Módulo 9 - Aulas 1 e 2

Módulo 9: Infraestrutura de Chaves Públicas e Blockchain

Aula 1: Autoridades certificadoras

Objetivos

- [x] Compreender o papel das Autoridades Certificadoras na infraestrutura de chaves públicas (PKI).
- [x] Identificar os diferentes tipos de Autoridades Certificadoras, desde as ACs raiz até as intermediárias, e compreender a hierarquia de confiança estabelecida entre elas.
- [x] Familiarizar-se com o processo de emissão, validação, revogação e renovação de certificados digitais, assim como com as políticas de certificação e as considerações de segurança associadas ao trabalho das Autoridades Certificadoras.

Conceitos

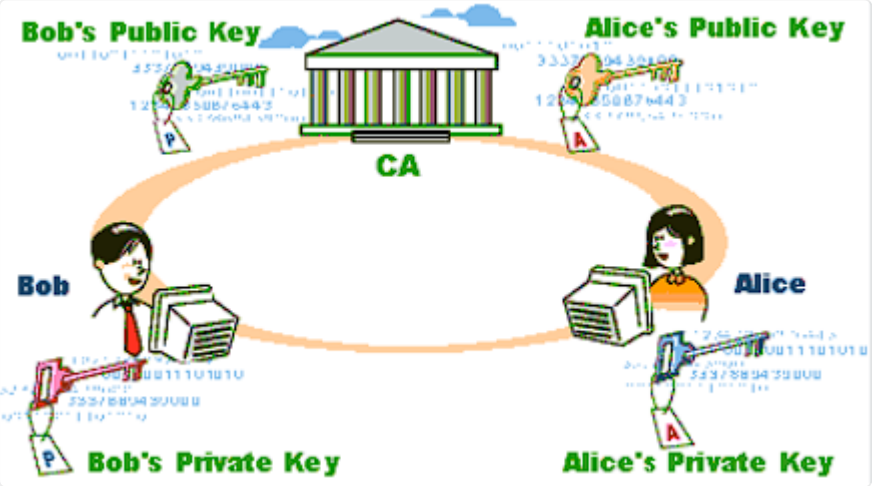
- [x] Autoridades Certificadoras (ACs).
- [x] Certificados Digitais.
- [x] Infraestrutura de Chaves Públicas (PKI).

Introdução

Nesta aula, mergulharemos no mundo das Autoridades Certificadoras (ACs) e exploraremos seu papel fundamental na infraestrutura de chaves públicas (PKI). As

ACs desempenham um papel crucial na emissão e validação de certificados digitais, garantindo a autenticidade e a integridade das informações transmitidas eletronicamente. Ao entender o funcionamento das ACs, você estará capacitado a compreender como os certificados digitais são emitidos, validados e utilizados em diversas aplicações.

Exploraremos os diferentes tipos de Autoridades Certificadoras, desde as ACs raiz até as intermediárias, compreendendo suas responsabilidades e a hierarquia de confiança estabelecida entre elas. Além disso, analisaremos a estrutura de um certificado digital e as informações essenciais presentes nele, como o nome do titular, a chave pública e o período de validade. Compreenderemos o processo de emissão e validação de certificados, assim como as medidas de revogação e renovação desses documentos.



Autoridade Certificadora.

Public Key Infrastructure - PKI

A Infraestrutura de Chaves Públicas (PKI - Public Key Infrastructure) é um conjunto de tecnologias, políticas e procedimentos que são usados para estabelecer e gerenciar a segurança em ambientes digitais. Ela é baseada na criptografia assimétrica, que utiliza um par de chaves criptográficas: uma chave pública e uma chave privada.

A PKI permite que diferentes partes em um ambiente digital se autentiquem mutuamente, garantindo a confidencialidade, integridade, autenticidade e não

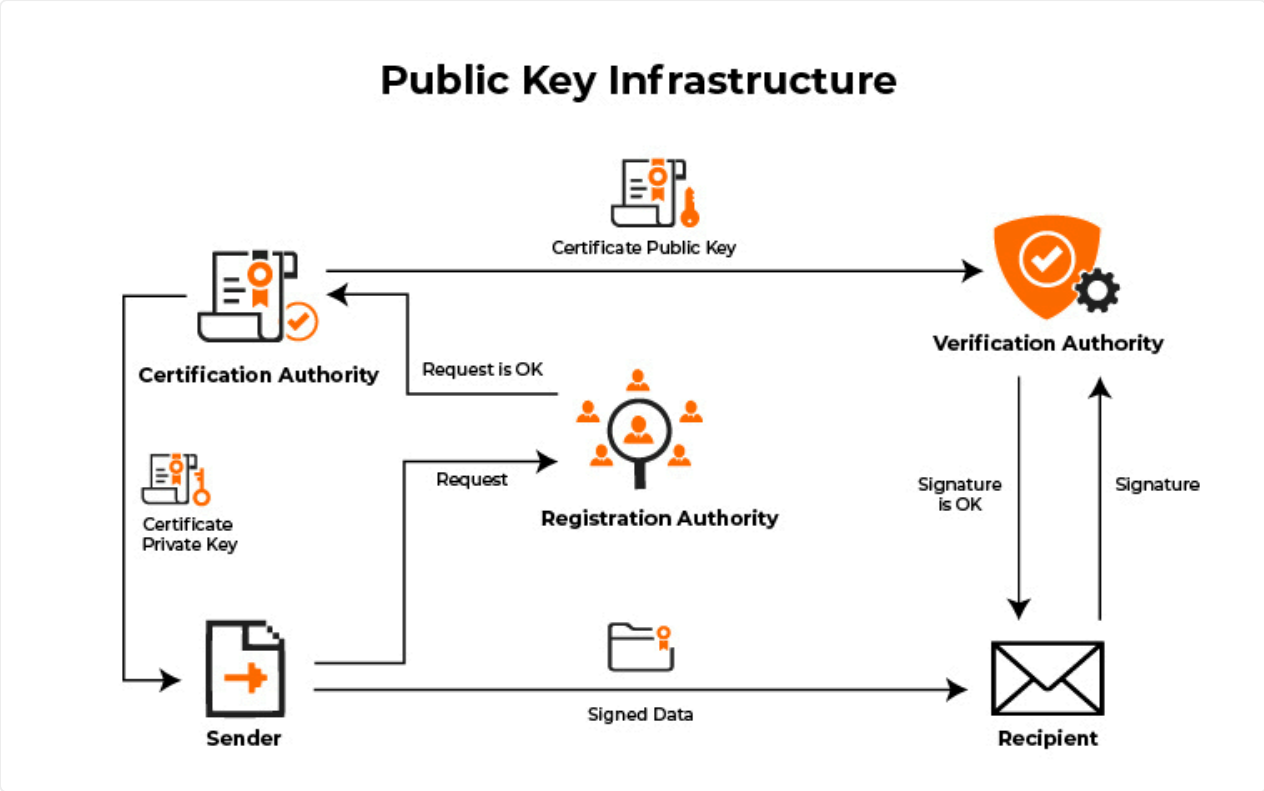
repúdio das informações transmitidas. Ela é amplamente utilizada em transações online, comunicações seguras, assinaturas digitais e identificação eletrônica.

