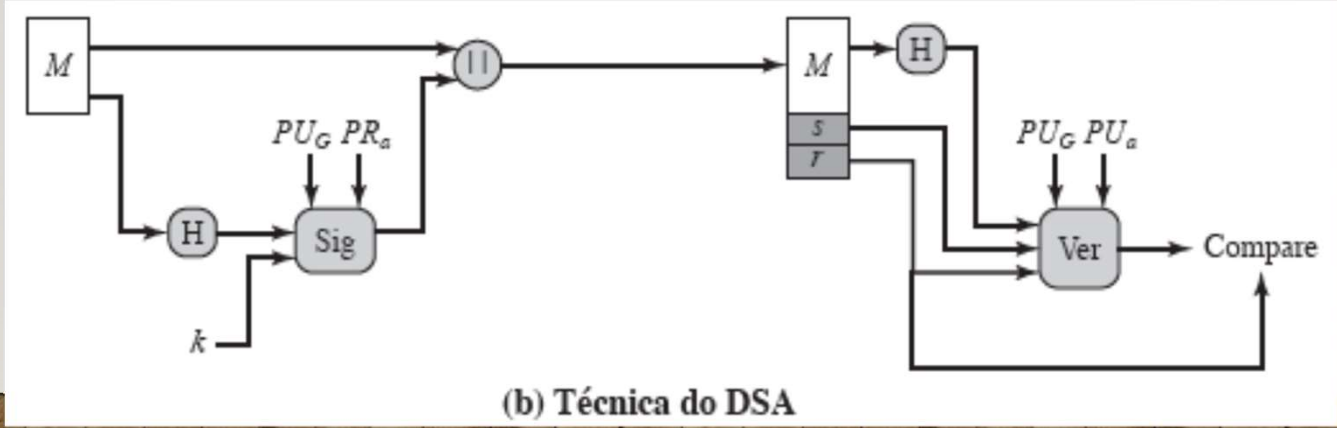
FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Assinatura Digital e Certificado Digital

- Assinatura Direta:
  - Refere-se a um esquema de assinatura digital que envolve apenas as partes em comunicação (origem, destino). Considera-se que o destino conhece a chave pública da origem. A confidencialidade pode ser fornecida pela encriptação da mensagem inteira mais a assinatura com uma chave secreta (encriptação simétrica);
  - Em caso de disputa, algum terceiro deverá ver a mensagem e sua assinatura;
  - A validade do esquema depende da segurança da chave privada do emissor.
- Assinatura Digital do NIST - DSA:
  - O National Institute of Standards and Technology (NIST) publicou o Federal Information Processing Standard FIPS 186, conhecido como algoritmo de assinatura digital (Digital Signature Algorithm — DSA). O DSA utiliza o Secure Hash Algorithm (SHA);
  - O DSA utiliza um algoritmo que é projetado para oferecer apenas a função de assinatura digital;

Assinatura Digital e Certificado Digital

- Assinatura Digital do NIST - DSA:
  - O DSA usa uma função de hash. O código de hash é fornecido como entrada de uma função de assinatura, junto com um número aleatório k, gerado para essa assinatura em particular. A função de assinatura também depende da chave privada do emissor (PRa) e um conjunto de parâmetros conhecidos de um grupo de membros em comunicação. Podemos considerar esse conjunto como constituindo uma chave pública global (PUg). O resultado é uma assinatura que consiste em dois componentes, rotulados com s e r;



(b) Técnica do DSA

Assinatura Digital e Certificado Digital

- Assinatura Digital do NIST - DSA:
  - Na ponta receptora, o código de hash da mensagem que chega é gerado. Isso mais a assinatura são utilizados como entrada de uma função de verificação. A função de verificação também depende da chave pública global, além da chave pública do emissor (PUa), que é emparelhada com a chave privada dele. A saída da função de verificação é um valor igual ao componente de assinatura r se a assinatura for válida;
  - A função de assinatura é tal que somente o emissor, com conhecimento da chave privada, poderia ter produzido a assinatura válida.

