

# Gestão de Chaves Assimétricas

# Problemas a resolver

## Garantir a utilização apropriada dos pares de chaves

- **Privacidade das Chaves Privadas**
  - Para garantir autenticidade
  - Para prevenir a repudiação das assinaturas
- **Distribuição correta das chaves públicas**
  - Para garantir confidencialidade
  - Para garantir a validação correta das assinaturas digitais

# Problemas a resolver

## **Evolução temporal do mapeamento entre entidade<->par de chaves**

- **Lidar com ocorrências catastróficas**
  - Perda de chave privada
- **Lidar com requisitos básicos da sua exploração**
  - Atualizar pares para reduzir riscos de impersonificação

# Problemas a resolver

## **Garantir a geração correta dos pares de chaves**

- **Garantir uma qualidade dos pares de chave**
  - Aleatoriedade do gerador dos valores secretos
  - Evitar que possam ser adivinhados
- **Melhorias da eficiência sem comprometer a segurança**
  - Tornar os mecanismos mais úteis
  - Aumentar a performance

# Objetivos

## 1. Geração de pares de chaves

- Quando e como devem ser gerados

## 2. Manuseamento de chaves privadas

- Como manter privadas

## 3. Distribuição de chaves públicas

- Como devem ser distribuídas para todo o mundo

## 4. Ciclo de vida dos pares de chaves

- Qual a sua expiração
- Como podem ser utilizadas
- Como verificar a sua obsolescência

# Geração de Chaves: Princípios

## Utilizar geradores bons na produção de segredos

- **Resultado é indistinguível de ruído**
  - Todos os valores possuem probabilidade igual
  - Não existem padrões derivados no número da iteração ou valores anteriores
- **Exemplo: Gerador de Bernoulli**
  - Gerador sem memória
  - $P(b=1) = P(b=0) = 1/2$
  - Igual a atirar uma moeda perfeita ao ar

# Geração de Chaves: Princípios

**Facilitar os processos sem comprometer a segurança**

- **Chaves públicas eficientes**

- Dimensão reduzida, tipicamente valores  $2^k+1$  (**3, 17, 65537**)
- Acelera operações com chaves públicas
- Não adiciona questões de segurança

# Geração de Chaves: Princípios

**A chave privada deve ser *gerada pelo próprio***

- **Para assegurar ao máximo a sua privacidade**
  - Apenas o seu dono possui a chave
  - Melhor: O dono também não ter a chave, apenas acesso aos processos com ela
- **Este princípio pode ser relaxado se não se pretender assinaturas digitais**
  - Onde não existem questões relacionadas com não repudiação

# Utilização de Chaves Privadas: Cuidados

## Correção

- **A chave privada representa um sujeito**
  - ex: um cidadão
  - O risco do seu comprometimento deve ser minimizado
  - Considerar igualmente cópias de salvaguarda
- **O caminho de acesso à chave deve ser controlado**
  - Correção das aplicações que a usam
  - Utilização de autenticação nas aplicações
  - Cifra da chave privada

# Utilização de Chaves Privadas: Cuidados

## Confinamento

- **Armazenamento da chave numa entidade autónoma segura**
  - Módulo seguro de hardware interno
  - Partição lógica segura a nível do CPU
  - Smartcard ou chave externa
- **Utilização protegida da chave**
  - Aplicações não utilizam a chave
  - Invoca-se ao dispositivo a realização de operações

# Distribuição de Chaves Públicas

- **Problema: Como distribuir uma chave pública ao mundo?**
- **Distribuição a quem pretenda enviar informação confidencial**
  - Distribuição manual
  - Distribuir protegida por um segredo partilhado
  - Distribuir de forma Ad-hoc usando certificados digitais
- **Distribuição a quem pretenda validar informação autenticada**
  - Distribuição manual
  - Distribuição de forma Ad-hoc usando certificados digitais

