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

AULA 2: Padrão X.509

O padrão X.509 começou em associação com o padrão X.500 em 1988 (Versão 1) e assumiu um sistema hierárquico das autoridades de certificação para a emissão de certificados. Em 1993, uma versão melhorada do X.509 - versão 2, foi introduzida com a adição de mais dois campos, de apoio e controle de acesso diretório. A versão 3 do padrão foi implementada em junho de 1997 devido a ineficiência encontrada nas versões anteriores. Foram adicionados campos de extensão, o que torna o certificado mais flexível e com uma expansão na utilização. Adicionou-se a compatibilidade com outras topologias, como malhas e pontes, bem como a opção de usá-lo em uma rede P2P. Mais recentemente, foi lançada a versão 4 do padrão X.509. Esta versão está definida na recomendação X.509/ISO/TEC 9594-8 2001.

Certificados Digitais

O Certificado Digital é um arquivo eletrônico que contém informações de identificação, permitindo assegurar a identidade de um site na Internet ou de quem assina uma mensagem ou documento eletrônico (Figura 1).

Um certificado digital é formado por um conjunto de campos padrão e campos de extensões que são necessários para definir as funções do certificado, personalizar um certificado e demais especificidades. Na ICP-Brasil, os certificados são utilizados de acordo com o seu tipo, em aplicações como:

- **Tipo A (ou de assinatura digital):** confirmação da identidade na web, correio eletrônico, transações on-line, redes privadas virtuais (VPN), transações eletrônicas, informações eletrônicas, cifração de chaves de sessão e assinatura de documentos com verificação da integridade de suas informações;
- **Tipo S (ou de sigilo)**: cifração de documentos, bases de dados, mensagens e outras informações eletrônicas.

Uma regra em sistemas de criptografia com chave pública é que os usuários devem ser constantemente vigilantes para assegurar que eles estão encriptando para a chave correta da pessoa ou instituição. Em um ambiente onde é seguro a troca livre de chaves por servidores públicos, os ataques originados no meio de transmissão são uma ameaça potencial. Por esse motivo, é extremamente importante verificar algumas informações contidas no certificado digital do site que se pretende acessar na Internet.

Figura 1 - Certificado Digital

Um exemplo de um certificado emitido para um site de uma instituição é mostrado a seguir (Figura 2).

```
This Certificate belongs to:   This Certificate was issued by:
 www.example.org                www.examplesign.com/CPS Incorp.by Ref.
 Terms of use at                LIABILITY LTD.(c)97 ExampleSign
 www.examplesign.com/dir (c)00  ExampleSign International Server CA -
 UF Tecno                       Class 3
 Example Associados, Inc.       ExampleSign, Inc.
 Cidade, Estado, BR

Serial Number:
  70:DE:ED:0A:05:20:9C:3D:A0:A2:51:AA:CA:81:95:1A
This Certificate is valid from Sat Aug 20, 2005 to Sun
Aug 20, 2006
Certificate Fingerprint:
  92:48:09:A1:70:7A:AF:E1:30:55:EC:15:A3:0C:09:F0
```

Figura 2 - Conteúdo de Certificado Digital de um site da Internet

O usuário deve verificar a autenticidade do certificado, ou seja, se o mesmo foi emitido para o site da instituição que se deseja acessar. Para tanto, as seguintes informações devem ser checadas:

- Endereço eletrônico do site;
- Nome da instituição (dona do certificado);
- Prazo de validade do certificado.

Um certificado digital é considerado aceito a partir de sua primeira utilização, ou após haver decorrido o prazo pré-estipulado para sua rejeição. Um caso pode ocorrer ao entrar pela primeira vez em um site que utiliza conexão segura, quando o browser apresenta uma janela pedindo para confirmar o recebimento de um novo certificado. Neste caso, é necessário verificar se os dados do certificado correspondem realmente à instituição que se deseja acessar e se o browser reconheceu a Autoridade Certificadora que emitiu o certificado.

Entretanto, no caso de acessar regularmente um site com conexão segura o browser apresentar uma janela pedindo confirmação do recebimento de um novo certificado, muita atenção é necessária. É possível que a validade do certificado do site tenha vencido ou o certificado tenha sido revogado por outros motivos, e um novo certificado foi emitido para o site. Mas isto também pode significar um site falsificado que apresenta um certificado ilegítimo.