- Outros tipos de Assinatura Digital utilizadas são: ECDSA, RSA-PSS

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Assinatura Digital e Certificado Digital

- Agora que já discutimos a aplicação das funções de hash e das assinaturas digitais, precisamos discutir a questão de distribuição segura das chaves envolvidas no processo;

- Os tópicos de gerenciamento e distribuição de chave criptográfica são complexos, envolvendo considerações criptográficas, de protocolo e de gerenciamento;

- Veremos aqui algumas soluções para a distribuição de chaves simétricas e chaves assimétricas, considerando o número de participantes e as questões de comunicação segura já indicadas.

Assinatura Digital e Certificado Digital

- Distribuição de Chaves Simétricas:
  - Para que a encriptação simétrica funcione, as duas partes precisam compartilhar a mesma chave, que precisa ser protegida contra o acesso por outras partes;
  - Além disso, mudanças frequentes na chave normalmente são desejáveis para limitar a quantidade de dados comprometidos caso um atacante a recupere;
  - Para a encriptação de ponta a ponta, um centro de distribuição de chaves é responsável por distribuir chaves a pares de usuários (hosts, processos, aplicações) conforme a necessidade. Cada usuário precisa compartilhar uma chave exclusiva com o centro de distribuição de chaves, para fins de distribuição delas;
  - O uso de um centro de distribuição de chaves é baseado no uso de uma hierarquia de chaves. No mínimo, dois níveis de chaves são usados;
  - A comunicação entre os sistemas finais é encriptada usando uma chave temporária, normalmente referenciada como uma chave de sessão;

Assinatura Digital e Certificado Digital

- Distribuição de Chaves Simétricas:
  - Normalmente, a chave de sessão é usada pela duração de uma conexão lógica, como uma conexão frame relay ou conexão de transporte, e depois descartada. Cada chave de sessão é obtida a partir do centro de distribuição de chaves pelas mesmas instalações de rede usadas para a comunicação do usuário final. Por conseguinte, as chaves de sessão são transmitidas em formato encriptado, usando uma chave mestra que é compartilhada pelo centro de distribuição de chave e um sistema ou usuário final;
  - Para cada sistema ou usuário final, existe uma chave mestra exclusiva, que ele compartilha com o centro de distribuição de chaves. Naturalmente, essas chaves mestras precisam ser distribuídas de alguma maneira;
  - As chaves mestras podem ser distribuídas de alguma maneira não criptográfica, como a remessa física;

Assinatura Digital e Certificado Digital

- Distribuição de Chaves Simétricas usando Encriptação Assimétrica:
  - Devido à ineficácia dos criptossistemas de chave pública, eles quase nunca são usados para a encriptação direta do bloco de dados de tamanho razoável, mas são limitados a blocos relativamente pequenos. Um dos usos mais importantes de um criptossistema de chave pública é encriptar chaves simétricas para distribuição;
  - Um sistema simples pode ser descrito a seguir:
    - A gera um par de chaves pública/privada {PUa, PRa} e transmite uma mensagem para B consistindo em PUa e um identificador de A, IDA;
    - B gera uma chave secreta, *Ks*, e a transmite para A, encriptada com a chave publica de A;
    - A calcula D(PRa, E(PUa, Ks)) para recuperar a chave secreta. Como somente A pode decriptar a mensagem, apenas A e B saberão a identidade de Ks;
    - A descarta PUa e PRa e B descarta PUa.
    - A e B agora podem seguramente se comunicar usando a encriptação convencional e a chave da sessão Ks. Ao término da troca, tanto A quanto B descartam Ks.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Assinatura Digital e Certificado Digital

- Distribuição de Chaves Simétricas usando Encriptação Assimétrica:
  - O sistema apresentado não é imune ao ataque man-in-the-midlle, que pode interceptar as mensagens e usar as duas próprias chaves antes de repassar ao destinatário;
  - Para adicionar segurança contra ataques ativos e passivos, começamos em um ponto em que se considera que A e B trocaram chaves públicas por um dos esquemas
  - descritos anteriormente nesta seção. Depois, ocorrem as seguintes etapas:
    - A usa a chave pública de B para encriptar uma mensagem para B contendo um identificador de A (IDA) e um nonce (N1), que é usado para identificar essa transação de forma exclusiva;
    - B envia uma mensagem para A encriptada com PUa e contendo o nonce (N1) de A, além de um novo nonce, gerado por B (N2). Como somente B poderia ter decriptado a mensagem (1), a presença de N1 na mensagem (2) garante a A que o correspondente é B.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Assinatura Digital e Certificado Digital