# Distribuição de Chaves Públicas

- **Problema: Como garantir a correção de uma chave pública?**
- **Disseminação confiável de chaves públicas**
  - Usar caminhos ou grafos de relações de confiança

**Se A confia em  $K_x+$ , e B confia em A,**

**então B confia em  $K_x+$**

- **Hierarquias e grafos de certificação**
  - Expressão clara das relações de confiança entre entidades
  - Certificação é unidirecional

# Certificados digitais de chaves públicas

**Documentos digitais emitidos por uma Entidade Certificadora (EC)/Certification Authority (CA)**

- **Ligam uma chave pública a uma entidade**
  - Pessoa, sistema ou serviço
- **São documentos públicos**
  - Contém apenas informação pública
  - Podem contém informação adicional associada à entidade
- **São seguros por meios criptográficos**
  - Possuem uma impressão digital para identificação
  - São assinados com uma assinatura digital criada pelo emissor (CA)

# Certificados digitais de chaves públicas

**Usados para distribuir chaves públicas de forma confiável**

- **Os verificadores podem validar os documentos**
  - Validar identificação com o contexto atual
  - Validar instantes temporais
  - Validar a utilização da chave pública
  - Validam a assinatura digital do documento usando a chave pública da CA
- **Os verificadores confiam no comportamento das CA**
  - Portanto confiam nos documentos que emitem
  - Se uma CA associou uma chave pública a A, se o verificador confiar na CA, irá confiar que a associação de A é correta.

# Certificados digitais de chaves públicas

- **Norma X.509v3**
  - Campos obrigatórios
    - Versão
    - Sujeito (subject)
    - Chave pública
    - Datas (início e expiração)
    - Emissor (issuer)
    - Assinatura
    - ...
  - Extensões: definem utilização
    - Críticas ou não Críticas
- **PKCS #6**
  - Extended-Certificate Syntax Standard
- **Formatos binários**
  - ASN.1 (Abstract Syntax Notation
    - DER, CER, BER, etc.
  - PKCS #7
    - Cryptographic Message Syntax Standard
  - PKCS #12
    - Personal Information Exchange Syntax Standard
- **Outros formatos**
  - PEM (Privacy Enhanced Email)
    - Base64

# Utilizações de um par de chaves

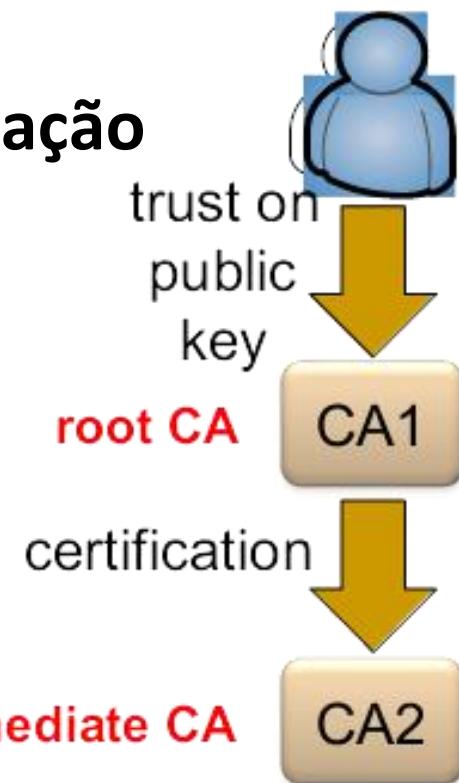
- O certificado associa um par de chaves a um perfil de utilização restrito
  - Uma entidade terá vários certificados, um para cada utilização
  - Definido no certificado, extensão crítica: Key Usage
- Perfis típicos
  - Autenticação/Distribuição de chaves
    - Assinaturas digitais, Cifra de Chaves, Cifra de Dados, Negociação de chaves
  - Assinatura de documentos
    - Assinaturas digitais, Não-repudiação
  - Emissão de certificados
    - Assinaturas de certificados e objetos relacionados

