Public-Key Infrastructure

Teórica #12 de Criptografia Aplicada

Public-Key Infrastructure (PKI)

Porquê PKI?

Todas as primitivas criptográficas de chave pública assumem que as chaves publicas são autenticas, caso contrário, os protocolos que as usam são vulneráveis a ataques MiTM.

De formar a segurar que esta propriedade é cumprida, existem duas abordagens que se podem seguir:

- Numa distribuição ad-hoc, onde cada chave pública é confirmada manualmente para cada entidade;
- Através de uma PKI, que é requerida legalmente/pela regulação, onde devem ser descritos os standards técnicos utilizados, como estes devem-se utilizados, responsabilidades e direitos das entidades e as garantias e penalidades relativamente à regulação.

Certificados Chave Pública (Public-Key Certificates)

A Alice e o Bob desejam comunicar entre si sobre um canal inseguro, através de criptografia de chave pública. Para realizar a troca de chaves, o Bob tem de saber que a chave recebida da Alice é realmente da Alice. Para tal, como estão num canal inseguro, o Bob tem que comunicar com uma *Trusted-Third-Party* (TTP), sobre um canal seguro, ed forma a que consiga provar que foi a Alice que lhe enviou a chave, usando o valor desta. Em certificados de chave pública, a TTP é chamada de *Certification Authority* (CA) e a Alice prova à CA que a sua chave pública é a que o Bob recebeu, ao assinar um *certificate request* (**PKCS#11**), dado que é o CA que fornece a chave secreta à Alice.

O certificado fornecido pela CA providencia informação que uma entidade necessita de verificar:

- Identidade da entidade + a sua chave pública;
- Metadados da CA, como o *serial number* e *issue identity*
- Validade do certificado.

No final o CA assina o certificado, formando-se assim certificado de chave pública.

A confiança que um pode ter num certificado é sempre menor do que num CA.

O que é o ASN.1?

Linguagem de notação utilizada para descrever um certificado e muitos outros standards de redes, de forma agnóstica/independente da linguagem/plataforma. **DER** (Distinguished Encoding Rules) é

o formato utilizado para codificar a informação dos certificados.

Os certificados estão descritos em ASN.1 de forma a que as CA que os receba saibam os interpretar, relativamente ao uso dos algoritmos de hashing, cifras, etc.

Os certificados podem ser transmitidos sobre canais inseguros?

Nem todos

Verificação de Certificados Chave Pública

Na comunicação entre duas entidades, Alice e Bob, uma vez o Bob recebendo o certificado da Alice, este tem que certificar que este pertence mesmo à Alice. Para tal, este realizar primeiro umas validações primárias no seu lado, como verificar se o certificado não expirou, metadados vão de acordo com o especificado. Depois, a CA é comunicada de forma a que esta verifique que a chave pública presente no certificado é realmente da Alice.

Os certificados estão estandardizados como *X.509* na IETF (Internet Engineering Task Force). As estruturas de dados importantes contem objetos identificadores únicos.

A versão atual dos certificados, 3, inclui informação básica como:

- Subject (entidade):
- Issuer (CA);
- Validade;
- Public Key Info;
- Serial Number.

Os certificados podem conter também extensões/attachments, dos quais podem ser marcados como **críticos** e não críticos. Todos as extensões são identificados com um object identifier, e se marcadas como criticas e não sejam reconhecidas, deve-se rejeitar o certificado. Existem também extensões importantes, que denotam:

- Chave identificadora da entidade/autoridade, que representa o fingerprint da chave pública;
- Restrições básicas, que identificam se o certificado é especial, e como se deve utilizar as chaves.

O que é uma PKI?

