

Curso de Tecnologia em Redes de Computadores
Disciplina: Tópicos Avançados II – 5º período
Professor: José Maurício S. Pinheiro

Aula 1 – Introdução à Certificação Digital

Existem dois tipos de necessidades relacionadas com a troca de mensagens eletrônicas, são elas a autenticação e a privacidade. Como não há a criação física das mensagens, é necessário um mecanismo que garanta a autenticidade e inviolabilidade da mensagem, o que é conhecido como “autenticação”. Além disto, em certos casos, o objetivo é garantir que somente um destinatário receba e leia a mensagem, o que é conhecido como “privacidade”.

1. Assinatura Digital

A autenticação ou assinatura digital é a versão digital da assinatura de punho em documentos físicos. A assinatura digital apresenta um grau de segurança muito superior ao de uma assinatura de punho.

O destinatário de uma mensagem assinada digitalmente pode verificar se a mensagem foi realmente emitida pela pessoa cuja assinatura nela consta, ou se a mensagem não foi em algum ponto adulterada intencional ou acidentalmente depois de assinada. Mais ainda, uma assinatura digital que tenha sido verificada não pode ser negada. Aquele que assinou digitalmente a mensagem não pode dizer mais tarde que sua assinatura digital foi falsificada. Em outras palavras, assinaturas digitais habilitam "autenticação" de documentos digitais, garantindo ao destinatário de uma mensagem digital tanto a identidade do remetente quanto a integridade da mensagem.

A assinatura digital é um conjunto de procedimentos matemáticos realizados com a utilização de técnicas de criptografia assimétrica que permite, de forma única e exclusiva, a comprovação da autoria de um determinado conjunto de dados. Por exemplo, para personalizar uma mensagem, um determinado usuário A codifica uma mensagem utilizando sua chave secreta e a envia para o destinatário B. Somente a chave pública de A permitirá a decodificação dessa mensagem. Portanto é a prova de que A enviou a mensagem para B. A mensagem assim pode ser decodificada por qualquer um que tenha a chave pública de A. Uma assinatura é considerada autêntica quando um usuário usa a chave pública de A para decifrar uma mensagem. Nesse momento ele confirma que foi A e somente A quem enviou a mensagem. A assinatura não pode ser forjada porque somente A conhece sua chave secreta e um documento, uma vez assinado, não pode ser alterado. Se ocorrer qualquer alteração no texto criptografado, este não poderá ser restaurado com o uso da chave pública de A.

A assinatura digital não é reutilizável, ou seja, a assinatura é uma função do documento e não pode ser transferida para outro documento. Da mesma forma a assinatura não pode ser repudiada. O usuário B não precisa de

nenhuma ajuda de A para reconhecer sua assinatura e A não pode negar ter assinado o documento.

A assinatura digital pode ser implementada basicamente de três formas: função hash por meio dos padrões MD5 e SHA (Secure Hash Algorithm), DSS - Digital Signature Standard e utilizando o conceito de chaves públicas com o padrão RSA.

2. Propriedades da assinatura digital

A assinatura digital, analogamente à assinatura escrita, deve possuir as seguintes propriedades:

- Ser capaz de verificar o autor e a data/hora da assinatura;
- Autenticar o conteúdo original;
- A assinatura deve ser verificável por terceiros (resolver disputas).

Com base nas propriedades citadas, a assinatura digital deve satisfazer os seguintes requerimentos:

- Dependem do Conteúdo;
- Usar informação única do originador;
- Fácil de produzir;
- Fácil de reconhecer e verificar;
- Inviável de forjar;
- Prática para manter uma cópia da assinatura.

3. Tipos de assinatura digital

A assinatura digital pode ser dividida em dois tipos básicos: direta e arbitrada. A assinatura digital direta envolve somente as partes comunicantes (origem “X” e destino “Y”). Assume-se que o destino conheça a chave pública da origem.

A assinatura digital pode ser formada encriptando toda a mensagem com a chave privada de “X” ou encriptando apenas o código hash. Neste tipo de assinatura, “X” pode negar a assinatura em algum documento alegando que sua chave foi roubada. Para isto, existe também um selo de tempo que será anexada a mensagem com data e hora da assinatura. Os problemas associados com a assinatura digital direta podem ser resolvidos se usar um árbitro. A assinatura digital arbitrada prevê a presença de um árbitro “A”. A mensagem que será enviada de “X” para “Y” passa primeiramente por “A” para ser verificada e datada.