# Entidades Certificadoras

- **Organizações que gerem certificados de chave pública**
  - Empresas, entidades sem fins lucrativos ou governamentais
  - Normalmente possuem a tarefa de validar associações chave-entidade
    - Importante que operem corretamente para serem confiáveis
- **Definem políticas e mecanismos para**
  - Emissão de certificados
  - Revogação de certificados
  - Distribuição de certificados
  - Emitir e distribuir as chaves privadas correspondentes
- **Gerem processos de revogação de certificados**
  - Listas de identificadores de certificados revogados
  - Interfaces para verificação do estado do certificado

# Entidades Certificadoras Confiáveis

- **Entidades certificadores em que um sujeito confia**
  - Podem ser confiáveis por um grupo restrito, ou uma maioria
  - Possuem processos de gestão confiáveis
    - Isto tem custos
- **Raízes de confiança ou raízes de certificação**
  - Alguém possui e confia numa chave pública
  - Certificados das CAs são auto assinadas
    - Podem também ser assinados por outras CAs
  - Distribuição Manual
    - nos browsers, no SO



U  
C  
S  
A  
E  
S  
E[General](#) [Details](#)**This certificate has been verified for the following uses:**

SSL Client Certificate

SSL Server Certificate

**Issued To**

Common Name (CN) www.ua.pt

Organization (O) Universidade de Aveiro

Organizational Unit (OU) sTIC

Serial Number 06:B4:17:0C:D7:EF:AC:9F:A3:79:9A:78:0E:7E:5A:8C

**Issued By**

Common Name (CN) TERENA SSL CA 3

Organization (O) TERENA

Organizational Unit (OU) &lt;Not Part Of Certificate&gt;

**Period of Validity**

Begins On May 27, 2019

Expires On June 3, 2021

**Fingerprints**SHA-256 Fingerprint 6C:BA:BD:A1:7E:A9:8D:EA:7B:18:22:44:EC:71:D5:41:4D:08:D  
4:A6:FC:48:1B:3C:9B:05:EB:DA:69:A6:A5:EE

SHA1 Fingerprint 17:79:15:B5:0E:E0:34:51:2D:FA:DE:DF:77:1E:E1:0A:B3:4B:2F:2B

[Close](#)

U  
C  
S  
A  
E  
S  
E

General Details

**Certificate Hierarchy**

- ▼ DigiCert Assured ID Root CA
  - ▼ TERENA SSL CA 3
    - www.ua.pt

**Certificate Fields**

- ▼ www.ua.pt
  - ▼ Certificate
    - Version
    - Serial Number
    - Certificate Signature Algorithm
    - Issuer
  - Validity
    - Subject
  - ▼ Subject Public Key Info
    - Subject Public Key Algorithm

**Field Value**

CN = www.ua.pt  
OU = sTIC  
O = Universidade de Aveiro  
L = Aveiro  
C = PT

[Export...](#)[Close](#)

General Details**This certificate has been verified for the following uses:**

SSL Certificate Authority

• f

**Issued To**

Common Name (CN) TERENA SSL CA 3  
Organization (O) TERENA  
Organizational Unit (OU) <Not Part Of Certificate>  
Serial Number 08:70:BC:C5:AF:3F:DB:95:9A:91:CB:6A:EE:EF:E4:65

**Issued By**

Common Name (CN) DigiCert Assured ID Root CA  
Organization (O) DigiCert Inc  
Organizational Unit (OU) www.digicert.com

**Period of Validity**

Begins On November 18, 2014  
Expires On November 18, 2024

**Fingerprints**

SHA-256 Fingerprint BE:B8:EF:E9:B1:A7:3C:84:1B:37:5A:90:E5:FF:F8:04:88:48:E3:  
A2:AF:66:F6:C4:DD:7B:93:8D:6F:E8:C5:D8  
SHA1 Fingerprint 77:B9:9B:B2:BD:75:22:E1:7E:C0:99:EA:71:77:51:6F:27:78:7C:AD