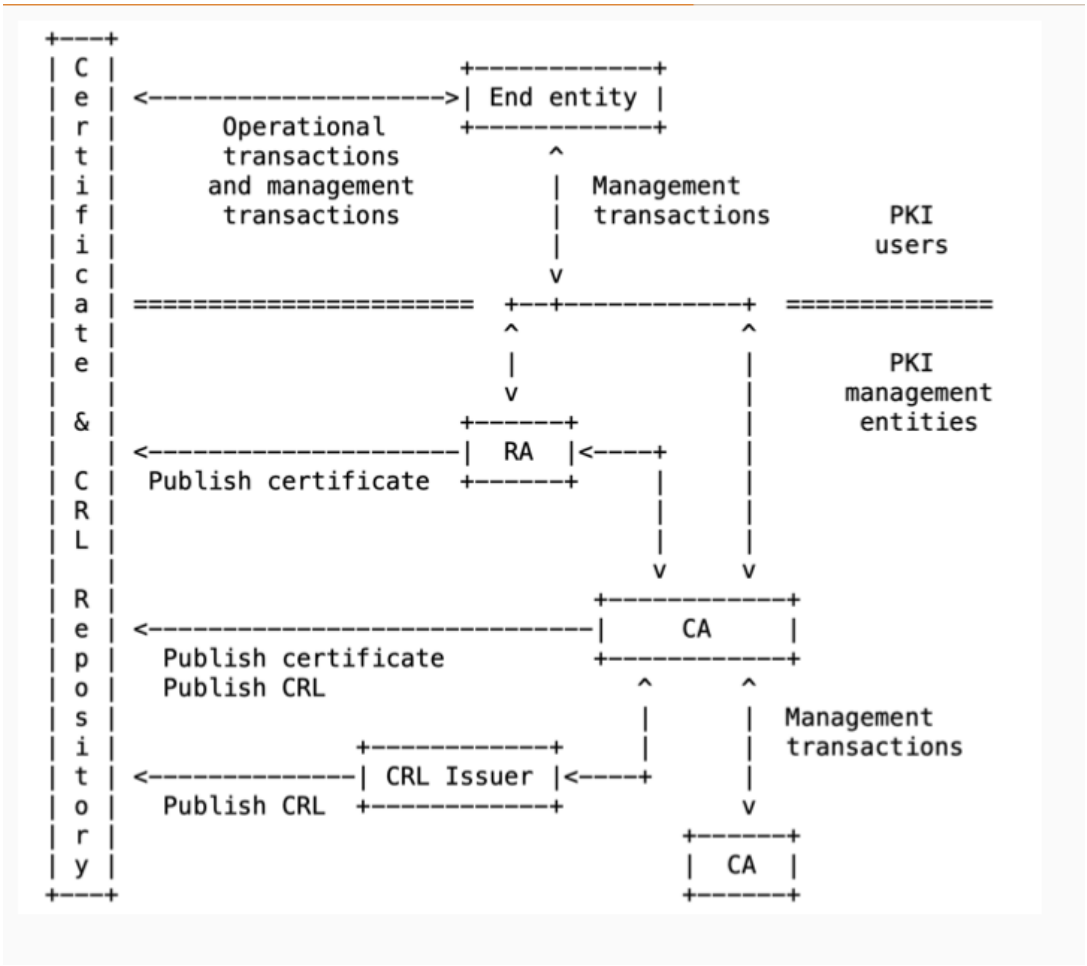
Uma PKI é um conjunto de papéis, politicas, hardware, software e procedimentos necessárias para criar, manter, distribuir, usar, guardar e revocar certificados digitais.

Papeis fundamentais de uma PKI:

- Verificar e autenticar um utilizador com um certificado;
- Verificar que uma chave pública pertence a uma entidade.

Como funciona uma PKI?

Existem diversas áreas e responsabilidades numa PKI.



Gestão e Operações de Transações

Parte vital de uma PKI que se responsabiliza em gerir a forma como os certificados são armazenados e transferidos entre a PKI. Este especifica os protocolos usados para o armazenamento (e.g., LDAP), transferência (HTTP, FTP, MIME) e codificação.

Exemplos de protocolos de operação:

- TLS especifica na sua RFC como os certificados são trocados;
- S/MIME especifica que os certificados são incluídos em attachments do PKCS#7;
- Certificados do sistema operativo são geridos e mantidos por módulos criptográficos standard.

PKI Management

Como é que uma entidade Y verifica uma assinatura CA num certificado?

1. Interpretar o certificado X.509;
2. Obter chaves públicas do/s CA/s no certificado;
3. Verificar assinatura da entidade X, através da chave publica do CA.

Como é que uma entidade Y confia numa CA?

- A entidade Y obtém um certificado diretamente da CA;
- A entidade Y confia em CA através de outra CA que confia (se Y confia em CA 1 e CA 1 confia em CA 2, então Y confia em CA 2).

Como se comunica com uma CA?

As **Registration Authorities** (RA) são o *frontend* dos certificados, permitindo contacto direto com entidade finais. É responsável por verificar a informação presente nos certificados e garantir que as entidades únicas possuem a chave secreta (e.g., Registo Civil, Loja do Cidadão).

As **Certification Authorities** (CA) são o *backend* dos certificados, sendo aqui que está presente a infra-estrutura que assina os certificados, sendo fortemente segura com segurança física, air gaps, etc (e.g., Casa da Moeda).

Como se revoca um certificado?

Os certificados tornam-se inválidos a partir do momento que período de vida destes expira, é perdida uma chave secreta, ocorre uma data breach, metadados tornam-se incorretos, etc.

Existem diferentes formas de revocar um certificado:

- Incluí-lo numa CRL (**Certificate Revokation Lists**) da CA, que representa uma blacklist de certificados revogados;
- Usar **Trusted Service Provider Lists** (TSL), que representam whitelists de certificados de confiança. Normalmente utilizado em entidade mais fechadas como a banca ou governo;
- Através do OCSP - **Online Certificate Status Protocol**, onde um trusted server verifica as CRLs. Por norma este é período pelas CA e são usados em contextos de organizações de larga escala;
- Certificate Pinning, onde os webservers/browsers/applications tem as suas próprias whitelists e fazem a verificação localmente.

Root CA

Root Certification Authorities são CA “pais” de outras CAs. São estas que validam as CA filhos, sendo que confiando numa Root CA, então confia-se nas CA que esta mantém.

Se uma entidade Y não consegue verificar implicitamente que uma CA é de confiança, esta vai requisitando CA superiores a esta, até encontrar uma que confie. Se neste processo a entidade Y não conseguir arranjar certificados, então o processo termina.

A entidade X envia para entidade Y todos os certificados CA que este necessite até verificar a confiança, excepto o Root CA.

Certificate Policies

As politicas dos CA podem ser identificadas nos próprios certificados, através de específicos object identifiers, fazendo parte da lei cumprir estas politicas a quem interagir com os certificados. Dado isto, é necessário realizar uma auditoria à CA antes de esta publicar os certificados.