Public Key Infrastructure (PKI)

O que é o PKI?

Conjunto de hardware, software, pessoas, políticas e procedimentos necessários para a criação, gestão armazenamento, distribuição e revogação de chaves públicas

- Principal questão associada ao desenvolvimento destes modelos: Confiança

Certificados Digitais

Caracteristicas (1)

- É baseado na cifragem assimétrica
- Infraestrutura tão segura quanto o mecanismo utilizado na distribuição certificada de informação
- Integra 3 componentes principais
  - Certificados Digitais/Assinaturas
  - Criptografia de chave pública
  - Certificate Authorities (CA)

Caracteristicas (2)

- Protecção da informação de várias formas
  - Autenticação da identidade
  - Verificação da integridade
  - Privacidade
  - Autorização de acessos
  - Autorização de transações
  - Não repúdio

Certificados Digitais

- Associam entidades a chaves públicas
- Contêm informação detalhada sobre a entidade
- A validade dum certificado é assegurada pela presença da assinatura digital de uma terceira entidade
- Vamos ver:
  - **Certificados X.509**

Certificados X.509

Descrição (1)

- Criados pelo ITU-T e pela OSI no âmbito do Serviço de Directoria (recomendações da série X.500 que definem os serviços de directoria)
- Utilização do Serviço de Directoria como repositório de chaves públicas das entidades
- O X.509 é importante porque a sua estrutura é usada em vários contextos:
  - S/MIME, IPSec, SSL, etc

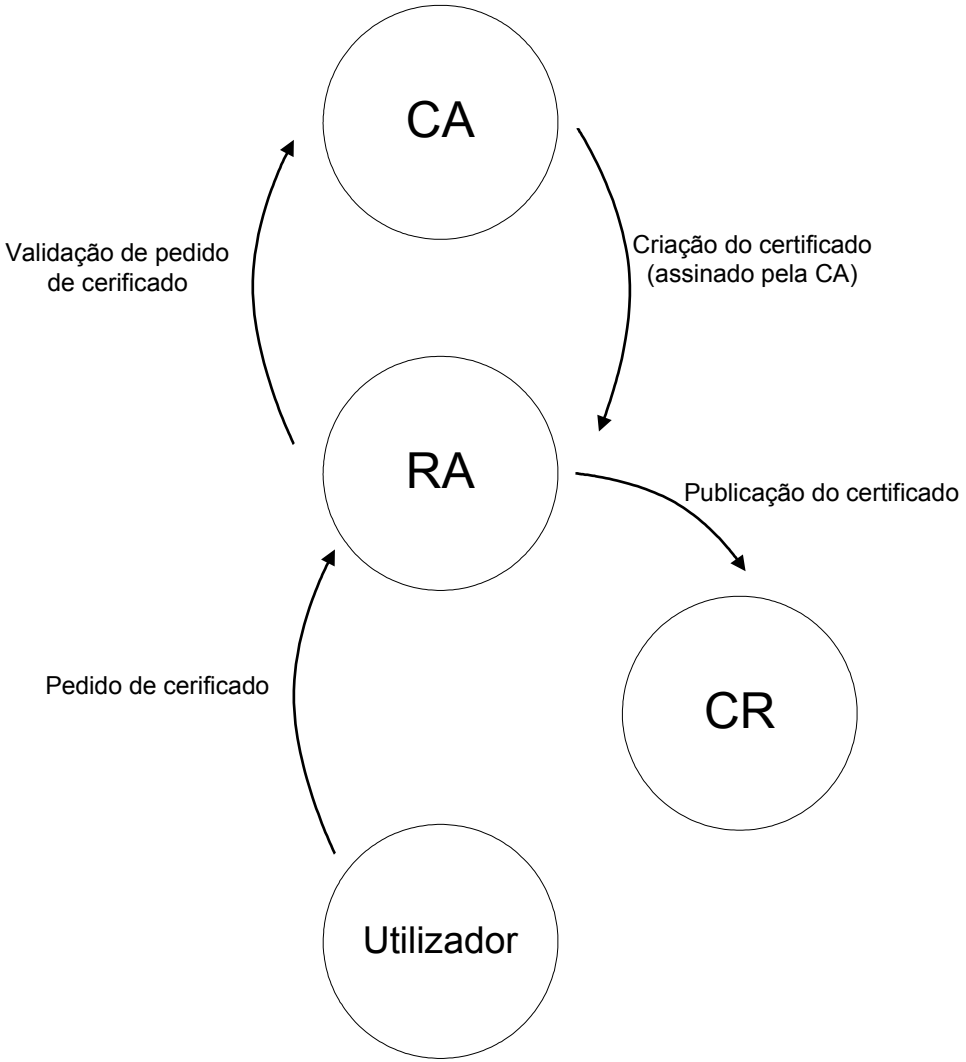
Descrição (2)