Close



General Details

**This certificate has been verified for the following uses:**

SSL Certificate Authority

**Issued To**

Common Name (CN)	TERENA SSL CA 3
Organization (O)	TERENA
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	08:70:BC:C5:AF:3F:DB:95:9A:91:CB:6A:EE:EF:E4:65

**Issued By**

Common Name (CN)	DigiCert Assured ID Root CA
Organization (O)	DigiCert Inc
Organizational Unit (OU)	www.digicert.com

CA Intermédia  
(Certificado emitido por  
outra CA)

**Period of Validity**

Begins On	November 18, 2014
Expires On	November 18, 2024

**Fingerprints**

SHA-256 Fingerprint	BE:B8:EF:E9:B1:A7:3C:84:1B:37:5A:90:E5:FF:F8:04:88:48:E3: A2:AF:66:F6:C4:DD:7B:93:8D:6F:E8:C5:D8
SHA1 Fingerprint	77:B9:9B:B2:BD:75:22:E1:7E:C0:99:EA:71:77:51:6F:27:78:7C:AD

**Close**



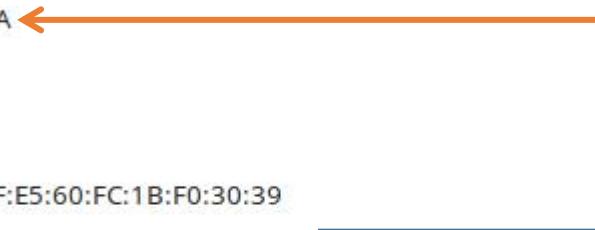
General Details

**This certificate has been verified for the following uses:**

SSL Certificate Authority

**Issued To**

Common Name (CN)	DigiCert Assured ID Root CA
Organization (O)	DigiCert Inc
Organizational Unit (OU)	www.digicert.com
Serial Number	0C:E7:E0:E5:17:D8:46:FE:8F:E5:60:FC:1B:F0:30:39

**Issued By**

Common Name (CN)	DigiCert Assured ID Root CA
Organization (O)	DigiCert Inc
Organizational Unit (OU)	www.digicert.com

CA Raiz  
(Certificado auto-emitido)

**Period of Validity**

Begins On	November 10, 2006
Expires On	November 10, 2031

**Fingerprints**

SHA-256 Fingerprint	3E:90:99:B5:01:5E:8F:48:6C:00:BC:EA:9D:11:1E:E7:21:FA:BA: 35:5A:89:BC:F1:DF:69:56:1E:3D:C6:32:5C
SHA1 Fingerprint	05:63:B8:63:0D:62:D7:5A:BB:C8:AB:1E:4B:DF:B5:A8:99:B2:4D:43

Close

# Hierarquias de Certificação: modelo PEM

- **PEM: Privacy-enhanced Electronic Email**
- **Proposto pelo IETF em 1993 (ERF1421-1423)**
- **Modelo de Monopólio**
  - Uma raiz única: IPRA (Internet Policy Registration Authority)
  - Várias PCA (Policy Creation Authorities) abaixo da raiz
  - Várias CAs abaixo de cada PCA
    - Pertencentes a organizações e empresas
  - Forma uma cadeira de certificação
    - Árvore de raiz única

# Hierarquias de Certificação: modelo PEM

- **Modelo nunca foi implementado globalmente**
  - Exceto pequenas implementações (90s)
- **Preferido: Floresta de hierarquias em cada CA, sem uma IPRA**
  - Hierarquias independentes sem uma raiz única
  - Oligarquia
- **Cada CA raiz negocia a distribuição da sua chave pública em cada entidade**
  - Entidade: Browsers, Distribuições, Sistemas, Sistema Operativos