4. Certificação Digital

O certificado digital equivale a uma carteira de identidade virtual ao permitir a identificação de uma pessoa no meio digital/eletrônico quando

enviando uma mensagem ou em alguma transação pela Internet que necessite validade legal e identificação inequívoca.

Um certificado digital contém dados de seu titular, tais como nome, identidade civil, e-mail, nome e assinatura da Autoridade Certificadora que o emitiu, entre outras informações. É importante saber que essa tecnologia confere a mesma validade jurídica ao documento assinado digitalmente do equivalente em papel assinado de próprio punho.

O certificado digital é um arquivo eletrônico que contém dados de uma pessoa ou instituição, utilizados para comprovar sua identidade. Este arquivo pode estar armazenado em um computador ou em outra mídia, como um token ou smart card.

Exemplos semelhantes a um certificado digital são o CNPJ, RG, CPF e carteira de habilitação de uma pessoa. Cada um deles contém um conjunto de informações que identificam a instituição ou pessoa e a autoridade (para estes exemplos, órgãos públicos) que garante sua validade.

Algumas das principais informações encontradas em um certificado digital são:

- Dados que identificam o dono (nome, número de identificação, estado, etc);
- Nome da Autoridade Certificadora (AC) que emitiu o certificado;
- Número de série e o período de validade do certificado;
- Assinatura digital da AC.

O objetivo da assinatura digital no certificado é indicar que outra entidade (a Autoridade Certificadora) garante a veracidade das informações nele contidas.

Autoridade Certificadora (AC) é a entidade responsável por emitir certificados digitais. Estes certificados podem ser emitidos para diversos tipos de entidades, tais como: pessoa, computador, departamento de uma instituição, instituição, etc.

Os certificados digitais possuem uma forma de assinatura eletrônica da AC que o emitiu. Graças à sua idoneidade, a AC é normalmente reconhecida por todos como confiável, fazendo o papel de "Cartório Eletrônico".

Alguns exemplos típicos do uso de certificados digitais são:

- Ao acessar um site com conexão segura, como, por exemplo, o acesso aos serviços bancários pela Internet é possível checar se o site apresentado é realmente da instituição que diz ser, através da verificação de seu certificado digital;
- Quando o usuário consulta o banco pela Internet, este tem que se assegurar de sua identidade antes de fornecer informações sobre a conta;
- No envio de um e-mail, o aplicativo de e-mail pode utilizar o certificado para assinar "digitalmente" a mensagem, de modo a assegurar ao destinatário que o e-mail é seu e que não foi adulterado entre o envio e o recebimento.

Autoridades Certificadoras são órgãos autorizados a emitir Certificados Digitais pelo ITI (Instituto Nacional de Tecnologia da Informação), órgão do Governo Federal ligado à Presidência da República. O ITI é a primeira autoridade da cadeia de certificação, a chamada AC Raiz (Autoridade Certificadora Raiz), que emite e controla a ICP-Brasil (Infra-Estrutura de Chaves Públicas Brasileira), modelo de Certificação Digital adotado no País.

Atualmente, existem sete AC's no Brasil que emitem certificados tanto para pessoas físicas quanto jurídicas. São elas:

- Serpro (Serviço Federal de Processamento de Dados);
- CertiSign, empresa privada especializada em certificação digital;
- Serasa;
- IMESP (Imprensa Oficial do Estado de São Paulo);
- PRODEMG, empresa de tecnologia de informação do Governo de Minas Gerais;
- Caixa Econômica Federal
- SINCOR (Sindicato dos Corretores de Seguros do Estado de São Paulo).

A emissão da Certificação Digital só pode ser feita presencialmente. O interessado deve procurar uma AC, preencher um formulário com seus dados e pagar uma taxa que varia de acordo com o modelo do documento. Depois deve se apresentar em uma AR (Autoridade de Registro)

A Autoridade de Registro faz o reconhecimento presencial da pessoa que solicita a Certificação Digital. Entidades como Correios, Caixa Econômica Federal, Sincor, Banco do Brasil, Bradesco, Itaú, e Itaútec são ARs.