- Foi criada a norma PKIX (PKI X.509)
  - www.ietf.org/html.charters/pkix-charter.html
- Existem várias RFC sobre PKI, das quais se destacam:
  - **RFC 2510** *PKIX Certificate Management Protocols*
  - **RFC 2559, RFC 2585, RFC 2560** *Operational protocols*
  - **RFC 3647** *Certificate Policy and Certification Practices Framework* (Actualiza a RFC 2527)

Modelo PKIX (1)

- Componentes
  - **CA** (*Certification Authorities)* – são as entidades que emitem os certificados digitais.
  - **RA** (*Registration Authorities*) – entidades que ajudam as CA's na identificação dos candidatos ou requerentes de criação, renovação ou revogação de certificados digitais
  - **CR** (*Certificate Repositories*) – entidades que disponibilizam um espaço para publicação, armazenamento e acesso aos certificados digitais e outra informação relacionada com a infra-estrutura de chave pública
  - **Titulares** (*Subscribers* ou *Users*) – são as pessoas singulares ou organizações colectivas detentoras de um par de chaves cuja chave pública está certificada por uma autoridade certificadora e inclusa no respectivo certificado digital
  - **Partes Interessadas** (*Relying Partys, RP*) – entidades receptoras da chave pública e/ou assinatura digital de titulares, que confiam na autenticidade da chave pública certificada.
  - **Entidade Credenciadora** – Não faz parte da PKI em si mas é quem autoriza e reconhece o funcionamento de uma CA do ponto de vista legal. Em Portugal, o organismo que exerce essa função é o Instituto das Tecnologias da Informação na Justiça (ITIJ)

Modelo PKIX (2)



Documentação de uma PKIX

- Política de certificados (*Certificate Policy, CP*): requisitos gerais que os intervenientes na PKI devem satisfazer. Descreve os usos que os certificados podem ter. Por razões de segurança, os requisitos podem ser mantidos confidenciais.
- Declaração das práticas de certificação (*Certification Practice Statement, CPS*): descreve as práticas assumidas pela CA para a exerção das suas funções. Relata os procedimentos de uma perspectiva legal, técnica e de negócio e é mais detalhada do que a CP. A CPS pode também ser a base para a certificação cruzada entre duas CA's.
- Acordo de utilizador (*Subscriber Agreement, SA*): é o acordo estabelecido entre o titular de um certificado e uma CA ou RA. Este documento descreve as responsabilidades e condições de utilização dos certificados que o seu titular deve respeitar.
- Acordo das Partes Interessadas (*Relying Party Agreement, RPA*) – é o acordo estabelecido entre determinada entidade interessada em confiar num certificado e a CA que o emitiu ou a RA que aprovou a sua criação. Normalmente determina que a parte interessada deve verificar o estado do certificado antes de confiar nele.

CA (1)

- Serviços disponibilizados:
  - Gestão de chaves: inclui geração de pares de chaves, manipulação segura das chaves privadas da CA e distribuição das chaves públicas da CA
  - Criar um meio para que os requerentes de certificado possam submeter a sua requisição de certificado (por exemplo, uma página web)
  - Identificação e autenticação dos indivíduos ou entidades que requerem à CA a criação de certificados, renovação de certificados ou alteração de chaves
  - Aprovação ou rejeição de requisições de certificados submetidas à CA
  - Emissão de certificados referentes às requisições aprovadas
  - Publicação dos certificados num repositório para posterior usufruto das entidades interessadas
  - Revogação de certificados, quer a pedido do titular, quer por iniciativa própria
  - Publicação da lista de certificados revogados