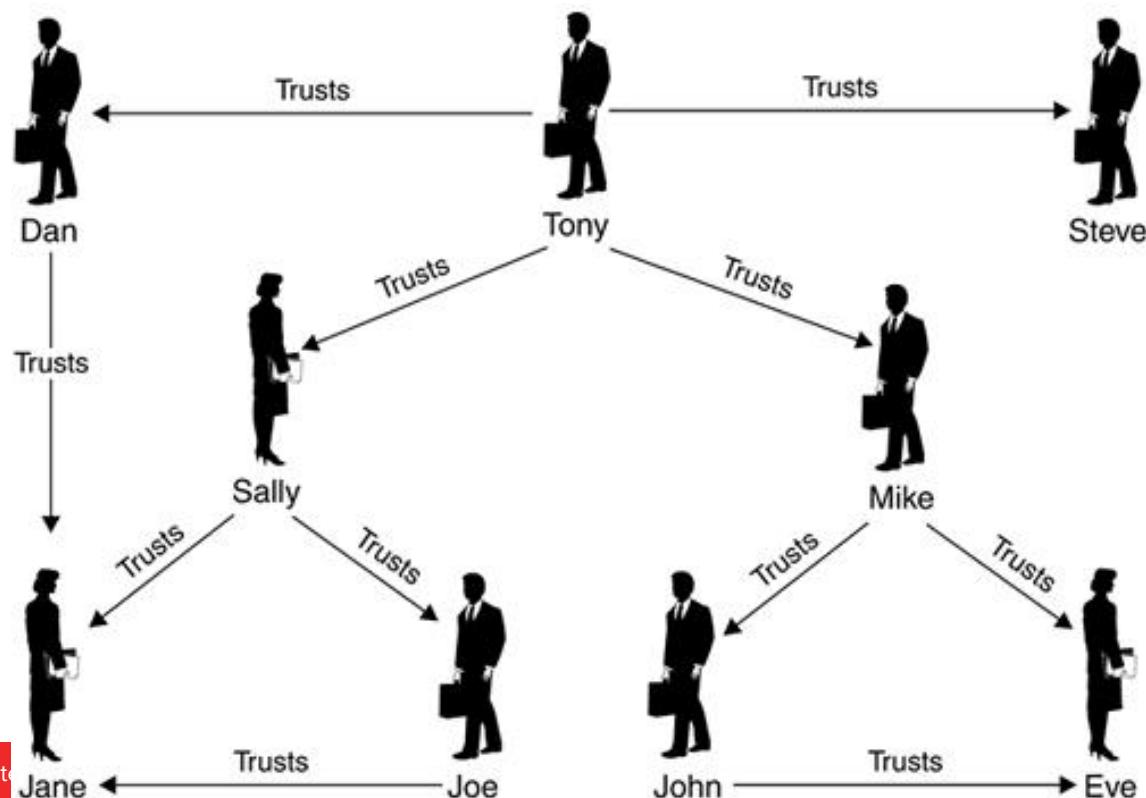
# Hierarquias de Certificação: Modelo PGP (Pretty Good Privacy)

- **Segue um modelo baseado numa rede de confiança**
  - E não numa árvore
- **Sem qualquer autoridade central de confiança**
  - Qualquer pessoa/entidade é um potencial certificador
  - Qualquer pessoa/entidade pode certificar uma chave pública e publicar a assinatura para os outros
- **Pessoas usam dois tipos de confiança**
  - Confiança nas chaves que conhecem
    - Validadas diretamente por qualquer meio (presença, telefone,...)
  - Confiança no comportamento de outros certificadores
    - Assumindo que verificam as chaves que certificam

