1.Certificados digitais

1.1 Certificados digitais e seu ciclo de vida

Certificados digitais são documentos eletrônicos que contêm informações de identidade e chave pública de um indivíduo, organização ou dispositivo. Eles são emitidos por Autoridades Certificadoras (CAs) confiáveis dentro de uma Infraestrutura de Chaves Públicas (PKI).

O ciclo de vida dos certificados digitais pode ser dividido em várias etapas, desde a sua emissão até a sua expiração ou revogação. As principais fases do ciclo de vida dos certificados digitais são as seguintes:

- **Solicitação:** O ciclo de vida começa quando uma entidade, como um indivíduo, organização ou dispositivo, solicita um certificado digital a uma Autoridade Certificadora (CA). A solicitação pode incluir informações de identidade e detalhes sobre o uso pretendido do certificado.
- **Verificação:** Após receber a solicitação, a CA realiza uma verificação rigorosa da identidade do solicitante. Isso pode envolver a solicitação de documentos, validação de informações fornecidas e outros procedimentos para garantir que a identidade seja autêntica.
- **Emissão:** Uma vez que a CA tenha concluído a verificação, ela emite o certificado digital. O certificado contém informações como a chave pública do titular, nome, organização, data de emissão e período de validade. A CA também assina digitalmente o certificado para garantir sua autenticidade e integridade.
- **Distribuição:** O certificado emitido é então entregue ao titular do certificado. Isso pode ser feito por meio de download de um arquivo ou por outros meios seguros, como um token de hardware ou smart card. O titular é responsável por armazenar e proteger adequadamente o certificado e a chave privada correspondente.
- **Uso:** Durante a fase de uso, o certificado é aplicado em várias situações, como autenticação, criptografia e assinatura digital. Ele é apresentado a outras partes para verificar a identidade do titular e garantir a segurança das comunicações ou transações.
- **Renovação:** Os certificados digitais têm uma data de validade definida. Antes do vencimento, o titular pode solicitar a renovação do certificado à CA. Isso envolve um processo similar ao da solicitação inicial, com uma nova verificação da identidade do titular. A renovação garante a continuidade do uso do certificado sem interrupções.
- **Revogação:** Em certos casos, um certificado pode precisar ser revogado antes da data de expiração. Isso pode ocorrer se a chave privada for comprometida, se houver suspeita de uso indevido ou se a identidade do titular for comprometida. A revogação é registrada em uma Lista de Certificados Revogados (CRL) ou por meio de serviços de Verificação do Estado de Certificado Online (OCSP).
- **Expiração:** Após o término do período de validade, o certificado digital expira e não pode mais ser considerado válido para autenticação ou outras finalidades. O titular deve solicitar um novo certificado, caso ainda necessite de um.

2.Tipos comuns de certificados digitais

Existem vários tipos de arquivos que podem conter certificados digitais, cada um com suas características e finalidades específicas. Abaixo estão os principais tipos de arquivos de certificados digitais.

2.1 Arquivos PEM (Privacy Enhanced Mail)

Os arquivos PEM são um formato de texto baseado em ASCII (American Standard Code for Information Interchange) amplamente utilizado para armazenar certificados digitais. Eles possuem extensões como .pem, .crt ou .cer. Os arquivos PEM contêm certificados codificados em Base64, com marcações específicas para indicar o início e o fim do certificado. Eles podem conter certificados individuais ou certificados intermediários e raiz em um único arquivo.

2.2 Arquivos DER (Distinguished Encoding Rules)

Os arquivos DER são um formato binário para armazenar certificados digitais. Eles são uma representação codificada em binário dos certificados, seguindo as regras de codificação ASN.1 (Abstract Syntax Notation One). Os arquivos DER geralmente têm a extensão .der ou .cer. Ao contrário dos arquivos PEM, os arquivos DER não são codificados em texto legível.

2.3 Arquivos PFX/P12

Os arquivos PFX (Personal Information Exchange) ou P12 (PKCS#12) são formatos de arquivo que podem armazenar certificados digitais junto com suas chaves privadas correspondentes. Esses arquivos são protegidos por uma senha para garantir a segurança da chave privada. Eles podem ser usados para exportar e importar certificados digitais e chaves privadas entre diferentes sistemas e aplicativos.

2.4 Arquivos P7B/PKCS#7

Os arquivos P7B ou PKCS#7 são usados para armazenar certificados digitais em um formato compacto. Eles geralmente têm a extensão .p7b ou .p7c. Esses arquivos podem conter um ou mais certificados em um formato codificado em Base64, permitindo que sejam facilmente compartilhados e instalados em diferentes aplicativos.

2.5 Arquivo CRL (Certificate Revocation List)

Os arquivos CRL são usados para armazenar listas de certificados revogados. Eles contêm informações sobre certificados que foram revogados antes do término do período de validade. Os arquivos CRL geralmente são fornecidos em um formato binário ou em texto codificado em Base64.