CA (2)

- Cada certificado contém a chave pública da entidade
- A chave pública da entidade é assinada (validada) com a chave privada da entidade emissora (Autoridade de Certificação)
- A verificação da identidade faz-se com a chave pública da Autoridade de Certificação

CA (3)

- Políticas que deve estabelecer
  - Que tipos de certificados existem
  - Para um determinado tipo de certificado, quais são os passos necessários para a verificação
  - Armazenamento dos certificados e das chaves privadas
  - Expiração dos certificados
  - Registo dos certificados

RA (1)

- Serviços disponibilizados
  - Criar um meio para que os requerentes de certificado possam submeter a sua requisição de certificado (por exemplo, uma página web)
  - Identificação e autenticação dos indivíduos ou entidades que requerem à CA a criação de certificados, renovação de certificados ou alteração de chaves
  - Aprovação ou rejeição de requisições de certificados submetidas à CA
  - Revogação de certificados, quer a pedido do titular, quer por iniciativa própria

Ciclo de vida do certificado (1)

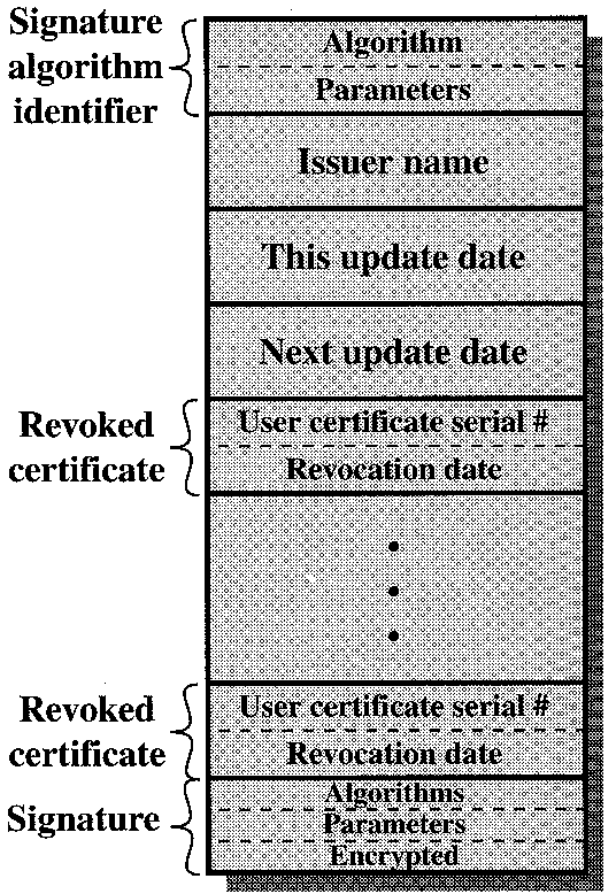
- Requisição
  - Pelo titular, ou por um procurador
  - Certificado pessoal, ou para um servidor, ...
- Aceitação
  - O titular deve verificar se existe alguma incorrecção
- Publicação
  - O certificado é assinado com a chave privada da CA
  - É colocado num repositório acessível a todas as partes interessadas
  - Envio do certificado ao titular (por e-mail, smart card, ...)

Ciclo de vida do certificado (2)

- Revogação
  - Por iniciativa do titular (perca da chave privada, a chave secreta está comprometida, etc)
  - Por iniciativa da CA (incumprimento do acordo de titulares)
  - adição do certificado à lista de certificados revogados
  - O utilizador já não é certificado pela CA
  - O certificado emitido pela CA está comprometido
  - Criação de uma *Certificate Revogation List* (CRL) que deve ser mantida na directoria
  - Utilização do *Online Certificate Status Protocol* (OCSP)

Ciclo de vida do certificado (3)

- Revogação (cont.)
  - CRL
    - Cada entrada contém o nº de série (que identifica o certificado dentro da CA) e a data de revogação
    - Quem recebe um certificado tem que verificar se pertence à CRL



Ciclo de vida do certificado (4)