Chave pública e chave privada em PKI

Em uma Infraestrutura de Chaves Públicas (PKI), a chave pública e a chave privada são elementos essenciais da criptografia assimétrica. Essa forma de criptografia utiliza um par de chaves criptográficas que estão matematicamente relacionadas, mas têm funções distintas.

1. **Chave pública**: A chave pública é uma chave criptográfica que pode ser divulgada e compartilhada livremente com outras partes. Ela é usada para criptografar informações ou verificar assinaturas digitais. A chave pública é derivada da chave privada correspondente por meio de algoritmos matemáticos específicos. Quando alguém deseja enviar informações confidenciais para um destinatário, essa pessoa utiliza a chave pública do destinatário para criptografar os dados antes de enviá-los. Somente a chave privada correspondente ao par de chaves pode descriptografar as informações criptografadas com a chave pública correspondente.
2. **Chave privada**: A chave privada é a contraparte da chave pública e é mantida em sigilo pelo seu proprietário. Ela não é divulgada nem compartilhada com outras partes. A chave privada é usada para descriptografar informações criptografadas com a chave pública correspondente ou para criar assinaturas digitais. Quando alguém deseja enviar uma assinatura digital para outra parte, essa pessoa utiliza sua chave privada para assinar digitalmente os dados. A assinatura digital é um valor criptográfico exclusivo que comprova a autenticidade e integridade dos dados. Para verificar a assinatura digital, qualquer pessoa com acesso à chave pública correspondente pode usar essa chave para verificar a autenticidade da assinatura e a integridade dos dados.

A relação entre as chaves públicas e privadas com os certificados digitais é estabelecida por meio das Autoridades Certificadoras (CAs). Os certificados digitais são documentos eletrônicos emitidos pelas CAs confiáveis que vinculam uma chave pública a uma identidade específica (como uma pessoa, organização ou dispositivo). O certificado digital contém informações como nome, organização, data de emissão e validade, além da chave pública do titular do certificado.



Infraestrutura de Chaves Públicas (PKI).

Autoridades Certificadoras (ACs) em PKI

As Autoridades Certificadoras (ACs) desempenham um papel fundamental na infraestrutura de chaves públicas (PKI) ao serem responsáveis por emitir, validar e revogar certificados digitais. Elas atuam como entidades confiáveis que garantem a autenticidade e integridade das informações transmitidas eletronicamente.

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. As funções de uma AC são as seguintes:

- Fornecer uma variedade de serviços de certificado úteis: 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.

- Garantir a validade e identidade dos certificados solicitados: A AC desempenha um papel fundamental na validação da identidade dos solicitantes de certificados. Antes de emitir um certificado, a AC realiza um processo de registro, no qual verifica a identidade do solicitante e garante sua autenticidade. Isso pode envolver a verificação de documentos de identificação, realização de entrevistas ou uso de outras formas de autenticação. Ao garantir a validade dos certificados e a identidade dos titulares, a AC estabelece a confiança na cadeia de certificados e na autenticidade das transações digitais.
- Estabelecer confiança na AC por parte dos usuários: A confiança desempenha um papel fundamental em uma infraestrutura de chaves públicas (PKI). A AC é responsável por estabelecer essa confiança, tanto por parte dos usuários quanto por parte das autoridades governamentais, regulatórias e das empresas. Isso é alcançado por meio da adesão a padrões de segurança e práticas recomendadas, conformidade com regulamentações e políticas, e realização de auditorias e certificações de segurança. Ao demonstrar sua confiabilidade e segurança, a AC conquista a confiança dos usuários e das partes interessadas, o que é essencial para o funcionamento efetivo da PKI.
- Gerenciar os servidores (repositórios): 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.
- Realizar a gestão do ciclo de vida das chaves e certificados: 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).