- Distribuição de Chaves Simétricas usando Encriptação Assimétrica:
  - O sistema apresentado não é imune ao ataque man-in-the-midlle, que pode interceptar as mensagens e usar as duas próprias chaves antes de repassar ao destinatário;
  - Para adicionar segurança contra ataques ativos e passivos, começamos em um ponto em que se considera que A e B trocaram chaves públicas por um dos esquemas
  - descritos anteriormente nesta seção. Depois, ocorrem as seguintes etapas:
    - A usa a chave pública de B para encriptar uma mensagem para B contendo um identificador de A (IDA) e um nonce (N1), que é usado para identificar essa transação de forma exclusiva;
    - B envia uma mensagem para A encriptada com PUa e contendo o nonce (N1) de A, além de um novo nonce, gerado por B (N2). Como somente B poderia ter decriptado a mensagem (1), a presença de N1 na mensagem (2) garante a A que o correspondente é B.

Assinatura Digital e Certificado Digital

- Distribuição de Chaves Públicas:
  - Várias técnicas têm sido propostas para a distribuição de chaves públicas. Praticamente todas essas propostas podem ser agrupadas nos seguintes esquemas gerais:
    - Anúncio público
    - Diretório disponível publicamente
    - Autoridade de chave pública
    - Certificados de chave pública

  - Anúncio Público:
    - O diferencial da encriptação de chave pública é que ela é pública;
    - Assim, se houver algum algoritmo de chave pública amplamente aceito, como RSA, qualquer participante pode enviar sua chave pública a qualquer outro ou transmitir a chave por broadcast à comunidade em geral;
    - Ponto fraco: Qualquer um pode falsificar esse anúncio público.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Assinatura Digital e Certificado Digital

- Distribuição de Chaves Públicas:
  - Diretório disponível publicamente:
    - A manutenção e a distribuição do diretório público teria que ser de responsabilidade de alguma entidade ou organização confiável;
    - Esse esquema incluiria os seguintes elementos:

1. A autoridade mantém um diretório com uma entrada {nome, chave pública} para cada participante;

2. Cada participante registra uma chave pública com a autoridade de diretório. O registro teria que ser feito pessoalmente ou por alguma forma de comunicação autenticada segura;

3. Um participante pode substituir a chave existente por uma nova a qualquer momento, seja por um desejo de substituir uma chave pública que já foi usada para uma grande quantidade de dados, ou porque a chave privada correspondente foi comprometida de alguma forma;

Assinatura Digital e Certificado Digital

- Distribuição de Chaves Públicas:
  - Diretório disponível publicamente:
    - Esse esquema incluiria os seguintes elementos (continuação):