- Revogação (cont.)
  - Dois modelos para a entrega de CRLs
    - **Polling**: a CRL é pedida pelo utilizador quando este precisa da chave de um certificado digital
      - Problema: Variação de tempo entre a revogação e a publicação
    - **Pushing**: cada CRL é entregue pelo CA ao utilizador assim que ocorre uma nova revogação
      - Problema: armazenamento de CRLs mesmo que não sejam necessárias e perigo de intercepção/remoção

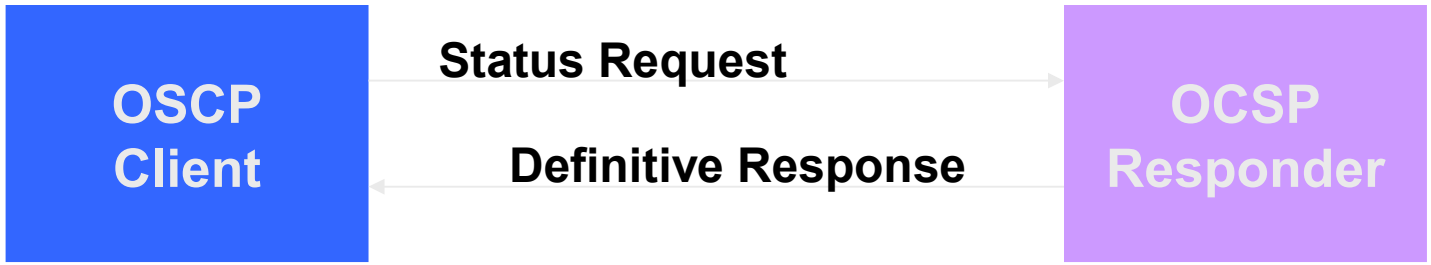
Ciclo de vida do certificado (5)

- Revogação (cont.)
  - Limitações
    - Os CRLs são emitidos/actualizados de forma periódica de acordo com a política da CA
    - Possibilidade de se aceitar um certificado digital revogado, mas ainda não publicado na CRL

Solução: OCSP

Ciclo de vida do certificado (6)

- Revogação (cont.)
  - Permite às aplicações determinarem a revogação de um certificado de uma forma mais expedita
  - Modelo cliente-servidor



Ciclo de vida do certificado (7)

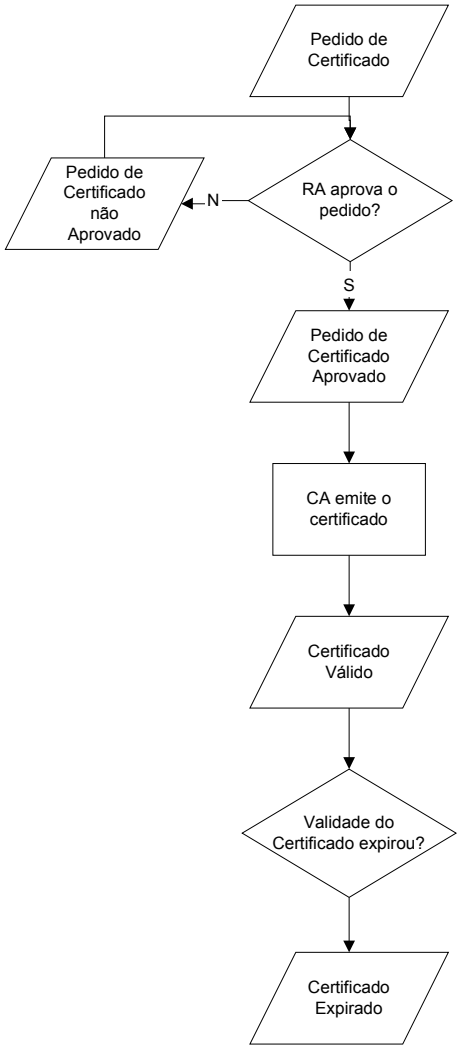
- Suspensão
  - Certificado inválido por um determinado período (férias, greves, inactividade, etc)
  - Serviço que não é disponibilizado por todas as PKI
  - Pode ser usado para publicar um certificado que ainda não foi aceite pelo titular
- Renovação
  - Os certificados tem uma validade a partir da qual deixam de ser válidos, por isso necessitam de ser renovados
  - O certificado é assinado pela CA com nova data limite

Ciclo de vida do certificado (8)