# Hierarquias de Certificação: Modelo PGP (Pretty Good Privacy)

## Confiança Transitiva

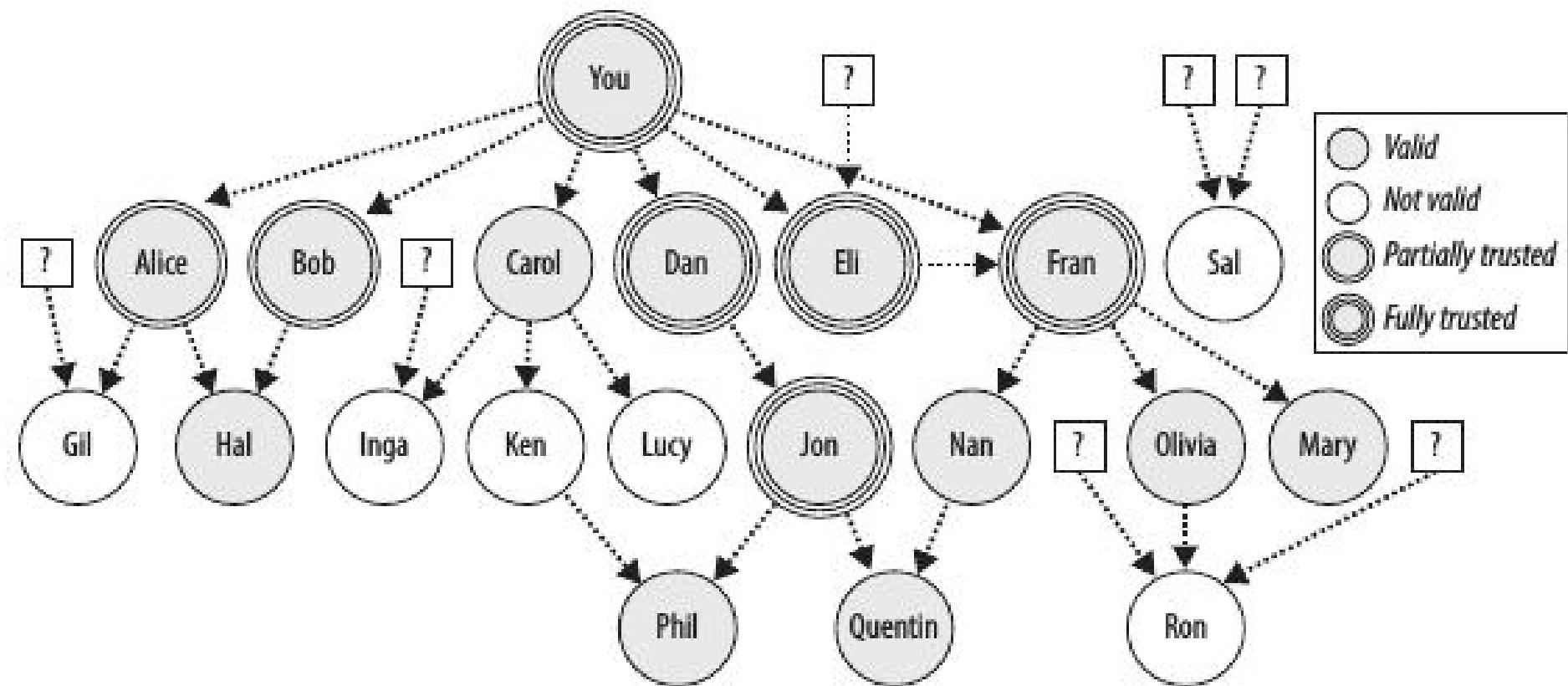
**SE Mike confia que o John é um certificador correto,  
E John certificou a chave pública da Eve,  
ENTÃO Mike confia na chave pública da Eve**



# Hierarquias de Certificação: Modelo PGP (Pretty Good Privacy)

- **Confiança: Quando uma pessoa confia noutra pessoa**
  - Confiança é unidirecional, pessoal e subjetiva
  - Níveis:
    - Ultimate: chaves próprias das quais se tem a chave privada
    - Complete
    - Marginal
    - NoTrust (ou Untrusted)
- **Validade: Quanta verificação a chave possui**
  - Válida:
    - A confia completamente em B
    - ou A confia marginalmente em C e D
    - e D ou B em conjunto com C assinaram a chave de E
  - Marginalmente Válida:
    - A confia marginalmente em B e B assinou a chave de E
  - Inválida: sem um caminho

