1.Introdução a chaves públicas e autoridades certificadoras

1.1 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.

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.

2.Chave pública

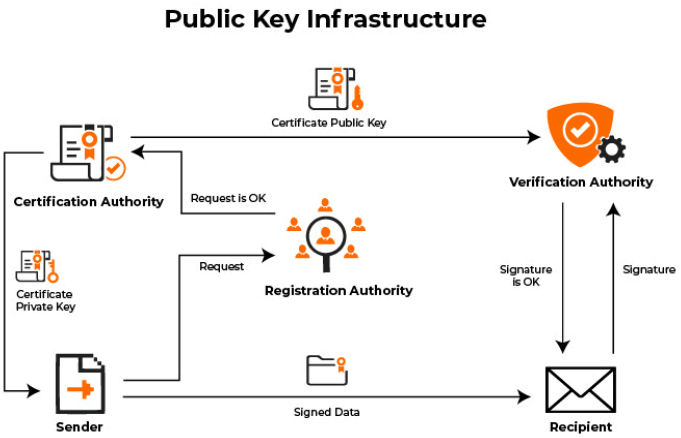
A chave pública é uma chave criptográfica que pode ser divulgada e compartilhada livremente com outras partes. Ela é usada para criptografar informações ou verificar assinaturas digitais. A chave pública é derivada da chave privada correspondente por meio de algoritmos matemáticos específicos. Quando 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.

3.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.



4.Autoridades Certificadoras (ACs) em PKIs

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 estão descritas abaixo

4.1 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.

4.2 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.

4.3 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.

4.4 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.

4.5 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).

5.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 descritos abaixo.

5.1 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.

5.2 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.

5.3 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.

5.5 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.

5.6 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.

5.7 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.

5.8 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.

5.9 Autoridade Certificadora de e-mail (E-mail 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.

5.10 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.

5.11 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).

5.12 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.

5.13 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.

5.14 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.

5.15 Autoridade 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.

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.

6.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:

- **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.
- **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.
- **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.

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.

7.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.
- **Promoter 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.