Modelos de Confiança da PKI

O modelo de confiança é um conceito crítico da PKI e mostra como os usuários e diferentes ACs podem confiar uns nos outros. Os modelos de confiança em PKI são:

AC Única

Uma Autoridade Certificadora (AC) Única em uma Infraestrutura de Chaves Públicas (PKI) é um modelo em que uma única entidade é responsável por emitir todos os certificados digitais dentro de um sistema. Nesse modelo, a AC única desempenha o papel central de confiança e é a única fonte de autoridade para validar a identidade dos solicitantes de certificados e emitir os certificados correspondentes.

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. Por exemplo, se a AC única for comprometida, todo o sistema de PKI será afetado e a confiança nos certificados emitidos pela AC será comprometida. Além disso, a AC única pode se tornar um ponto único de falha e um alvo atraente para ataques maliciosos. Devido aos riscos associados a uma AC única, muitas implementações de PKI adotam modelos hierárquicos

Hierárquico (AC Intermediária)

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.

Outro problema é que há oportunidades limitadas para a intercertificação, ou seja, confiar na AC de outra organização. Duas organizações podem concordar em compartilhar uma AC raiz, mas isso levaria a dificuldades operacionais que aumentariam conforme mais organizações aderissem. Na prática, a maioria dos clientes é configurada para confiar em várias ACs raiz.

Hierarquia de mercado.

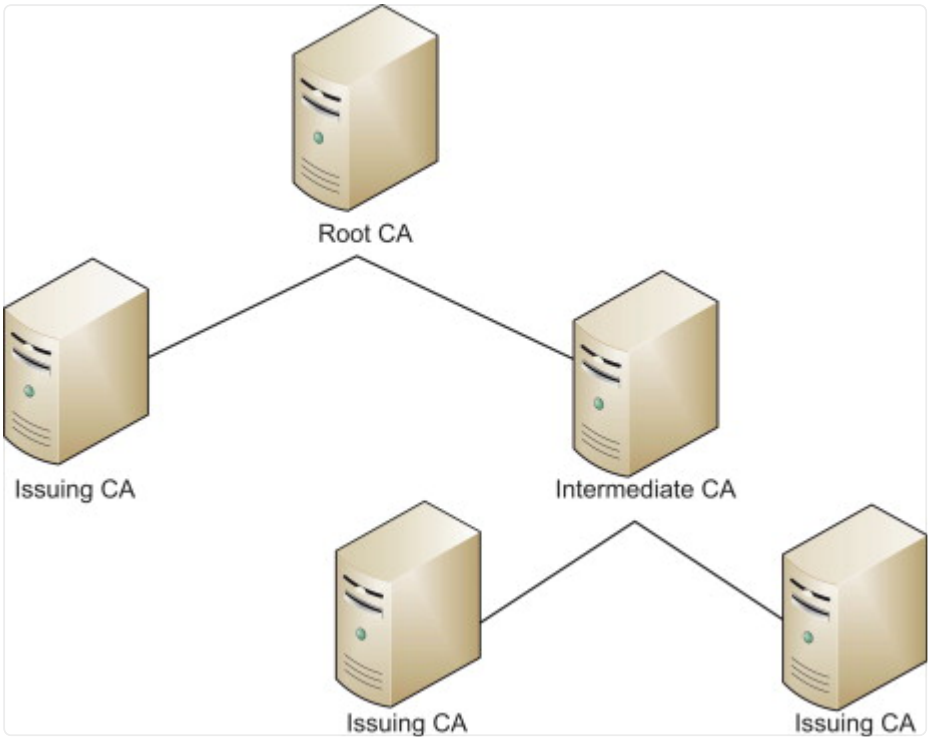
AC Online x AC Offline

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.

Tipos de ACs

As ACs são classificadas em:

1. Autoridade Certificadora 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.
2. Autoridade Certificadora Intermediária (Intermediate Certification Authority): 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.

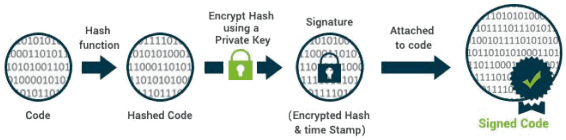


Certificadora Raiz e Intermediária.

3. Autoridade Certificadora Comercial (Commercial Certification Authority): A Autoridade Certificadora Comercial é uma AC operada por uma entidade comercial ou organização privada. Ela emite certificados digitais para entidades finais, como empresas, indivíduos ou dispositivos, com o objetivo de fornecer garantias de autenticidade, integridade e confidencialidade nas transações online. As ACs comerciais são amplamente reconhecidas e confiáveis pelos navegadores e aplicativos, permitindo que os usuários confiem nas identidades e criptografia utilizadas pelos sites e serviços online.
4. Autoridade Certificadora de Domínio (Domain Certification Authority): A Autoridade Certificadora de Domínio emite certificados para autenticar e proteger domínios de sites na Internet. Esses certificados são usados para estabelecer uma conexão segura entre o navegador do usuário e o servidor web, garantindo a criptografia das informações transmitidas. Eles são usados principalmente em protocolos como HTTPS para proteger a privacidade e a integridade dos dados durante a comunicação entre o cliente e o servidor. Os certificados de domínio são verificados por navegadores e outros aplicativos para garantir que o site seja autêntico e confiável.
5. Autoridade Certificadora de Email (Email Certification Authority): A Autoridade Certificadora de Email emite certificados digitais para autenticar e proteger as comunicações de e-mail. Esses certificados são usados para assinar digitalmente e criptografar mensagens de e-mail, garantindo a autenticidade do remetente, a integridade da mensagem e a confidencialidade das informações.

Eles permitem que os usuários verifiquem a origem e a integridade dos e-mails recebidos, bem como criem assinaturas digitais para provar a autenticidade de seus próprios e-mails.