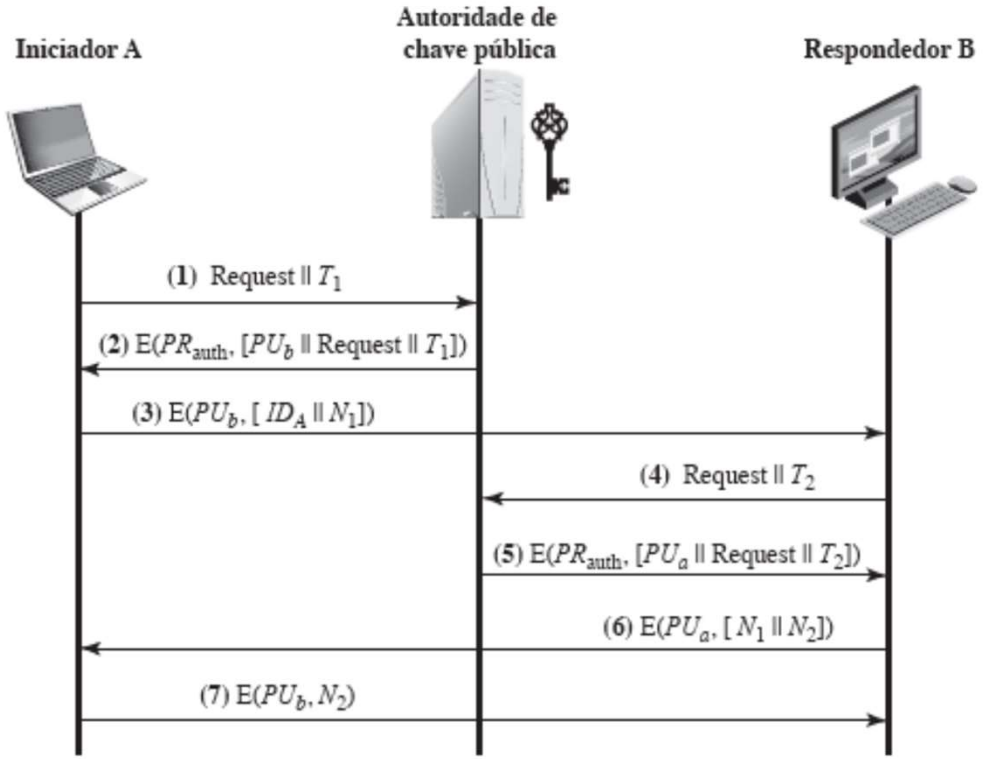
      4. Os participantes também poderiam acessar o diretório eletronicamente. É obrigatório que haja uma comunicação segura e autenticada da autoridade para o participante.
    - Esse esquema é claramente mais seguro do que os anúncios públicos individuais, mas ainda tem vulnerabilidades. Se um adversário conseguir obter ou calcular a chave privada da autoridade de diretório ou mexer nos registros mantidos pela autoridade.

  - Autoridade de chave pública:
    - O cenário mais seguro considera que uma autoridade central mantém um diretório dinâmico de chaves públicas de todos os participantes. Além disso, cada participante conhece com segurança uma chave pública para a autoridade, apenas com a autoridade conhecendo a chave privada correspondente;

Assinatura Digital e Certificado Digital

- Distribuição de Chaves Públicas - Autoridade de chave pública:

Figura 14.12 Cenário de distribuição de chave pública.



Assinatura Digital e Certificado Digital

- Distribuição de Chaves Públicas - Autoridade de chave pública:
  - As seguintes etapas ocorrem:

    1. A envia uma mensagem com estampa de tempo à autoridade de chave pública, contendo uma solicitação para a chave pública atual de B;

    2. A autoridade responde com uma mensagem que é encriptada usando a chave privada da autoridade, PRauth. Assim, A é capaz de decriptar a mensagem usando a chave pública da autoridade. Portanto, A tem garantias de que a mensagem foi originada pela autoridade. A mensagem inclui o seguinte:
    - A chave pública de B, PUb, que A pode usar para encriptar mensagens destinadas a B;
    - A solicitação original, para permitir que A compare essa resposta com a solicitação anterior correspondente e verifique se a solicitação original não foi alterada antes do recebimento pela autoridade;
    - A estampa de tempo original, para que A possa determinar que essa não é uma mensagem antiga da autoridade, contendo uma chave diferente da chave pública atual de B.

Assinatura Digital e Certificado Digital

- Distribuição de Chaves Públicas - Autoridade de chave pública:
  - As seguintes etapas ocorrem:

3. A armazena a chave pública de B e também a utiliza para encriptar uma mensagem para B, contendo um identificador de A (IDA) e um nonce (N1), que é usado para identificar essa transmissão exclusivamente;

4, 5. B obtém a chave pública de A na autoridade da mesma forma como A obteve a chave pública de B;

Nesse ponto, as chaves públicas foram entregues com segurança a A e B, e eles podem iniciar sua troca protegida. Porém, duas etapas adicionais são desejáveis:

6. B envia uma mensagem a A encriptada com PUa e contendo o nonce (N1) de A, além de um novo nonce gerado por B (N2). Como somente B poderia ter decriptado a mensagem (3), a presença de N1 na mensagem (6) garante a A que o correspondente é B.

