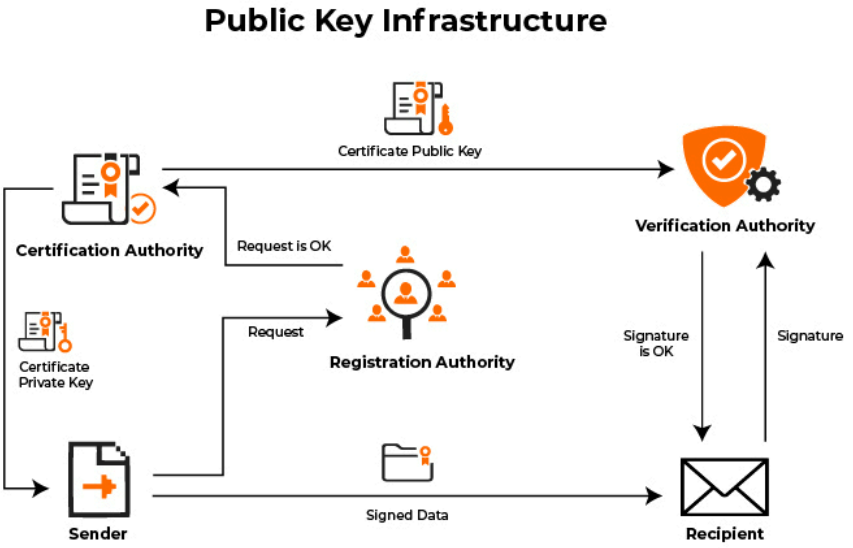
1.Public Key Infrastructure

A infraestrutura de chave pública (PKI) permite o gerenciamento de identidades digitais, em que uma autoridade de certificação (CA) emite certificados para sujeitos validados, como usuários e servidores. Esses certificados contêm a chave pública do sujeito e são assinados pela chave pública da AC. As chaves públicas permitem que terceiros verifiquem o certificado e a assinatura, garantindo a confiança na identidade do sujeito.

O par de chaves consiste na chave pública, que é incluída no certificado e pode ser divulgada amplamente, e na chave privada, que está vinculada à chave pública e deve ser mantida em segredo pelo proprietário. A chave privada pode ser armazenada no computador, seja no sistema de arquivos ou em um chip de plataforma confiável (TPM).

Essa abordagem com certificados e cartões inteligentes oferece uma camada adicional de segurança, uma vez que a chave privada é protegida fisicamente e pode ser transportada facilmente pelo usuário. Dessa forma, é possível autenticar-se de maneira segura e confiável em diferentes ambientes, sem a necessidade de expor a chave privada diretamente ao sistema em que se está autenticando.

O Gerenciamento de Chaves em uma PKI (Infraestrutura de Chaves Públicas) envolve a administração e o controle das chaves de criptografia utilizadas em certificados digitais. As chaves desempenham um papel essencial na segurança da comunicação e na autenticação de entidades em uma infraestrutura baseada em PKI.



1.2 Ciclo das chaves

O ciclo de vida das chaves em uma PKI é composto por várias etapas

1.2.1 Geração de chaves

Nessa etapa, as chaves criptográficas são geradas de forma segura. Uma chave privada é criada e associada a uma chave pública correspondente. A chave privada deve ser mantida em segredo e protegida adequadamente, enquanto a chave pública pode ser compartilhada livremente.

1.2.2 Solicitação e emissão de certificados

Após a geração das chaves, é feita uma solicitação de certificado digital que inclui a chave pública. A solicitação é enviada a uma Autoridade Certificadora (AC) confiável, que valida a identidade do solicitante e emite um certificado contendo a chave pública e outras informações relevantes.

1.2.3 Armazenamento e proteção

O armazenamento seguro das chaves privadas é crucial para evitar o acesso não autorizado. Recomenda-se o uso de dispositivos de segurança, como HSMs (Módulos de Segurança de Hardware) ou smart cards, para proteger as chaves privadas. Além disso, é importante implementar controles adequados de acesso e realizar backups regulares das chaves.

1.2.4 Renovação e proteção

Os certificados digitais (CAs) têm uma validade limitada, geralmente de um a três anos. Durante esse período, é necessário acompanhar a expiração dos certificados e realizar sua renovação antes que se tornem inválidos. Isso envolve a geração de uma nova solicitação de certificado e a substituição do certificado anterior pela nova versão.

1.2.5 Revogação

Em certas situações, um certificado digital pode se tornar comprometido ou não confiável antes de sua data de expiração. Nesses casos, é necessário revogar o certificado para indicar que ele não deve mais ser considerado válido. A revogação pode ocorrer por motivos como perda da chave privada, suspeita de comprometimento ou cessação de associação com uma organização.

1.2.6 Destruição

Quando um certificado digital não é mais necessário ou quando a chave privada associada é comprometida, é fundamental garantir sua destruição adequada. Isso evita o uso indevido da chave privada e garante a segurança contínua da infraestrutura.

2.Gerenciamento de chaves

O Gerenciamento de Chaves em uma PKI é essencial para garantir a confidencialidade, integridade e autenticidade das comunicações e transações digitais.

2.1 Tipos de gerenciamento de chaves

2.1.1 Gerenciamento de chaves centralizado

Nesse modelo, **todas as chaves de criptografia são armazenadas e gerenciadas em um único local centralizado**. Geralmente, isso é feito por uma entidade central, como uma Autoridade Certificadora (CA) ou um servidor de chaves dedicado. Todas as solicitações de certificados e operações relacionadas às chaves são direcionadas a esse ponto central, o que permite um controle mais rigoroso e padronizado sobre as chaves e os certificados. O gerenciamento centralizado facilita a aplicação de políticas de segurança e garante a conformidade com os padrões estabelecidos.

2.1.2 Gerenciamento de chaves descentralizado

Nesse modelo, **as chaves de criptografia são distribuídas e gerenciadas em diversos locais ou sistemas independentes**. Cada entidade ou sistema pode gerar suas próprias chaves e certificados, sem depender de uma autoridade central. Isso proporciona uma maior autonomia e flexibilidade, permitindo que cada entidade tenha controle total sobre suas chaves e certificados. No entanto, o gerenciamento descentralizado pode apresentar desafios em termos de coordenação e conformidade, uma vez que não há uma única autoridade central responsável pelo controle e pela aplicação de políticas de segurança.

3.Custódia de chaves

A Custódia de Chaves, também conhecida como ***Key Escrow*** em inglês, **consiste em um mecanismo pelo qual uma cópia das chaves privadas é armazenada em um local seguro e confiável**, geralmente fora da organização ou entidade que as utiliza.

A ideia por trás da Custódia de Chaves é garantir que, em caso de perda, corrupção ou comprometimento das chaves privadas originais, uma cópia de segurança possa ser recuperada e utilizada para recuperar o acesso aos certificados digitais associados.

A entidade ou organização que detém a Custódia de Chaves é geralmente uma terceira parte confiável, como uma Autoridade Certificadora (AC) ou uma agência governamental. Essa entidade possui os meios e os procedimentos para proteger e armazenar as chaves privadas de forma segura.

A Custódia de Chaves pode ser vista como uma medida de segurança adicional para mitigar o risco de perda completa das chaves privadas, garantindo a disponibilidade contínua dos certificados digitais em caso de problemas.

No entanto, é importante notar que a Custódia de Chaves também pode gerar preocupações em relação à privacidade e à segurança, uma vez que envolve confiar a terceiros o acesso às chaves privadas.