6. Autoridade Certificadora de Assinatura de Código (Code Signing Certification Authority): A Autoridade Certificadora de Assinatura de Código emite certificados digitais para desenvolvedores de software assinarem seus aplicativos, scripts e código. Esses certificados são usados para garantir a autenticidade e a integridade do código distribuído, permitindo que os usuários verifiquem se o software foi alterado ou adulterado desde a sua assinatura. Isso ajuda a prevenir a execução de código malicioso ou não autorizado em dispositivos e sistemas.



7. Autoridade Certificadora de Máquina/Computador (Machine/Computer Certification Authority): A Autoridade Certificadora de Máquina emite certificados digitais para autenticar e proteger máquinas, como servidores, computadores, smartphones e tablets. Esses certificados são usados para estabelecer a identidade confiável das máquinas em uma rede e garantir a comunicação segura entre elas. Eles podem ser usados em cenários como autenticação de máquina em uma rede local ou autenticação de dispositivos em uma infraestrutura de IoT (Internet das Coisas).
8. Autoridade Certificadora de Dispositivo (Device Certification Authority): A Autoridade Certificadora de Dispositivo emite certificados digitais para dispositivos de hardware, como smartphones, tablets, dispositivos IoT e outros dispositivos incorporados. Esses certificados são usados para autenticar e proteger a comunicação entre os dispositivos e garantir a integridade dos dados transmitidos. Eles permitem que os dispositivos se autentiquem em redes, serviços e aplicativos, ajudando a prevenir acessos não autorizados e ataques.
9. Autoridade Certificadora de Identidade (Identity Certification Authority): A Autoridade Certificadora de Identidade emite certificados digitais para autenticar a identidade de indivíduos. Esses certificados são usados em cenários como autenticação em serviços online, assinaturas digitais, acesso a recursos protegidos e transações eletrônicas seguras. Eles garantem que a identidade declarada por um indivíduo seja verificada e confiável, permitindo a criação de identidades digitais seguras.
10. Autoridade Certificadora de Servidor (Server Certification Authority): A Autoridade Certificadora de Servidor emite certificados digitais para autenticar

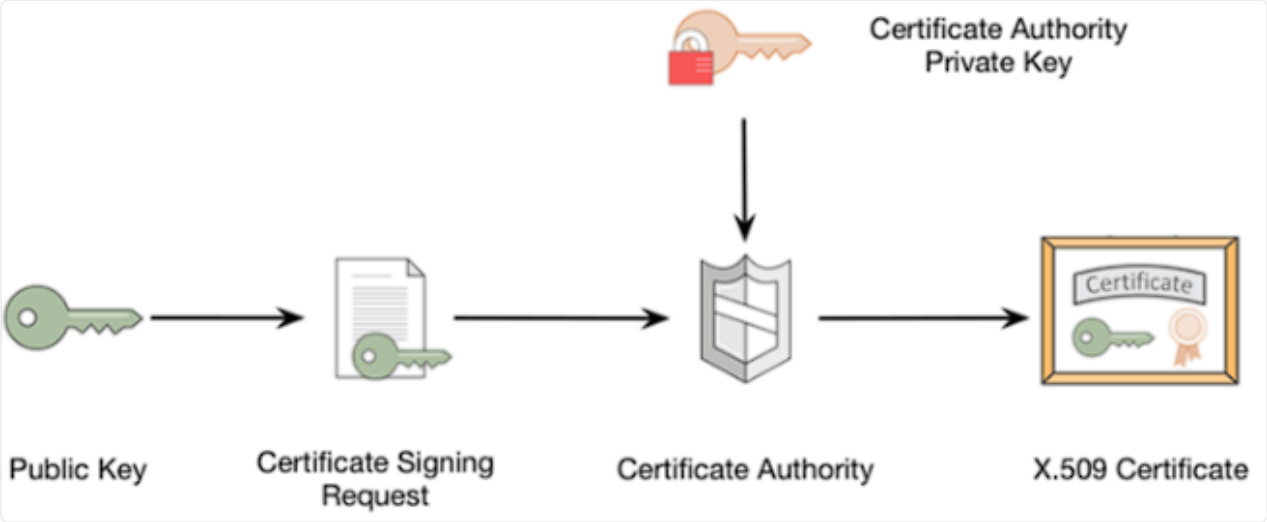
e proteger servidores e serviços online. Esses certificados são usados para estabelecer a identidade confiável de um servidor, garantindo que os clientes possam verificar a autenticidade do servidor com o qual estão se comunicando. Eles são amplamente utilizados em protocolos como HTTPS, SMTPS e LDAPS para garantir conexões seguras e proteger a privacidade das informações transmitidas entre os clientes e os servidores.

Autoridades de Registro (RA) e Solicitações de Assinatura de Certificado (CSRs)

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.



CSR.

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.

Autoridades Certificadoras no Brasil

No Brasil, existem várias Autoridades Certificadoras (ACs) que desempenham um papel fundamental na emissão e validação de certificados digitais. Essas ACs são responsáveis por estabelecer a confiança e a autenticidade dos certificados utilizados em transações eletrônicas, assinaturas digitais e outros serviços que exigem segurança e integridade.