2.6 Arquivos de container de chave

Além dos formatos mencionados acima, existem arquivos de container de chave específicos de sistemas operacionais ou aplicativos, como o Keychain no macOS e os Key Stores no Windows. Esses arquivos podem armazenar certificados digitais, juntamente com suas chaves privadas correspondentes, em um formato adequado ao sistema ou aplicativo em questão.

3.Tipos de certificados de servidor web

Um certificado de servidor garante a identidade de sites de comércio eletrônico ou qualquer tipo de site para o qual os usuários enviam dados que devem ser mantidos confidenciais. Um dos problemas da criptografia de chave pública e dos modelos de confiança é que qualquer pessoa pode configurar uma solução de PKI.

Também é simples registrar nomes de domínio com sons convincentes, como meu-banco-servidor.foo, onde o domínio "real" é meu-banco.foo. Se os usuários escolherem confiar em um certificado na crença ingênua de que ter um certificado torna um site confiável, eles podem se expor a fraudes.

Também houve casos de sites pouco respeitáveis obtendo certificados de ACs de terceiros que são automaticamente confiáveis pelos navegadores, que aparentemente validam suas identidades como instituições financeiras.

Certificados com diferentes níveis de classificação podem ser usados para fornecer níveis de segurança diferentes; por exemplo, um banco online requer maior segurança do que um site que coleta dados de marketing. Os tipos de certificados de servidor web são:

- **Certificado de Validação de Domínio (DV - Domain Validation):** Esse tipo de certificado é o mais básico e comumente usado. Ele apenas verifica se o solicitante do certificado possui controle sobre o domínio para o qual está solicitando o certificado. A validação é feita por meio de métodos simples, como responder a um e-mail enviado para o endereço de e-mail do domínio ou adicionando um registro DNS específico. Os certificados DV são rápidos de obter e geralmente têm um custo mais baixo.
- **Certificado de Validação Estendida (EV - Extended Validation):** Os certificados EV fornecem o mais alto nível de confiança aos usuários, pois passam por um processo de validação mais rigoroso. Além de verificar a propriedade do domínio, o solicitante do certificado deve passar por verificações detalhadas de identidade e autenticação da organização. Os certificados EV exibem informações adicionais na barra de endereços do navegador, como o nome da organização, fornecendo uma indicação clara de que o site é confiável. Esses certificados são amplamente utilizados por organizações que lidam com informações confidenciais, como instituições financeiras e comércio eletrônico.
- **Certificado de Organização Validada (OV - Organization Validation):** Os certificados OV também exigem uma validação mais rigorosa do que os certificados DV. Eles verificam a propriedade do domínio e realizam verificações adicionais para confirmar a identidade e a existência legal da organização. Esses certificados exibem informações da organização no certificado, fornecendo uma camada extra de confiança aos usuários que acessam o site. Os certificados OV são comumente usados por empresas e organizações que desejam transmitir credibilidade e confiança aos visitantes do site.

4.Outros tipos de certificados

Servidores web não são os únicos sistemas que precisam validar a identidade. Existem muitos outros tipos de certificados, projetados para diferentes propósitos.

4.1 Certificados de máquina/computador

Pode ser necessário emitir certificados para máquinas (servidores, PCs, smartphones e tablets), independentemente da função. Por exemplo, em um domínio Active Directory, certificados de máquina podem ser emitidos para Controladores de Domínio, servidores membros ou até mesmo estações de trabalho de clientes. Máquinas sem certificados válidos emitidos pelo domínio podem ser impedidas de acessar recursos de rede. Certificados de máquina podem ser emitidos para dispositivos de rede, como roteadores, switches e firewalls. O atributo SAN (Subject Alternative Name) e frequentemente o atributo CN (Common Name) devem ser configurados com o FQDN (Fully Qualified Domain Name) da máquina (nome do host e parte do domínio local).

4.2 Certificados de e-mail/usuário

Um certificado de email pode ser usado para assinar e criptografar mensagens de email, normalmente usando Extensões Seguras de Mensagens na Internet (S/MIME) ou Pretty Good Privacy (PGP). O endereço de email do usuário deve ser inserido como SAN e CN. Em uma rede local baseada em diretório, como o Windows Active Directory, pode haver a necessidade de uma variedade maior de tipos de certificados de usuário. Por exemplo, no AD existem modelos de certificados de usuário para usuários padrão, administradores, logon de cartão inteligente, usuários de agentes de recuperação e usuários de email do Exchange (com modelos separados para assinatura e criptografia). Cada modelo de certificado possui definições diferentes de uso de chave.

4.3 Certificados de assinatura de código

Um certificado de assinatura de código é emitido para um editor de software, após algum tipo de verificação de identidade e processo de validação pela AC. O editor então assina os executáveis ou DLLs que compõem o programa para garantir a validade de um aplicativo de software ou plug-in de navegador. Alguns tipos de ambientes de script, como o PowerShell, também podem exigir assinaturas digitais válidas. O CN é configurado com um nome de organização, como "CompTIA Development Services, LLC", em vez de um FQDN.