7. A retorna N2 encriptado, usando a chave pública de B, para garantir a B que seu correspondente é A.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Assinatura Digital e Certificado Digital

- Distribuição de Chaves Públicas - Certificados de chave pública:
  - O cenário de Autoridade de chave pública é atraente mas também apresenta fragilidades. A autoridade de chave pública poderia ser um gargalo no sistema, pois um usuário precisa apelar para a autoridade para obter uma chave pública para cada outro usuário com quem queira se comunicar. E o diretório de nomes e chaves públicas mantido pela autoridade é vulnerável a violação;
  - Uma alternativa a esse modelo é usar certificados que possam ser utilizados pelos participantes para trocar chaves sem contatar uma autoridade de chave pública, de um modo que seja tão confiável quanto se as chaves fossem obtidas diretamente de uma autoridade de chave pública;
  - Um certificado consiste em uma chave pública mais um identificador do proprietário da chave, com o bloco inteiro assinado por um terceiro confiável. Normalmente, o terceiro é uma autoridade certificadora, como uma agência do governo ou uma instituição financeira, na qual a comunidade de usuários confia;

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Assinatura Digital e Certificado Digital

- Distribuição de Chaves Públicas - Certificados de chave pública:
  - O usuário pode apresentar sua chave pública à autoridade de maneira segura e obter seu certificado;
  - São requisitos nesse esquema:

    1. Qualquer participante pode ler um certificado para determinar o nome e a chave pública do proprietário do certificado.

    2. Qualquer participante pode verificar se o certificado foi originado pela autoridade certificadora, e não é uma falsificação.

    3. Somente a autoridade certificadora pode criar e atualizar certificados.
  - Esses requisitos são satisfeitos pela proposta original em [KOHN78]. Denning [DENN83] acrescentou o seguinte requisito adicional:

    4. Qualquer participante pode verificar se o certificado está atualizado.
  - Nesse contexto, o comprometimento de uma chave privada é comparável à perda de um cartão de crédito (inclusive quanto aos cancelamentos).

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Assinatura Digital e Certificado Digital

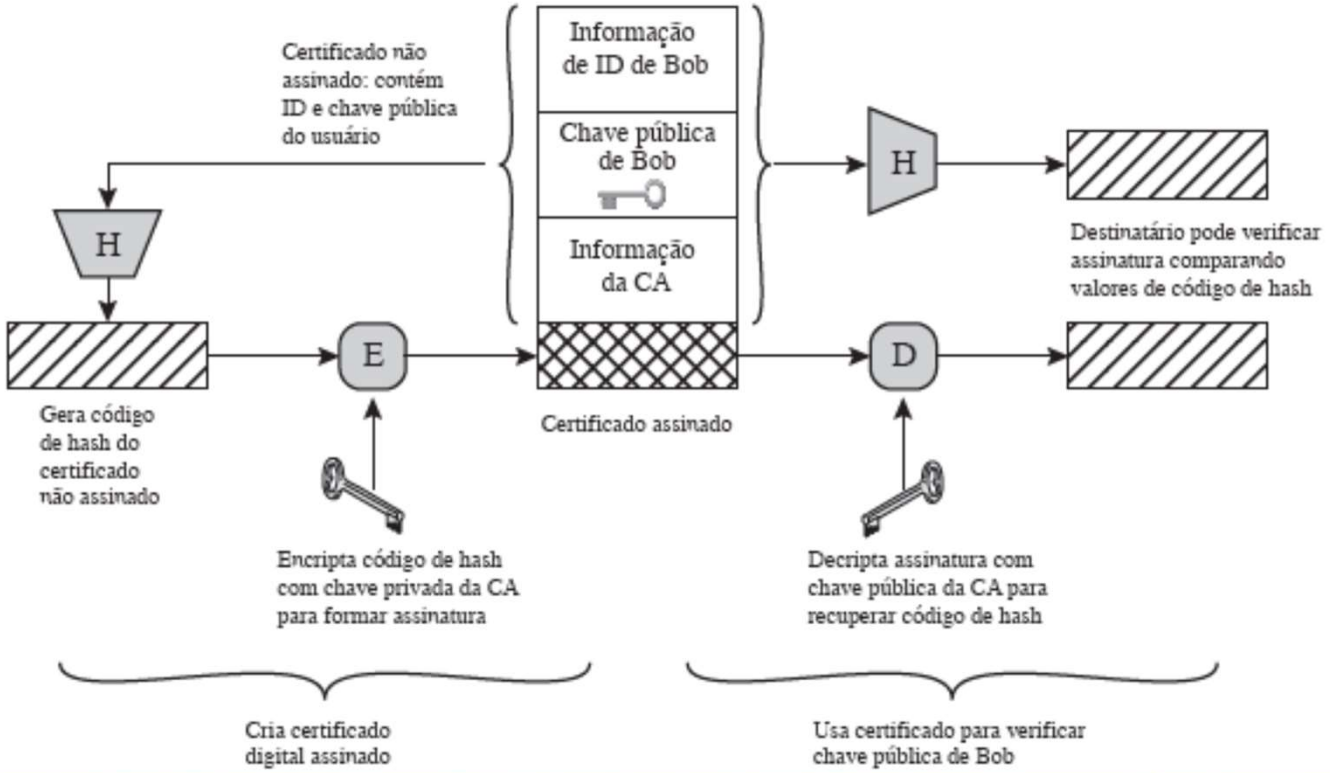
- Distribuição de Chaves Públicas - Certificados de chave pública:
  - Um esquema foi aceito universalmente para formatar certificados de chave pública: o padrão X.509;
  - O padrão X.509:
    - é um padrão definido pelo ITU-T importante porque a estrutura de certificado e os protocolos de autenticação definidos nele são usados em diversos contextos: em S/MIME, IP Security e SSL/TLS;
    - define uma estrutura para a provisão de serviços de autenticação pelo diretório aos seus usuários;
    - é baseado no uso da criptografia de chave pública e assinaturas digitais. O padrão não dita o uso de um algoritmo específico, mas recomenda o RSA. Assume-se que o esquema de assinatura digital exija o uso de uma função de hash, também não definida;
  - Ele foi proposto inicialmente em 1988. O padrão foi revisado posteriormente para resolver alguns dos problemas de segurança; uma recomendação revisada foi emitida em 1993. Uma terceira versão foi emitida em 1995 e revisada em 2000.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Assinatura Digital e Certificado Digital