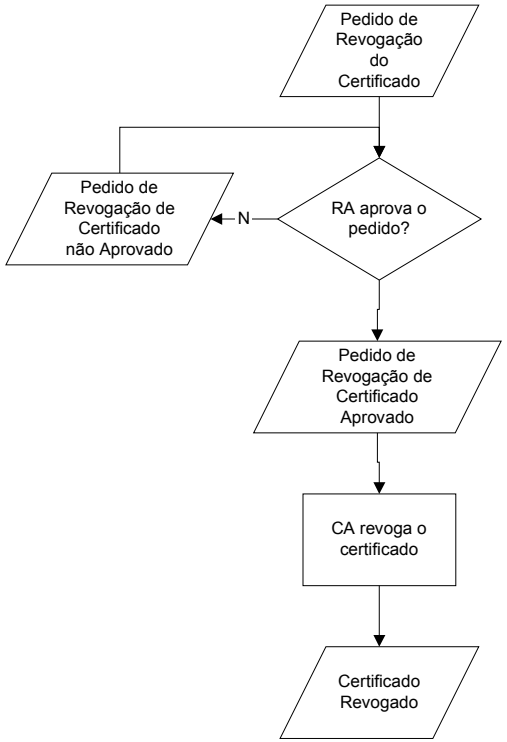
- Alteração
  - Pode ser necessário alterar um certificado devido a: alteração do nome legal do titular, alteração de informação regional, alteração do e-mail, alteração das chaves, etc
  - É emitido um novo certificado com a informação actualizada e o certificado antigo é revogado
- Verificação do estado
  - Lista de certificados revogados (CRL - *Certificate Revocation Lists*)
  - Verificação on-line (*On-line revocation/status checking*, e.g. OCSP – On-line Certificate Status Protocol)

Ciclo de vida do certificado (9)

Processo de emissão de certificados



Processo de revogação de certificados



Formato do Certificado (1)

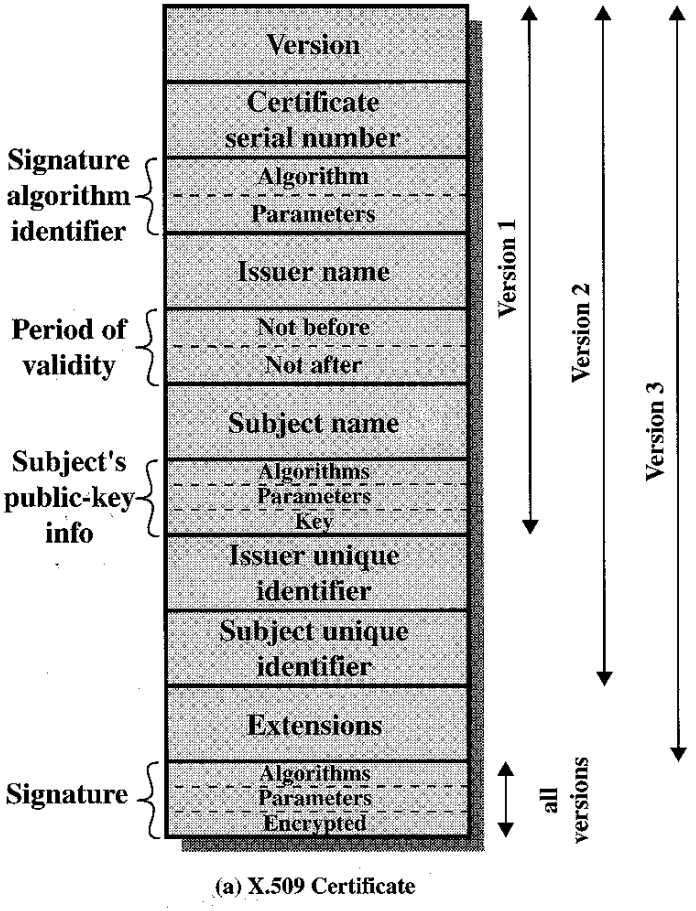
- Versão: Determina qual a versão da norma X.509 que o certificado respeita.
- Número de série: É um identificador único para cada certificado atribuído pela entidade que o emitiu e que permite distinguir inequivocamente todos os certificados emitidos. Este número é utilizado, por exemplo, quando o certificado é revogado este número é colocado numa lista de certificados revogados.
- Identificador do algoritmo de assinatura: Determina qual o algoritmo usado pela CA para assinar o certificado.
- Emissor do certificado: Indica o nome da entidade que emitiu o certificado.
- Período de validade: Define o tempo de vida do certificado.
- Nome do titular: Indica o nome da entidade (por exemplo pessoa) a quem foi emitido certificado. Este campo respeita a norma X.500.
- Chave pública do titular: Aqui vai a chave pública do titular do certificado.
- Algoritmo da chave pública: Indica qual o algoritmo usado para criar o par de chaves do titular.
- Assinatura: contém um *hash* de todos os campos que depois é assinado com a chave provada da CA