5.Arquitetura de Certificados Digitais

O arquivo que contém um certificado digital segue uma estrutura específica definida pela arquitetura X.509, que é um padrão amplamente adotado para certificados digitais. A arquitetura X.509 define a estrutura de um certificado digital e os formatos em que pode ser armazenado. A arquitetura básica do arquivo de certificado digital é:

- **Versão:** O campo "Versão" indica a versão do padrão X.509 utilizada para o certificado. Os valores mais comuns são 1, 2 e 3, correspondendo às versões X.509v1, X.509v2 e X.509v3, respectivamente.

- **Número de série:** O campo "Número de Série" identifica exclusivamente o certificado dentro da Autoridade Certificadora (CA) que o emitiu. Cada certificado possui um número de série único.
- **Algoritmo de assinatura do emitente:** Este campo indica o algoritmo de criptografia usado pela CA para assinar o certificado. Pode ser um algoritmo como RSA, DSA ou ECDSA.
- **Nome do emitente:** O campo "Nome do Emitente" identifica a CA que emitiu o certificado. Pode ser o nome da organização ou da entidade responsável pela emissão.
- **Período de validade:** Os campos "Validade a partir de" e "Validade até" indicam o período de tempo durante o qual o certificado é considerado válido. Após a data de validade, o certificado não deve ser confiado.
- **Nome do sujeito:** O campo "Nome do Sujeito" identifica o titular do certificado, ou seja, a entidade à qual o certificado foi emitido. Pode conter informações como o nome completo, nome da organização e outros atributos identificadores.
- **Chave pública:** O campo "Chave Pública" contém a chave pública correspondente à chave privada do titular do certificado. A chave pública é usada para operações criptográficas, como criptografia, verificação de assinaturas digitais e estabelecimento de chaves de sessão seguras.
- **Identificador de algoritmo de assinatura:** Este campo identifica o algoritmo de criptografia utilizado para assinar o certificado digital. É o algoritmo que verifica a autenticidade e a integridade do certificado.
- **Extensões:** O campo "Extensões" é opcional e pode conter informações adicionais sobre o certificado, como restrições de uso, política de certificação e informações de autoridade de certificação intermediária.
- **Assinatura digital:** O campo "Assinatura Digital" contém a assinatura digital do certificado, que é gerada pela CA usando sua chave privada. A assinatura garante a autenticidade e a integridade do certificado.

6.Atributos do Nome do Assunto (Subject Name Attributes)

Os Atributos do Nome do Assunto (Subject Name Attributes) em PKI (Infraestrutura de Chaves Públicas) são informações contidas nos certificados digitais que identificam o sujeito ou entidade para a qual o certificado foi emitido.

Esses atributos fornecem detalhes sobre a identidade do titular do certificado, como nome, organização, localidade, país, endereço de e-mail, entre outros. Os Atributos do Nome do Assunto são usados para verificar a identidade do titular do certificado durante o processo de autenticação. Eles desempenham um papel fundamental na estabelecimento de confiança na comunicação segura por meio de chaves públicas.

7.Nome Comum - Common Name (CN)

Refere-se ao nome comum do sujeito ou entidade para a qual o certificado foi emitido. O CN é usado para identificar de forma exclusiva o titular do certificado e é um dos principais componentes usados na verificação da identidade durante o processo de autenticação.

O CN geralmente contém o nome legal ou o nome de domínio totalmente qualificado (FQDN) do titular do certificado. No caso de um certificado de servidor web, o CN normalmente é o domínio do site para o qual o certificado foi emitido.

O CN desempenha um papel crucial na verificação da identidade do titular do certificado, especialmente em situações em que um certificado é apresentado para autenticação. Os sistemas e aplicativos que dependem de certificados digitais podem verificar se o CN no certificado corresponde ao nome de domínio do servidor com o qual estão se comunicando, garantindo assim a autenticidade e integridade das comunicações.

8.Nome Alternativo do Assunto - Subject Alternative Name (SAN)

Subject Alternative Name (SAN) é um campo presente em certificados digitais que permite especificar nomes alternativos para identificar o sujeito ou entidade do certificado, além do Common Name (CN). O SAN é usado principalmente em certificados SSL/TLS para suportar diferentes domínios ou subdomínios associados a um único certificado.

A inclusão do SAN em um certificado digital permite que ele seja válido para múltiplos domínios, o que é especialmente útil em cenários como certificados wildcard, onde um único certificado pode ser aplicado a todos os subdomínios de um domínio principal.

O SAN também pode ser utilizado para incluir domínios adicionais que estão associados ao mesmo serviço ou entidade, permitindo que todos os domínios sejam validados em um único certificado.