- Distribuição de Chaves Públicas - Certificados de chave pública:

Figura 14.14 Uso do certificado de chave pública.



FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Assinatura Digital e Certificado Digital

- Distribuição de Chaves Públicas - Certificados de chave pública:

  - Tanto ITU como a IETF desenvolveram padrões para autoridades certificadoras;
  - Recomendação ITU X.509 encontramos a especificação de um serviço de autenticação, bem como uma sintaxe específica para certificados.
  - O RFC 1422 descreve um gerenciamento de chaves baseado em CA. Essa recomendação é compatível com X.509, mas vai além, pois estabelece procedimentos e convenções para uma arquitetura de gerenciamento de chaves.

TABELA 8.4 CAMPOS SELECIONADOS DE UMA CHAVE PÚBLICA X.509 E RFC 1422

Nome do campo	Descrição
Versão	Número da versão da especificação X.509
Número de série	Identificador exclusivo emitido pela CA para um certificado
Assinatura	Especifica o algoritmo usado pela CA para assinar esse certificado
Nome do emissor	Identidade da CA que emitiu o certificado, em formato de nome distinto (DN) [RFC 2253]
Período de validade	Início e fim do período de validade do certificado
Nome do sujeito	Identidade da entidade cuja chave pública está associada a esse certificado, em formato DN
Chave pública do sujeito	A chave pública do sujeito, bem como uma indicação do algoritmo de chave pública (e parâmetros do algoritmo) a ser usado com essa chave

Fonte: KUROSE, J. Redes de computadores e a Internet: uma abordagem top-down/ James F. Kurose, Keith W. Ross ; tradução Daniel Vieira; revisão técnica Wagner Luiz Zucchi. – 6. ed. – São Paulo: Pearson Education do Brasil, 2013.