Formato do Certificado (2)

- Até agora foram publicadas 3 versões
  - A 1ª versão foi publicada em 1988
  - Em 1993 foi efectuada uma revisão
  - A mais recente é X.509 V3, foi publicada em 1995 e revista em 2000

- Notação:

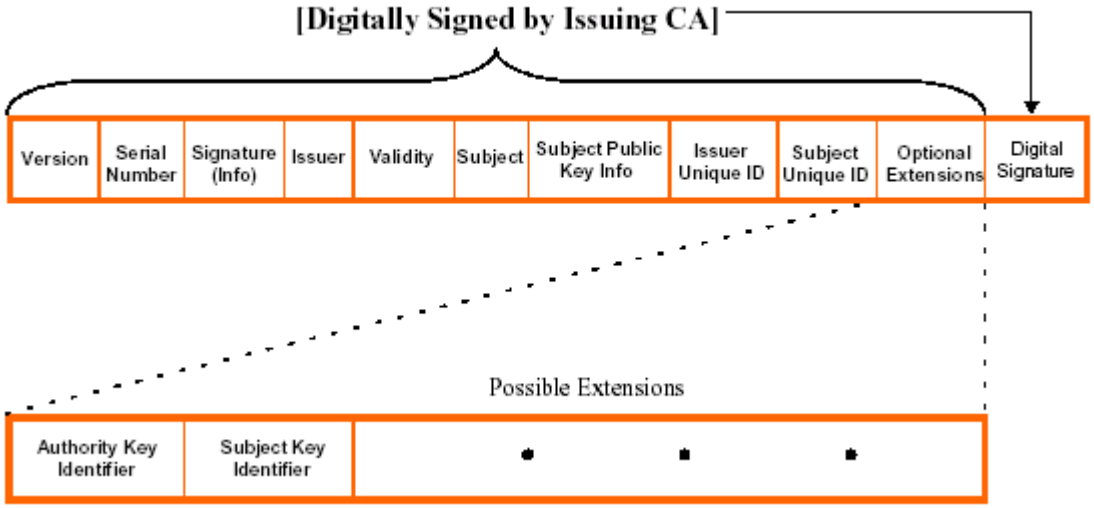
$CA\langle\langle A\rangle\rangle = CA\{V, SN, AI, CA, T_A, A, Ap\}$



(a) X.509 Certificate

Formato do Certificado (3)

- **Extensões do certificado X.509**
  - **permitem adicionar mais atributos ao certificado digital**



Formato do Certificado (4)

- **Exemplo dos campos de um certificado**

0	VERSION
123456789101112131 4	SERIAL NUMBER
RSA+SHA1, 2048	SIGNATURE ALGORITHM
C=US, S=VA, O=GMU, OU=ISE	ISSUER NAME
1/1/03-3/3/03	VALIDITY
C=US, S=VA, O=GMU, OU=ISE, CN=FPP	SUBJECT
RSA, 1024, xxxxxxxxxxxxxxxxxxxxxxxxxxx	SUBJECT PUBLIC KEY INFO
SIGNATURE	SIGNATURE

X.509 Versão 3 (1)