No país, as ACs são regulamentadas pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), que é uma iniciativa do Governo Federal para garantir a segurança e a interoperabilidade dos certificados digitais no Brasil. A ICP-Brasil

define os requisitos técnicos e legais que as ACs devem cumprir para operar de acordo com os padrões estabelecidos. As ACs no Brasil podem ser classificadas em três categorias:

1. ACs Raiz: São as entidades máximas da ICP-Brasil e emitem os certificados raiz, também conhecidos como certificados de confiança. Esses certificados são usados para assinar os certificados intermediários das ACs Subordinadas, garantindo a cadeia de confiança na hierarquia da ICP-Brasil.
2. ACs Subordinadas: São as ACs que emitem os certificados intermediários, também chamados de certificados de emissão. Esses certificados são utilizados para assinar os certificados emitidos para os usuários finais, como pessoas físicas e jurídicas. As ACs Subordinadas são supervisionadas e auditadas pelas ACs Raiz.
3. ACs Autorizadas: São as ACs que possuem autorização para emitir certificados digitais, mas não estão diretamente subordinadas às ACs Raiz. Elas são auditadas e supervisionadas pelas ACs Subordinadas, que garantem a conformidade com as normas da ICP-Brasil.

Infraestrutura de Chaves Públicas Brasileira.

Entre as ACs no Brasil, destacam-se algumas entidades como a Serasa Experian, Certisign, Valid Certificadora Digital, AC Notarial, entre outras. Cada uma dessas ACs possui suas próprias políticas de emissão de certificados e oferecem serviços específicos para atender às necessidades de diferentes setores e usuários.

Certisign.

Instituto Nacional de Tecnologia da Informação (ITI)

O Instituto Nacional de Tecnologia da Informação (ITI) é uma autarquia federal brasileira responsável por coordenar e supervisionar a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). O ITI foi criado em 2001 com o objetivo de promover a segurança e a confiança nos meios eletrônicos utilizados para transações digitais no país. Dentre as principais atribuições do ITI estão:

- Coordenar a ICP-Brasil: O ITI é responsável por coordenar todas as atividades relacionadas à ICP-Brasil, incluindo a definição de políticas, normas e padrões técnicos para a emissão, gestão e validação dos certificados digitais.
- Fiscalizar as Autoridades Certificadoras (ACs): O ITI possui poderes de fiscalização e controle sobre as ACs, verificando o cumprimento das normas estabelecidas pela ICP-Brasil. Isso inclui auditorias regulares, análise dos processos de emissão de certificados e garantia da segurança e integridade dos serviços prestados pelas ACs.
- Emitir certificados digitais: O ITI é responsável por emitir os certificados digitais das ACs Raiz, que são utilizados para assinar os certificados intermediários das ACs Subordinadas. Esses certificados garantem a cadeia de confiança na hierarquia da ICP-Brasil.
- Promover a interoperabilidade: O ITI trabalha para garantir a interoperabilidade dos certificados digitais emitidos pelas ACs, permitindo que sejam reconhecidos e aceitos em diferentes sistemas e aplicações no âmbito nacional e internacional.

Além disso, o ITI também desempenha um papel importante na elaboração de políticas de segurança da informação, no fomento à pesquisa e ao desenvolvimento de tecnologias relacionadas à certificação digital, e na representação do Brasil em fóruns e organizações internacionais que tratam do tema.

Instituto Nacional de Tecnologia da Informação.

Conclusão

Nesta aula, exploramos o papel fundamental das Autoridades Certificadoras (ACs) na infraestrutura de chaves públicas (PKI). As ACs desempenham diversas funções, desde fornecer serviços de certificação até garantir a validade dos certificados emitidos. Além disso, elas estabelecem a confiança dos usuários, autoridades governamentais e empresas na PKI. A hierarquia de confiança e a cadeia de certificados são elementos essenciais para garantir a autenticidade e a segurança dos certificados emitidos pelas ACs. Também exploramos diferentes tipos de ACs, como ACs raiz, ACs intermediárias e ACs comerciais. Compreender o funcionamento e a importância das ACs é essencial para utilizar de forma eficaz os Certificados Digitais e garantir a confiança nas comunicações e transações eletrônicas.

> Parabéns pelo seu esforço e dedicação em concluir a aula sobre Autoridades Certificadoras! Você adquiriu um conhecimento valioso sobre os diferentes tipos de ACs e sua importância na infraestrutura de chaves públicas (PKI). Continue se aprofundando nesse tema, pois ele desempenha um papel fundamental na segurança e autenticidade das comunicações digitais.

Aula 2: Certificado Digital

Objetivos

- [ ] Compreender o papel e a importância da Infraestrutura de Chaves Públicas (PKI) na segurança digital.
- [ ] Explorar os conceitos básicos da criptografia assimétrica e sua aplicação na certificação digital.
- [ ] Entender o processo de emissão, validação e gerenciamento de certificados digitais, incluindo a revogação e renovação quando necessário.

Conceitos

- [ ] Infraestrutura de Chaves Públicas (PKI).
- [ ] Criptografia assimétrica para certificados digitais.
- [ ] Certificados digitais.

Introdução

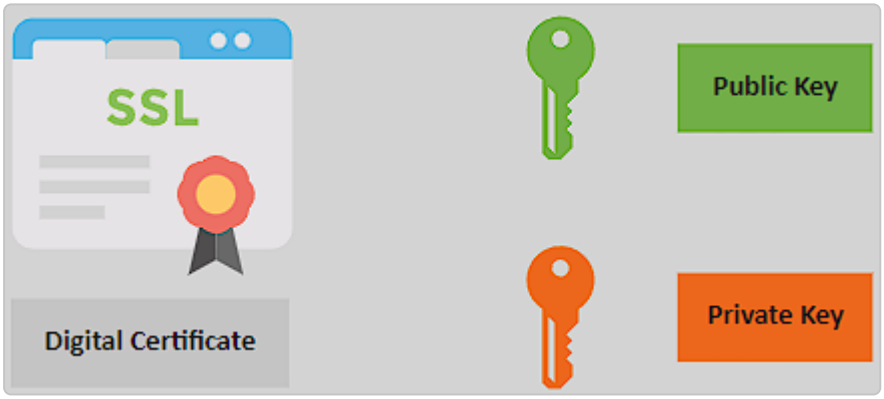
Nesta aula, exploraremos o conceito de certificados digitais, que são documentos eletrônicos que contêm informações de identidade e chave pública de uma entidade, organização ou dispositivo. Esses certificados são emitidos por Autoridades Certificadoras confiáveis dentro de uma Infraestrutura de Chaves Públicas (PKI).