Assinatura Digital e Certificado Digital

- Infraestrutura de chave pública:
  - A RFC 4949 define a infraestrutura de chave pública (PKI, do acrônimo em inglês para Public-Key Infrastructure) como o conjunto de hardware, software, pessoas, políticas e procedimentos necessários para criar, gerenciar, armazenar, distribuir e revogar certificados digitais com base na criptografia assimétrica;
  - O objetivo principal para desenvolver uma PKI é permitir a aquisição segura, conveniente e eficiente de chaves públicas. O grupo de trabalho Public Key Infrastructure X.509 (PKIX) da Internet Engineering Task Force (IETF) tem sido a força motriz por trás da preparação de um modelo formal (e genérico) baseado no X.509 que seja adequado para a implantação de uma arquitetura baseada em certificado na Internet.

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Assinatura Digital e Certificado Digital

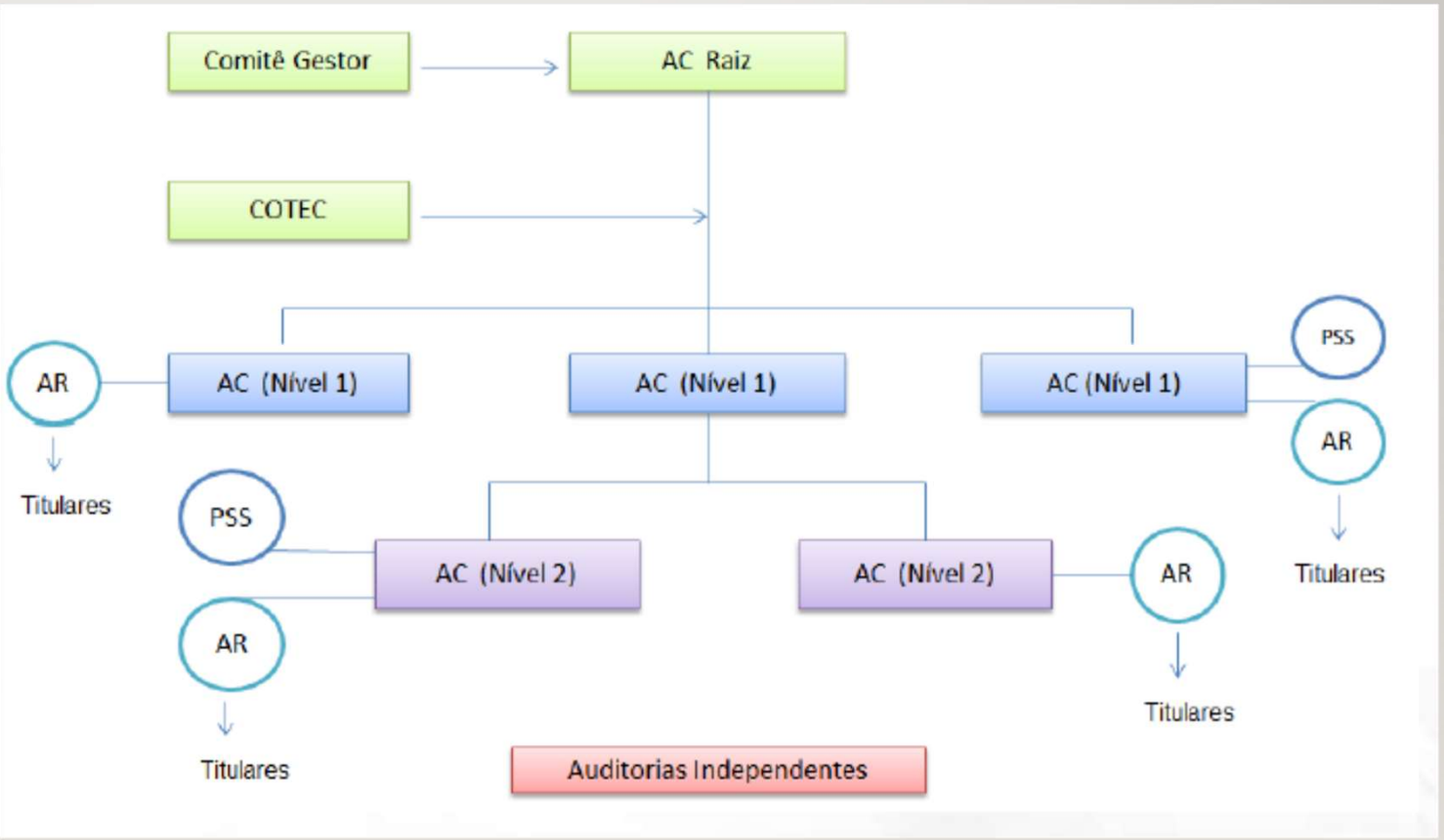
- Infraestrutura de chave pública:
  - A Infraestrutura de Chaves Públicas Brasileira, ICP-Brasil, é uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão. (https://www.iti.gov.br/icp-brasil);
  - Observa-se que o modelo adotado pelo Brasil foi o de certificação com raiz única, sendo que o ITI além de desempenhar o papel de Autoridade Certificadora Raiz (AC-Raiz), também, tem o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos;
  - A Autoridade Certificadora Raiz da ICP-Brasil é a primeira autoridade da cadeia de certificação;
  - É executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil;
  - À ICP-Raiz compete emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subsequente ao seu.