5. Certificado Digital

O Certificado Digital é um documento que contém dados de identificação da pessoa ou instituição que deseja comprovar, perante terceiros, a sua própria identidade. Serve, igualmente, para conferir a identidade de terceiros. Pode ser comparado como uma espécie de carteira de identidade eletrônica.

Graças aos certificados digitais, uma transação eletrônica realizada via Internet torna-se perfeitamente segura, pois permite que as partes envolvidas apresentem cada uma, as suas credenciais para comprovar, à outra parte, a sua real identidade.

Tecnicamente, os Certificados Digitais vinculam um par de chaves eletrônicas que pode ser usado para criptografar e assinar informações digitais. Possibilita verificar se um usuário tem, realmente, o direito de usar uma determinada chave, ajudando a impedir que as pessoas usem chaves falsificadas para personificar outros usuários. Usados em conjunto com a criptografia, os Certificados Digitais fornecem uma solução de segurança completa, assegurando a identidade de uma ou de todas as partes envolvidas em uma transação.

O Certificado Digital é emitido por uma terceira parte de confiança denominada Autoridade Certificadora (CA - *Certificate Authority*) e pode ser uma empresa, organização ou indivíduo, público ou privado, que atua como tabelião para verificar e autenticar a identidade de usuários de um sistema criptográfico de chave pública. As CA's devem tomar providências para estabelecer a identidade das pessoas ou organizações para as quais emitem Certificados Digitais. Depois de estabelecerem a identidade de uma organização, elas emitem um certificado que contém a chave pública da organização, e que é assinado com a chave privada da CA.

Os certificados digitais possuem uma forma de assinatura eletrônica de uma instituição reconhecida por todos como confiável, e que, graças à sua idoneidade, faz o papel de "Cartório Eletrônico". Os métodos criptográficos empregados impedem que a assinatura eletrônica seja falsificada, ou que os dados do documento sejam adulterados ou copiados, tornando-o absolutamente inviolável. Garante-se, assim, por quem assina que os dados de identificação do certificado são verdadeiros.

A Certificação Digital garante os três princípios básicos da comunicação segura em um ambiente em rede:

- Autenticidade;
- Privacidade;
- Inviolabilidade.

Assim, uma vez instalada no computador, a Certificação Digital o reconhecerá como habilitado. Da mesma forma, o equipamento estará apto a reconhecer um Site certificado como verdadeiro. Em outras palavras, o documento eletrônico gerado por quem possui um Certificado Digital não pode ser posteriormente refutado, sendo estabelecido um vínculo tão forte quanto o que é gerado por uma assinatura de punho em um documento em papel.

O certificado digital é uma estrutura de dados, dentro da qual estão as seguintes informações:

- Chave pública e nome do usuário;
- Número de série do certificado;
- Nome da certificadora que o emitiu;
- Assinatura digital da CA, assinada com sua respectiva chave secreta.

6. Tipos de Certificados

Os tipos de certificados são A1, A2, A3 a A4. A diferença entre eles é como são gerados e o grau de segurança que proporcionam. Entre os mais usados está o A1, gerado e armazenado em software. Pode ser gravado em HDs, CDs ou DVDs e tem validade de um ano. Este modelo é mais simples e menos seguro que os outros. O A3, também um dos modelos mais usados, é gerado e armazenado em hardwares como smartcards ou tokens (espécie de pen drive com saída USB e leitora embutida). Esta modalidade é mais segura que a A1 e tem validade de três anos.

Questionário

1. Defina “autenticação” e “privacidade”.
2. O que é a “assinatura digital”?
3. Qual sistema criptográfico é usado na assinatura digital?
4. Quais as formas de implementação da assinatura digital?
5. Quais as três propriedades da assinatura digital?
6. Como se chama o tipo básico de assinatura digital que prevê a existência de uma terceira pessoa para ser verificada e datada?
7. O que é o “certificado digital”?
8. Quem emite o certificado digital?
9. Quais são os princípios básicos de segurança seguidos pela certificação digital?
10. Quais informações são encontradas na estrutura do certificado digital?