- Resolver limitações das versões anteriores
  - Campo *Subject* muito pequeno não permitia a inclusão de detalhes necerssários (por exemplo *links* ou endereços de *email*)
  - Não há informação sobre a política de segurança (por exemplo para usar no IPSec)
  - Limitar os efeitos de um CA malicioso através de restrições.
  - Identificação das diferentes chaves utilizadas pelo mesmo utilizador em tempos distintos, para gerir o ciclo de vida dos certificados
- Utilização de extensões opcionais
  - Identificador da extensão
  - Indicador crítico (indica se pode ser ignorado ou não)
  - Valor
  - Extensões podem ser de três tipos:
    - Chave e informação sobre a política
    - Atributos do Issuer
    - Restrições do caminho de certificação

X.509 Versão 3 (2)

- Chave e informação sobre a política
  - ***Authority Key Identifier***: indica a chave pública a usar para verificar o certificado
  - ***Subject Key Identifier***: identifica a chave pública certificada
  - ***Key Usage***: indica restrições à utilização do certificado (assinatura digital, não repudiação, cifragem, etc)
  - ***Private-key Usage Period***: a validade de uso da chave privada pode ser diferente da validade da chave pública (numa assinatura digital a chave privada normalmente tem validade inferior)
  - ***Certificate Policies***: usada quando existem várias políticas
  - ***Policy Mappings***: usado apenas nos certificados de um CA emitidos para outro CA

X.509 Versão 3 (3)

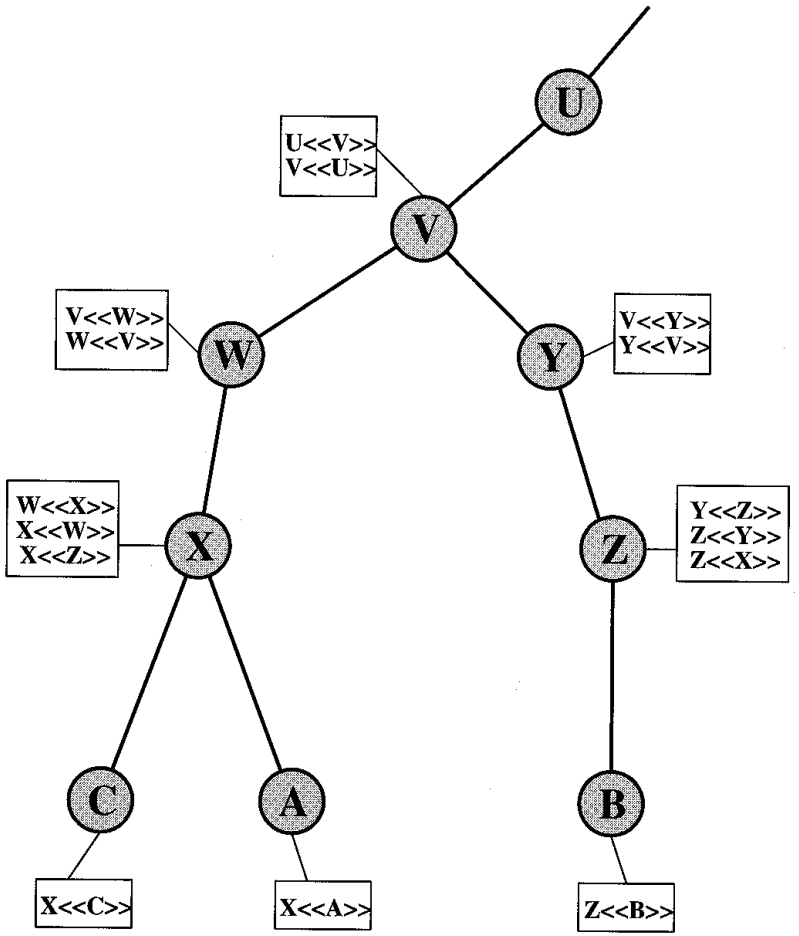
- Sujeito e Atributos da CA
  - ***Subject alternative name***
  - ***Issuer alternative name***
  - ***Subject directory attributes***: permite adicionar qualquer atributo da directoria X.500
- Restrições do caminho de certificação
  - ***Basic constraints***: indica se o sujeito pode actuar como CA
  - ***Name constraints***: indica um espaço de nomes (semelhante ao DNS)
  - ***Policy constraints***

Cadeias de Certificados (1)