O ciclo de vida dos certificados digitais envolve várias etapas, desde a solicitação até a expiração ou revogação do certificado. Vamos discutir as principais fases desse ciclo, como a solicitação, verificação, emissão, distribuição, uso, renovação, revogação e expiração dos certificados. Além disso, abordaremos os tipos comuns de arquivos que podem conter certificados digitais, como os arquivos PEM, DER, PFX/P12, P7B/PKCS#7 e CRL. Cada um desses formatos possui características específicas e é utilizado para diferentes finalidades.

Focaremos também nos tipos de certificados de servidor web, como o Certificado de Validação de Domínio (DV), o Certificado de Validação Estendida (EV) e o

Certificado de Organização Validada (OV). Cada tipo de certificado oferece diferentes níveis de validação e confiança, adequados para diversas situações e necessidades de segurança. Além dos certificados de servidor web, exploraremos outros tipos de certificados, como os certificados de máquina/computador, certificados de email/usuário e certificados de assinatura de código. Cada um desses certificados desempenha um papel específico na validação de identidade em diferentes contextos.

Por fim, discutiremos a arquitetura de certificados digitais definida pelo padrão X.509, que estabelece a estrutura e os formatos dos arquivos de certificado. Veremos os principais campos presentes em um certificado digital, como a versão, número de série, algoritmo de assinatura do emitente, período de validade, nome do sujeito e chave pública.



Certificado Digital.

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:

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.
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.
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.
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.
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.
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.
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).
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.

O ciclo de vida dos certificados digitais pode variar em detalhes, dependendo das políticas e procedimentos específicos da CA e das regulamentações aplicáveis.

Tipos comuns de Certificados Digitais

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

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.

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.

Arquivos PFX/P12

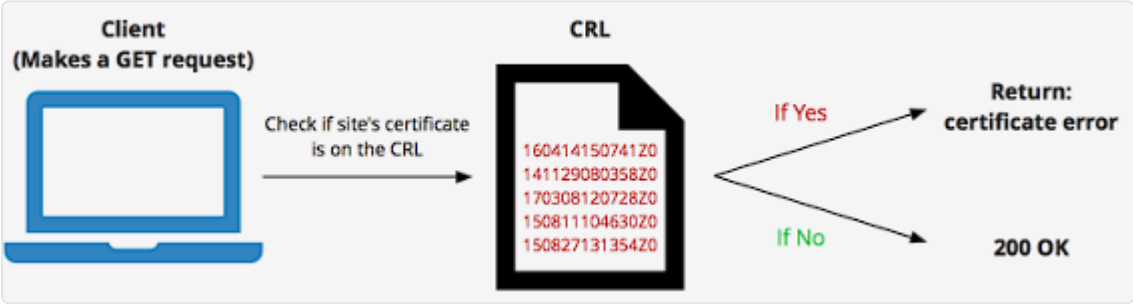
Os arquivos PFX (Personal Information Exchange) ou P12 (PKCS#12) são formatos de arquivo que podem armazenar certificados digitais junto com suas chaves privadas correspondentes. Esses arquivos são protegidos por uma senha para garantir a segurança da chave privada. Eles podem ser usados para exportar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

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.

Arquivos CRL (Certificate Revocation List)

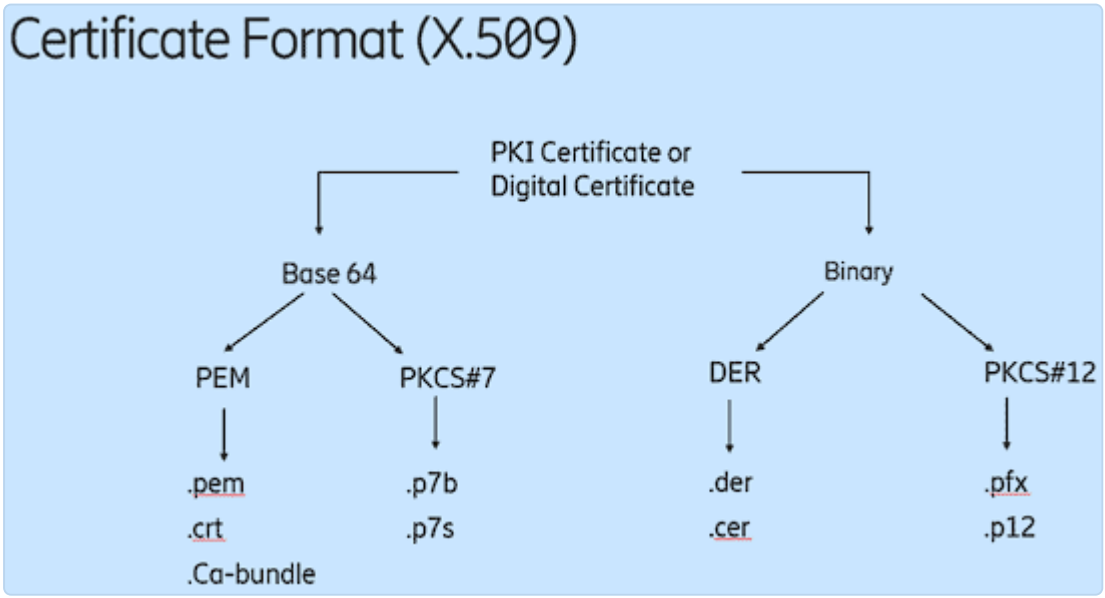
Os arquivos CRL são usados para armazenar listas de certificados revogados. Eles contêm informações sobre certificados que foram revogados antes do término do período de validade. Os arquivos CRL geralmente são fornecidos em um formato binário ou em texto codificado em Base64.