# Hierarquias de Certificação: Modelo PGP (Pretty Good Privacy)



# Refrescamento de chaves assimétricas

- **Pares de chaves devem ter uma validade limitada**
  - Porque as chaves privadas podem ser perdidas ou descobertas
  - Para implementar mecanismos de atualização periódicos
- **Problemas:**
  - Os certificados podem ser copiados e distribuídos livremente
  - O universo de possuidores de certificados é desconhecido
    - Não é viável contactar todos os possuidores de certificados para eliminar certificados específicos
- **Soluções:**
  - Certificados com uma validade temporal definida (não antes, não depois)
  - Listas de Revogação de Certificados (CRL)
    - Para permitir revogar certificados antes que expirem

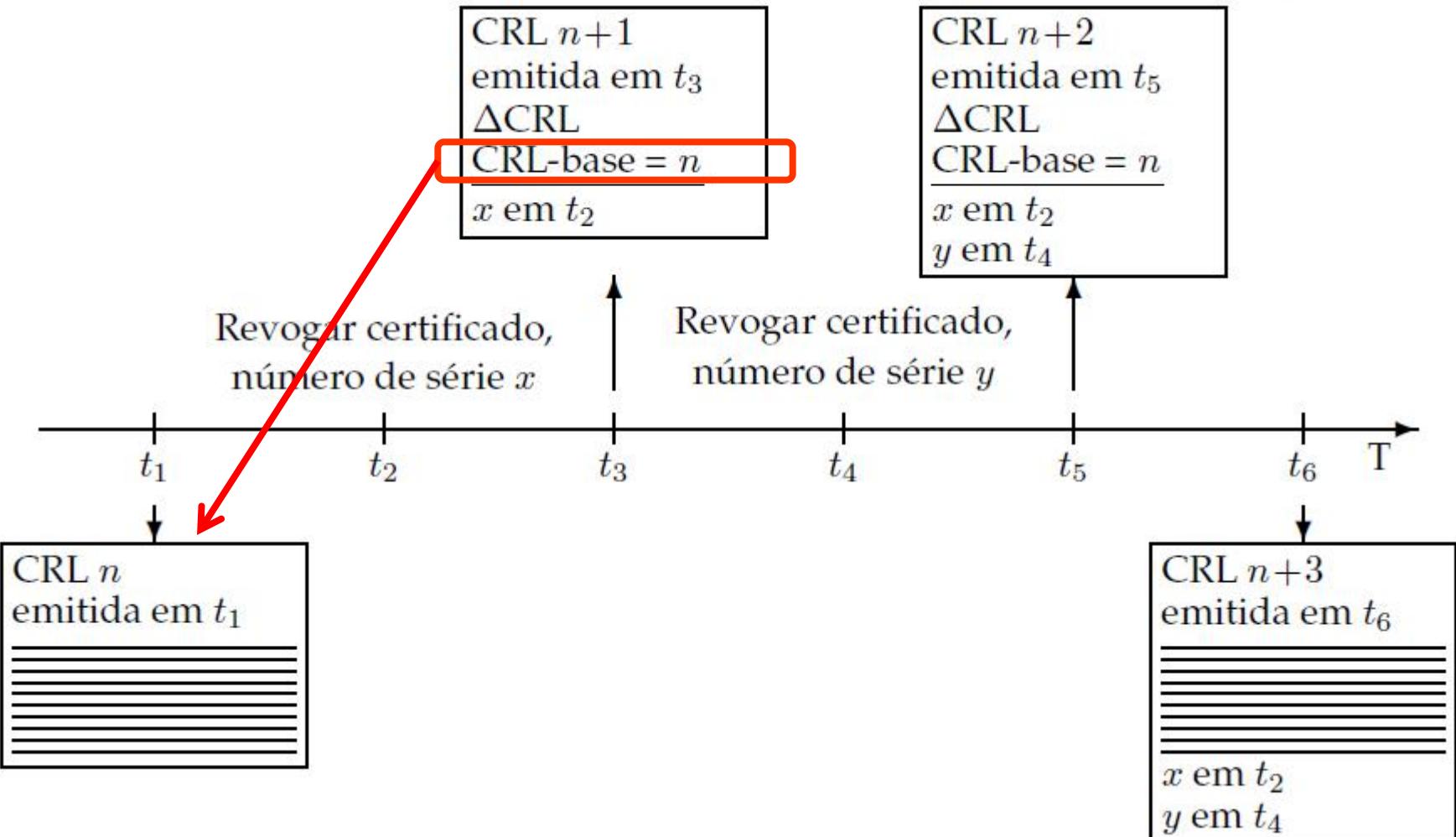
# Listas de Revogação de Certificados (CRL)