Formatos de certificado

Um certificado digital é basicamente uma coleção de informações de identificação junto com uma chave pública e assinado por uma terceira parte confiável para provar sua autenticidade. Um certificado digital pode ser um de um número de formatos diferentes. Destacam-se dois formatos de certificado diferentes:

- **Certificados PGP** (Pretty Good Privacy) - sistema de criptografia híbrido, que utiliza uma combinação das funcionalidades da criptografia assimétrica e a criptografia simétrica. É destinado a criptografia de e-mail pessoal. Algoritmos suportados: hashing: MD5, SHA-1, simétricos: CAST-128, IDEA e 3DES, assimétricos: RSA, Diffie-Hellman/DSS;
- **Certificados X.509** - Recomendação ITU-T, a especificação X.509 define o relacionamento entre as autoridades de certificação. Faz parte das séries X.500 de recomendações para uma estrutura de diretório global, baseada em nomes distintos para localização. Utilizado pelo S/MIME, IPSec, SSL/TLS e SET. Baseado em criptografia com chave pública (RSA) e assinatura digital (com hashing).

O Padrão X.509

Formato criado pelo ITU-T e ISO/IEC, que proporciona as informações necessárias para identificar o certificado digital, a especificação X.509 é um padrão que especifica o formato dos certificados digitais, de tal maneira que se possa amarrar firmemente um nome a uma chave pública, permitindo autenticação forte. Faz parte das séries X.500 de recomendações para uma estrutura de diretório global, baseadas em nomes distintos para localização.

O uso de certificados digitais e de criptografia deixa de ser uma opção e passa a ser uma necessidade em corporações que desejam fazer uso da praticidade da troca eletrônica de mensagens sem estarem expondo sua empresa aos problemas de autenticação e privacidade. Na ICP-Brasil utiliza-se certificados no padrão X-509 V3. Atualmente, os certificados digitais utilizam a versão 3 definida neste padrão ITU-T.

O padrão é descrito por diversas RFC's (Request for Comments) que são revisadas com freqüência. Destacam-se:

- RFC 2527 – Internet X.509 Public Key Infrastructure Certificate Policy and Certifications Practices Frame work;

- RFC 2560 - Internet X.509 Public Key Infrastructure Online Certificate Status Protocol (OCSP);
- RFC 2585 - Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP;
- RFC 3029 - Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols;
- RFC 3161 – Internet X.509 Public key Infrastructure: Time-Stamp Protocol (TSP);
- RFC 3279 - Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL);
- RFC 3280 - X.509 Internet Public Key Infrastructure Certificate and Certificate Revocation List (CRL);
- RFC 3779 - X.509 Extensions for IP Addresses and AS Identifiers;
- RFC 3820 - Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile;
- RFC 4055 - Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

Os certificados digitais foram inicialmente padronizados no esquema X.509. Das várias propostas de codificação de certificados, a mais conhecida, aceita e utilizada é a recomendação ITU-T X.509 v3.

A versão dos certificados digitais X.509 v3, apresenta informações obrigatórias e extensões (opcionais) conforme mostra a Figura 3. Assim, além das informações obrigatórias, a AC poderá acrescentar outras informações que achar pertinentes.

As extensões oferecem controles gerenciais e administrativos úteis para a autenticação com objetivos distintos. As extensões de certificados possuem uma função indicada por um valor padrão de Identificador de Objeto. Assim, os tipos de extensões possuem funções diferenciadas e podem ser do tipo crítica ou não-crítica:

- **Crítica** – não poderá ser ignorada pelo usuário e também limita o uso de assinaturas para favorecer a certificação. Este tipo de extensão deve ser padronizado. Exemplo: campo “cpf” em um certificado do tipo e-cpf;
- **Não-crítica** – pode ser ignorada pelo usuário de certificados. Exemplo: endereço do titular do certificado.

Cada extensão é assinada com um valor de verdadeiro ou falso de importância, determinada pela AC, baseado nas informações fornecidas pelo usuário no ato da solicitação do certificado. É este valor que determina se a extensão é crítica ou não-crítica. Algumas extensões do padrão X.509 v3:

- **Informações sobre Políticas e Chaves** – fornecem informações para identificar uma chave pública particular e a política usada na certificação (crítica para chave e não-crítica para políticas);

- **Atributo de Emissão e do sujeito** – fornece informações sobre os nomes e restringe a área dentro da qual os nomes das entidades devem estar localizados (extensão crítica);
- **Restrições de Caminho de Certificação** - possibilita que a AC imponha condições para evitar possíveis fraudes (crítica);
- **Extensões de LCR's (Listas de Certificados Revogados)** – fornecem informações sobre quais LCR's obter e onde (não crítica).