Certificate Revocation List.

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.



Formato de Certificado X.509.

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.

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:

- 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).
- Certificados de Email/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.
- 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.

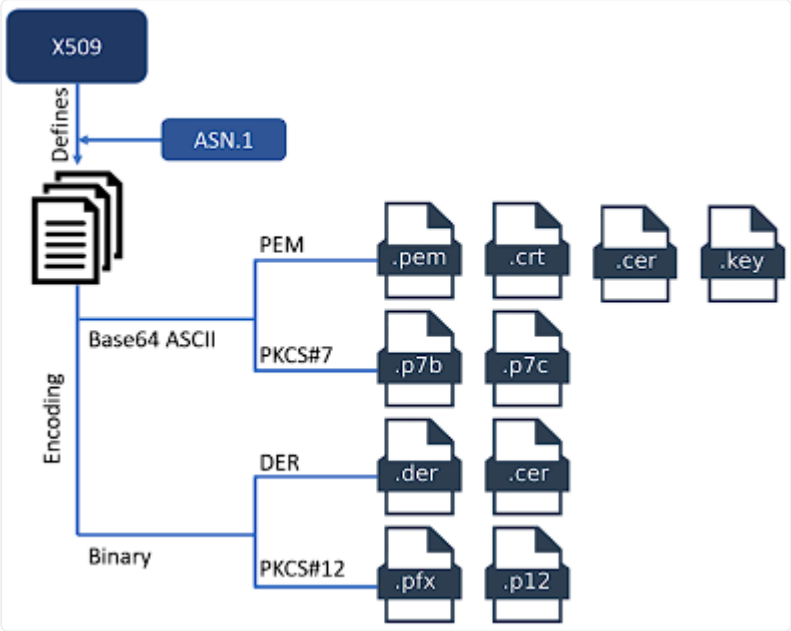
Arquitetura de Certificados Digitais

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:

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. 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.

8. 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.
9. 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.
10. 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.

Os diferentes formatos de arquivo de certificado digital, como PEM, DER e PKCS#12, seguem essa estrutura para armazenar os dados do certificado de maneira adequada ao formato específico.



Extensões de certificados.

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.

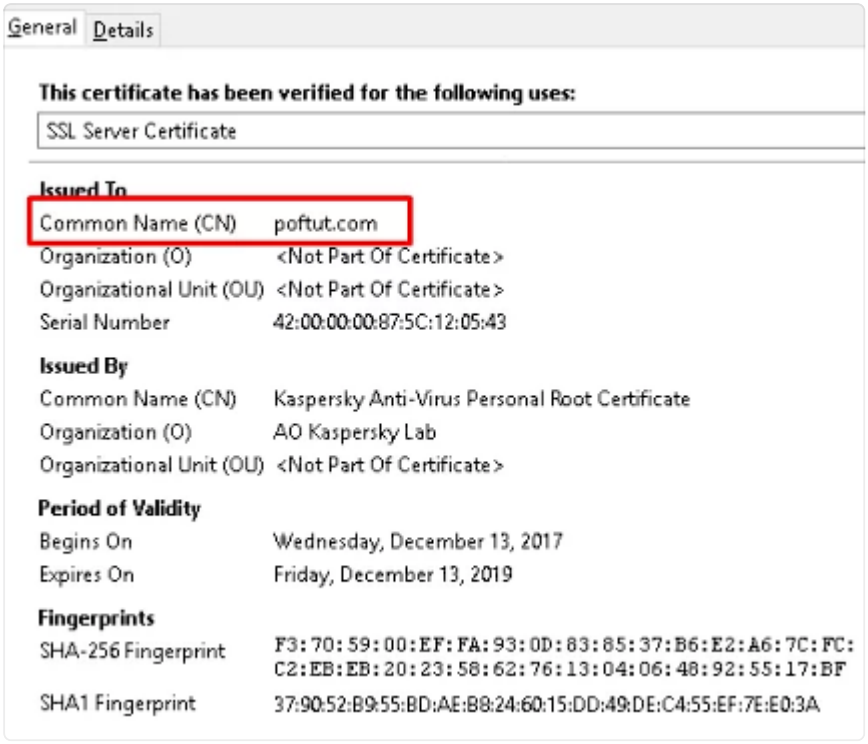
Os Atributos do Nome do Assunto são usados para verificar a identidade do titular do certificado durante o processo de autenticação. Eles desempenham um papel fundamental na estabelecimento de confiança na comunicação segura por meio de chaves públicas. Por exemplo, em um certificado SSL/TLS para um site, os Atributos do Nome do Assunto podem incluir o nome de domínio do site, informações sobre a organização proprietária do site e outros detalhes que ajudam a verificar a autenticidade e a legitimidade do certificado.

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. Por exemplo, em um certificado para o site "www.exemplo.com", o CN seria "www.exemplo.com".

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.



Common Name.