Fonte: Internet – Página do ICP Brasil

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Assinatura Digital e Certificado Digital

- Infraestrutura de chave pública - Estrutura da ICP-Brasil:
  - AC = Autoridade Certificadora
  - AR = Autoridade de Registro
  - PSS = Prestador de Serviço de Suporte
  - Para mais detalhes sobre os entes que compõem a estrutura, acesse: https://www.iti.gov.br/icp-brasil/entes-da-icp-brasil



Fonte: Internet – Página do ICP Brasil

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Assinatura Digital e Certificado Digital

- Tipos de Certificados Digitais:
  - Na ICP-Brasil estão previstos oito tipos de certificado;
    - São duas séries de certificados, com quatro tipos cada:
    - A série A (A1, A2, A3 e 4) reúne os certificados de assinatura digital, utilizados na confirmação de identidade na Web, em e-mail, em redes privadas virtuais (VPN) e em documentos eletrônicos com verificação da integridade de suas informações;
    - A série S (S1, S2, S3 e S4) reúne os certificados de sigilo, utilizados na codificação de documentos, de bases de dados, de mensagens e de outras informações eletrônicas sigilosas;
    - Os oito tipos são diferenciados pelo uso (aplicação), pelo nível de segurança e pela validade, conforme quadro apresentado a seguir.

Fonte: Internet – Página do ICP Brasil e Autoridades Certificadoras

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Assinatura Digital e Certificado Digital

- Resumo de Certificados Digitais:

Tipo de certificado	Chave criptográfica			Validade máxima (anos)
	Tamanho (bits)	Processo de geração	Mídia armazenadora	
A1 e S2	1024	Software	Arquivo	1
A2 e S2	1024	Software	Smart card ou token, sem capacidade de geração de chave	2
A3 e S3	1024	Hardware	Smart card ou token, com capacidade de geração de chave	3
A4 e S4	2048	Hardware	Smart card ou token, com capacidade de geração de chave	3

Fonte: Internet – Página do ICP Brasil e Autoridades Certificadoras

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Assinatura Digital e Certificado Digital

- Exemplo de Certificado Digital:

  - O e-CPF é a versão eletrônica do CPF que garante a autenticidade e a integridade nas transações eletrônicas de pessoas físicas;
  - Criado para identificar o contribuinte pessoa física na internet, o e-CPF é emitido pelas seguintes autoridades certificadoras: Serasa, Certisign, Prodemg, Serpro, Imesp e Sincor. Ele pode ser dos tipos A1 e A3.

Fonte: Internet – Página do ICP Brasil e Autoridades Certificadoras

FAETERJ-Rio
Faculdade de Educação Tecnológica do Rio de Janeiro

Assinatura Digital e Certificado Digital

- Os certificados mais comuns são:
  - A1:
    - De menor nível de segurança;
    - É gerado e armazenado no computador do usuário;
    - Os dados são protegidos por uma senha de acesso.
    - Somente com essa senha é possível acessar, mover e copiar a chave privada a ele associada.
  - A3:
    - De nível de segurança médio a alto;
    - É gerado e armazenado em um hardware criptográfico, que pode ser um cartão inteligente ou um token;
    - Apenas o detentor da senha de acesso pode utilizar a chave privada, e as informações não podem ser copiadas ou reproduzidas.

Fonte: Internet – Página do ICP Brasil e Autoridades Certificadoras