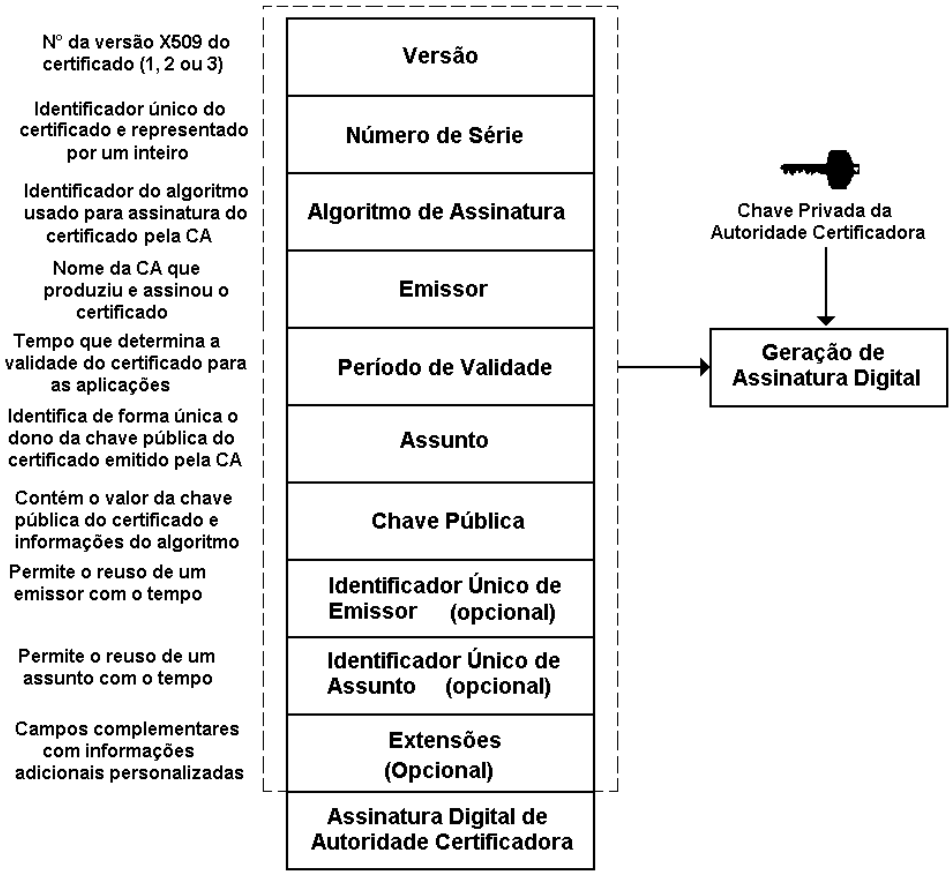

Figura 3 - Estrutura do Certificado X.509 v3

Com certificados X.509, a validação é sempre feita por uma Autoridade de Certificação ou alguém designado por uma CA. Tecnicamente, certificados X.509 criados para uma aplicação podem ser usados por qualquer aplicação que obedece X.509. Na prática, porém, existem algumas extensões para certificados X.509 que dificultam a aplicação do padrão ao nível global.

Um certificado X.509 é um conjunto padrão de campos contendo informações sobre um usuário ou dispositivo e suas correspondente chave pública. O padrão X.509 define qual informação vai no certificado e descreve como codificar isto (o formato dos dados).

Todos os certificados X.509 têm os seguintes dados:

- **Número da versão 509 do certificado** - identifica qual padrão é aplicado na versão do X.509 para este certificado, o que afeta qual informação pode ser especificada;
- **A chave pública do possuidor do certificado** - a chave pública, junto com um algoritmo de identificação que especifica a qual sistema de criptografia pertence a chave e quaisquer parâmetros associados;
- **O número de série do certificado** - a entidade (aplicação ou pessoa) que criou o certificado é responsável por neste um número de série para distinguir este de outros certificados. Esta informação é usada de várias maneiras; por exemplo, quando um certificado é revogado, seu número serial é colocado em uma Lista de Revogação de Certificados.
- **Identificação única do possuidor de certificado** (ou DN - *Distinguished Name* - nome distinguido). Este nome tem que ser único pela Internet. Um DN consiste em múltiplas subseções e pode parecer com algo do tipo: CN=Bob Allen, OU=Total Network Security Division, O=Network Associates, Inc., C=US (Estes se referem ao Nome Comum do assunto, Organizacional, Unidade, Organização, e País.)
- **O período de validade do certificado** - a data de inicio da validade do certificado / tempo e data de vencimento / tempo; indica quando o certificado expira.
- **O nome único do emissor do certificado** - o nome único da entidade que assinou o certificado. Esta normalmente é uma CA. Usando o certificado implica em confiar na entidade que assinou este certificado. (Note que em alguns casos, como raiz do certificado ou top-level da CA, o emissor assina seu próprio certificado).
- **Assinatura digital do emissor** - a assinatura que usa a chave privada da entidade que emitiu o certificado.
- **Identificador do Algoritmo de assinatura** - identifica o algoritmo usado pela CA para assinar o certificado.