Nome Alternativo do Assunto – Subject Alternative Name (SAN)

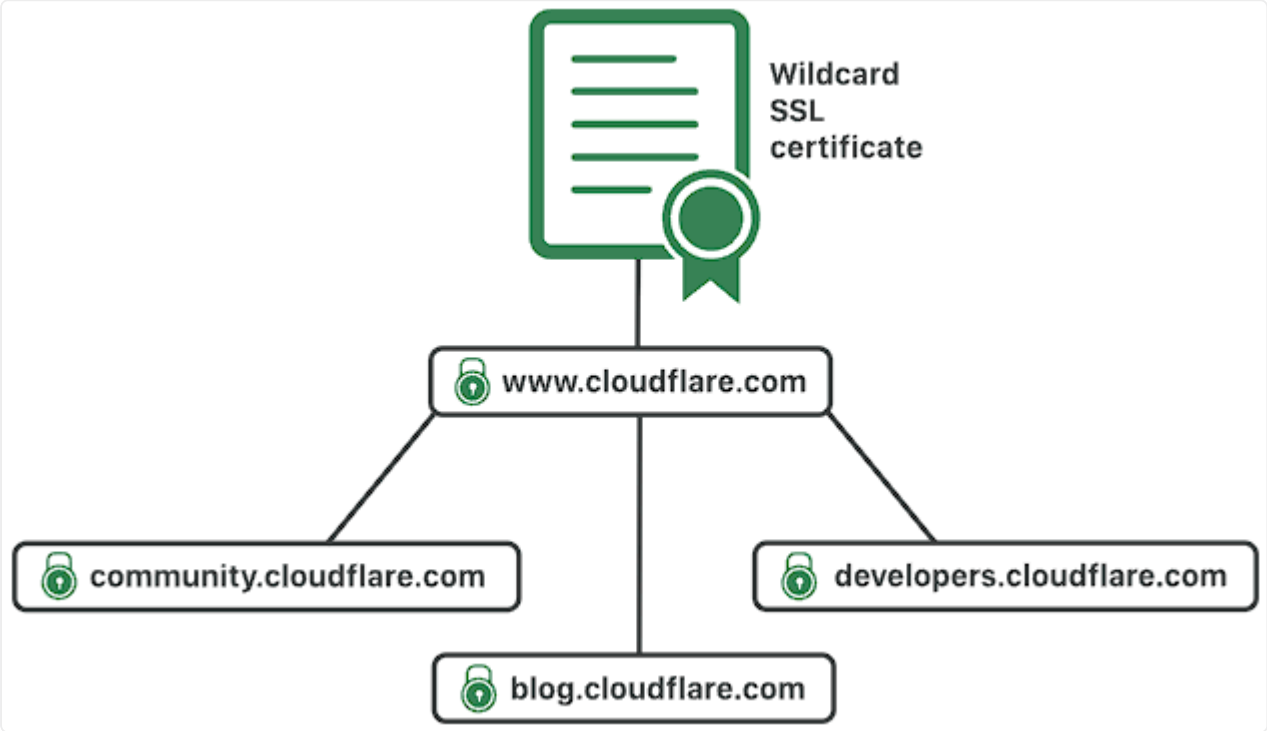
Subject Alternative Name (SAN) é um campo presente em certificados digitais que permite especificar nomes alternativos para identificar o sujeito ou entidade do certificado, além do Common Name (CN). O SAN é usado principalmente em certificados SSL/TLS para suportar diferentes domínios ou subdomínios 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. Veja três exemplos de domínios que podem ser incluídos no campo Subject Alternative Name de um certificado:

- www.example.com: Um domínio principal usado para acessar um site específico.
- mail.example.com: Um subdomínio usado para acesso ao servidor de e-mail associado ao domínio example.com.
-

- secure.example.net: Um domínio diferente, mas relacionado, que também faz parte do mesmo serviço ou entidade.

Esses exemplos mostram como o campo SAN pode ser utilizado para incluir diferentes domínios em um único certificado, permitindo que todos eles sejam validados e confiáveis para uso seguro na comunicação online.



Certificado Wildcard.

Conclusão

Em conclusão, esta aula abordou a importância da Infraestrutura de Chaves Públicas (PKI) na segurança digital, explorando os conceitos básicos da criptografia assimétrica e sua aplicação na certificação digital. Foi destacado o papel dos certificados digitais na identificação e autenticação de entidades digitais, assim como o processo de emissão, validação e gerenciamento desses certificados.

Durante a aula, foi enfatizada a importância da PKI como uma tecnologia fundamental para estabelecer e gerenciar a segurança em ambientes digitais. A criptografia assimétrica, que utiliza pares de chaves pública e privada, foi apresentada como a base para a certificação digital, garantindo a confidencialidade, integridade, autenticidade e não repúdio das informações

transmitidas. O ciclo de vida dos certificados digitais, desde a solicitação até a expiração ou revogação, foi abordado, ressaltando a importância da verificação da identidade do solicitante, a distribuição adequada do certificado e a renovação quando necessário.

Além disso, foram apresentados os principais tipos de arquivos que podem conter certificados digitais, como PEM, DER, PFX/P12, P7B/PKCS#7 e CRL, cada um com suas características e finalidades específicas. A estrutura dos certificados digitais, definida pela arquitetura X.509, foi discutida, destacando os campos como versão, número de série, algoritmo de assinatura do emitente, nome do emitente, período de validade, nome do sujeito e chave pública.

> Parabéns pela conclusão desta aula! Você demonstrou um excelente comprometimento e dedicação em aprender sobre Certificado Digital e Infraestrutura de Chaves Públicas (PKI). Ao compreender o papel e a importância da PKI na segurança digital, assim como os conceitos fundamentais da criptografia assimétrica e a aplicação na certificação digital, você adquiriu conhecimentos essenciais para garantir a confiabilidade e autenticidade em ambientes digitais.