- Qualquer utilizador com acesso à chave pública da CA pode recuperar a chave pública certificada
- Nenhuma outra parte, além da CA, pode modificar o certificado sem que seja detectado
- Quando há muitos utilizadores, eles são distribuídos por várias CAs
- A autenticação entre dois utilizadores de diferentes CA's:
  - X1<< X2 >> X2<< X3 >> … XN<< B >>

Cadeias de Certificados (2)

- *Forward certificates*
  - Certificados de X gerados por outros CAs
- *Reverse certificates*
  - Certificados gerados por X, que certificam outros CAs

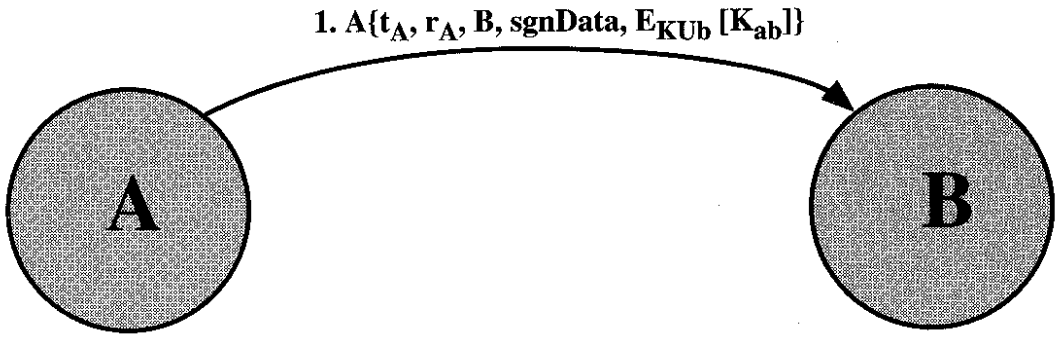


Procedimentos de autenticação (1)

- Existem várias forma de autenticação (assumindo que ambas as entidades conhecem as chaves públicas uma da outra)
  - Autenticação *one-way*
  - Autenticação *two-way*
  - Autenticação *three-way*

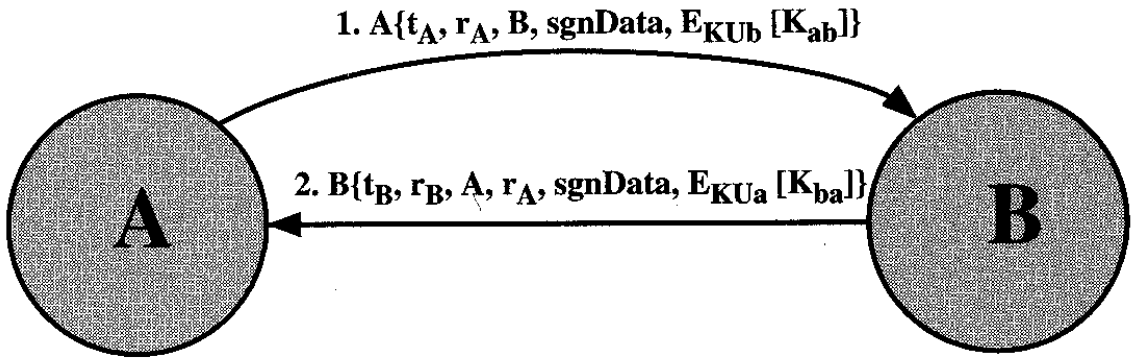
Procedimentos de autenticação (2)

- Autenticação *one-way*
  - Envio de apenas uma mensagem que garante:
    - A autenticidade de *A* e que a mensagem foi criada por *A*
    - Que o destinatário de mensagem é *B*
    - A integridade da mensagem e a originalidade (que não foi enviada mais do que uma vez)
- Não é verificada a identidade de *B*



Procedimentos de autenticação (3)

- Autenticação *two-way*
  - Envio de duas mensagens, garante que:
    - A identidade de *B* e que a mensagem de resposta foi gerada por *B*
    - Que a mensagem se destina a *A*
    - A integridade e originalidade da resposta
- Permite a identificação de ambas as entidades



Procedimentos de autenticação (4)

- Autenticação *three-way*
  - Devolvida uma mensagem $A \rightarrow B$ com o *nounce* r_B assinado
  - Utilizado quando não há sincronização de relógios na transmissão