1.Certificados digitais

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:

1.1 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.

1.2 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.

1.3 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.

1.4 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.

1.5 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.

1.6 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.

1.7 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).

1.8 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.

2.1 Arquivos PEM

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

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

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.

3.Autoridades Certificadoras (CAs)

O principal papel das ACs é verificar a identidade dos solicitantes de certificados e garantir que as chaves públicas contidas nesses certificados sejam legítimas. Isso é feito por meio da verificação de documentos e informações pessoais dos usuários, como o uso de criptografia assimétrica.

Inclui emitir certificados digitais para indivíduos, organizações ou dispositivos, garantindo que os certificados sejam emitidos de acordo com as políticas de certificação e diretrizes estabelecidas. As políticas de certificação são documentos que estabelecem os procedimentos e diretrizes para a emissão, validação, revogação e gerenciamento dos certificados digitais pelas Autoridades Certificadoras. Elas são fundamentais para garantir a consistência e a confiabilidade dos processos envolvidos. **Além disso, a AC pode oferecer serviços adicionais, como renovação de certificados, emissão de certificados de recuperação e serviços de assinatura digital**.

Uma AC é responsável por gerenciar os servidores ou repositórios que armazenam e administram os certificados emitidos. Isso inclui a implementação de medidas de segurança para proteger os certificados contra acessos não autorizados, gerenciamento de backups para garantir a disponibilidade contínua dos certificados e implementação de políticas de retenção de dados. Além disso, a AC pode ser responsável por fornecer serviços de busca e recuperação de certificados, permitindo que os usuários acessem facilmente os certificados necessários.

A gestão do ciclo de vida das chaves e certificados é uma tarefa crítica para uma AC. Isso inclui a geração segura de chaves criptográficas, emissão de certificados, renovação, revogação e expiração dos mesmos. A AC deve implementar um processo eficiente para lidar com a revogação de certificados inválidos, seja devido a perda de confidencialidade da chave privada, comprometimento da identidade do titular do certificado ou outros motivos de revogação. A revogação garante que os certificados inválidos não possam ser utilizados indevidamente, mantendo a segurança e a integridade da PKI. **A AC é responsável por manter e atualizar as listas de revogação de certificados** (CRLs) **ou fornecer serviços de verificação em tempo real, como o Protocolo de Status de Certificado Online** (OCSP).

3.1 AC única

Na AC Única, todos os usuários confiam nos certificados emitidos por essa autoridade central. Isso significa que, para estabelecer a confiança em um certificado, os usuários devem confiar na AC única que emitiu o certificado. Qualquer entidade que deseje verificar a autenticidade de um certificado digital pode verificar a cadeia de certificados até a AC única. Esse modelo é relativamente simples de ser implementado, pois envolve apenas uma AC e não requer coordenação entre várias autoridades. No entanto, também apresenta alguns desafios e riscos.

3.2 AC hierárquica

No modelo hierárquico, uma única AC (chamada de raiz) **emite certificados para várias ACs intermediárias. As ACs intermediárias emitem certificados para os assuntos** (entidades finais). Esse modelo tem a vantagem de permitir que diferentes ACs intermediárias sejam configuradas com diferentes políticas de certificado, permitindo que os usuários percebam claramente para que serve um determinado certificado.

Cada certificado de folha pode ser rastreado até a AC raiz ao longo do caminho de certificação. Isso também é conhecido como encadeamento de certificados ou cadeia de confiança.

O certificado da raiz é autoassinado. No modelo hierárquico, a raiz ainda é um único ponto de falha. Se a raiz estiver danificada ou comprometida, toda a estrutura colapsa. No entanto, para mitigar isso, o servidor raiz pode ser desconectado, pois a maioria das atividades regulares da AC é realizada pelos servidores das ACs intermediárias.

3.3 AC *online* x AC *offline*

Uma AC online está disponível para aceitar e processar solicitações de assinatura de certificados, publicar listas de revogação de certificados e realizar outras tarefas de gerenciamento de certificados. Devido ao alto risco representado pela comprometimento da AC raiz, uma configuração segura envolve tornar a raiz uma AC offline. Isso significa que ela é desconectada de qualquer rede e geralmente é mantida desligada. A AC raiz precisará ser conectada para adicionar ou atualizar ACs intermediárias.

3.4 AC raiz (*Root Certification Authority*)

A Autoridade Certificadora Raiz (Root CA) **é o nível mais alto na hierarquia de certificação**. Ela emite certificados digitais para outras ACs intermediárias ou diretamente para entidades finais. O certificado raiz é autoassinado, ou seja, é emitido pela própria AC raiz e não requer validação por uma autoridade externa. O certificado raiz é confiável pelos usuários e estabelece a base de confiança

para toda a infraestrutura de chaves públicas (PKI). A AC raiz é responsável por emitir e revogar certificados intermediários, além de garantir a integridade e segurança da PKI.

3.5 AC intermediária

A Autoridade Certificadora Intermediária é uma AC secundária que obtém certificados diretamente da AC raiz ou de outras ACs intermediárias de níveis superiores. Ela emite certificados para entidades finais, como usuários, servidores e dispositivos, e atua como um elo intermediário entre a AC raiz e as entidades finais. As ACs intermediárias fornecem maior escalabilidade à PKI, permitindo a emissão de certificados em grande quantidade. Elas também podem ser organizadas em diferentes níveis, formando uma hierarquia de certificação.

3.6 CSR e RA

O registro é o processo pelo qual os usuários finais criam uma conta com a AC e são autorizados a solicitar certificados. Os processos exatos pelos quais os usuários são autorizados e sua identidade é comprovada são determinados pela implementação da AC. Por exemplo, em uma rede do Windows Active Directory, os usuários e dispositivos frequentemente podem se registrar automaticamente na AC apenas autenticando-se no Active Directory.

As ACs comerciais podem realizar uma série de testes para garantir que um sujeito seja quem ele ou ela afirma ser. É do interesse da AC garantir que ela emita certificados apenas para usuários legítimos, caso contrário, sua reputação será prejudicada.

Quando um sujeito deseja obter um certificado, ele preenche uma solicitação de assinatura de certificado (CSR, na sigla em inglês) e a envia para a AC. **A CSR é um arquivo Base64 ASCII que contém as informações que o sujeito deseja usar no certificado, incluindo sua chave pública**.

A AC revisa o certificado e verifica se as informações são válidas. Para um servidor da web, isso pode significar simplesmente verificar se o nome do sujeito e o nome de domínio totalmente qualificado (FQDN, na sigla em inglês) são idênticos e verificar se a CSR foi iniciada pela pessoa responsável administrativamente pelo domínio, conforme identificado nos registros WHOIS do domínio. Se a solicitação for aceita, a AC assina o certificado e o envia para o sujeito.

A função de registro pode ser delegada pela AC para uma ou mais autoridades de registro (RAs, na sigla em inglês). **Essas entidades realizam a verificação de identidade e enviam CSRs em nome dos usuários finais, mas elas não assinam nem emitem certificados efetivamente**.

Em conclusão, as Autoridades de Registro são responsáveis por verificar a identidade dos solicitantes de certificados e coletar as informações necessárias para a emissão de certificados. As Solicitações de Assinatura de Certificado (CSRs) são os documentos gerados pelos solicitantes que contêm as informações necessárias para a criação do certificado. Esses dois elementos desempenham papéis cruciais na PKI, garantindo a segurança e autenticidade dos certificados emitidos.