- **Listas assinadas com identificadores de certificados revogados prematuramente**
  - Devem ser consultadas periodicamente pelos verificadores
  - Entradas podem conter a razão
- **Publicação e distribuição de CRLs**
  - Cada CA possui a sua CRL
  - De acesso público
  - CAs trocam CRLs para facilitar distribuição
- **Vários formatos disponíveis**
  - Base CRL: Lista completa com todos os certificados revogados
  - Delta CRL: Lista com as diferenças desde a última Base CRL
  - OCSP: API para verificação individual de cada certificado

## RFC 3280

unspecified (0)  
keyCompromise (1)  
CACompromise (2)  
affiliationChanged (3)  
superseded (4)  
cessationOfOperation (5)  
certificateHold (6)  
  
removeFromCRL (8)  
privilegeWithdrawn (9)  
AACompromise (10)

# Base CRL, Delta CRL e Revogação



# Online Certificate Status Protocol

- **Protocolo baseado em HTTP para verificar a revogação de certificados**
  - Pedido inclui o número de série do certificado
  - Resposta assinada afirma qual o estado
  - Uma verificação por certificado
- **Reduz a largura de banda usada pelos clientes**
  - Um pedido por certificado, em vez de toda a lista (Base CRL)
- **Pode envolver maior largura de banda para as CAs**
  - Se clientes validarem sempre os certificados
  - Pode comprometer a privacidade. CA sabe quando um sistema acede a um serviço
- **OCSP Stapling**
  - Inclui um instante temporal assinado na resposta
  - Clientes podem guardar respostas durante a sua validade

# Distribuição de certificados de chave pública

- **Transparente e integrado nos sistemas e aplicações**
  - Sistemas de Diretórios
    - Grandes escala: usando X.500 através de LDAP
    - Organizações: Windows Active Directory, Manualmente
  - Online: incluído nos protocolos
    - comunicações seguras usando TLS
    - Assinaturas digitais de correio com MIME ou em documentos
  - Pré-distribuição
    - Incluído nas aplicações, Sistemas Operativos
- **Explicitamente pelos utilizadores**
  - Utilizador pede um certificado específico
    - Por email, acesso a uma página HTTP

# PKI: Public Key Infraestruture

## Infraestrutura de apoio ao uso de pares de chaves e certificados

- **Criação segura de pares de chaves assimétricas**
  - Políticas de subscrição
  - Políticas de geração de pares de chaves
- **Criação e distribuição de certificados de chaves públicas**
  - Políticas de subscrição
  - Definição de atributos do certificado
- **Definição e uso de cadeias de certificação**
  - Inserção numa hierarquia de certificação
  - Certificação de outras CAs
- **Atualização, publicação e consulta de listas de certificados revogados**
  - Políticas para revogar certificados
  - Distribuição permanente de CRLs
  - Serviço OCSP
- **Uso de estruturas de dados e protocolos que permitem a interoperação entre componentes**

# PKI: Políticas do Cartão de Cidadão

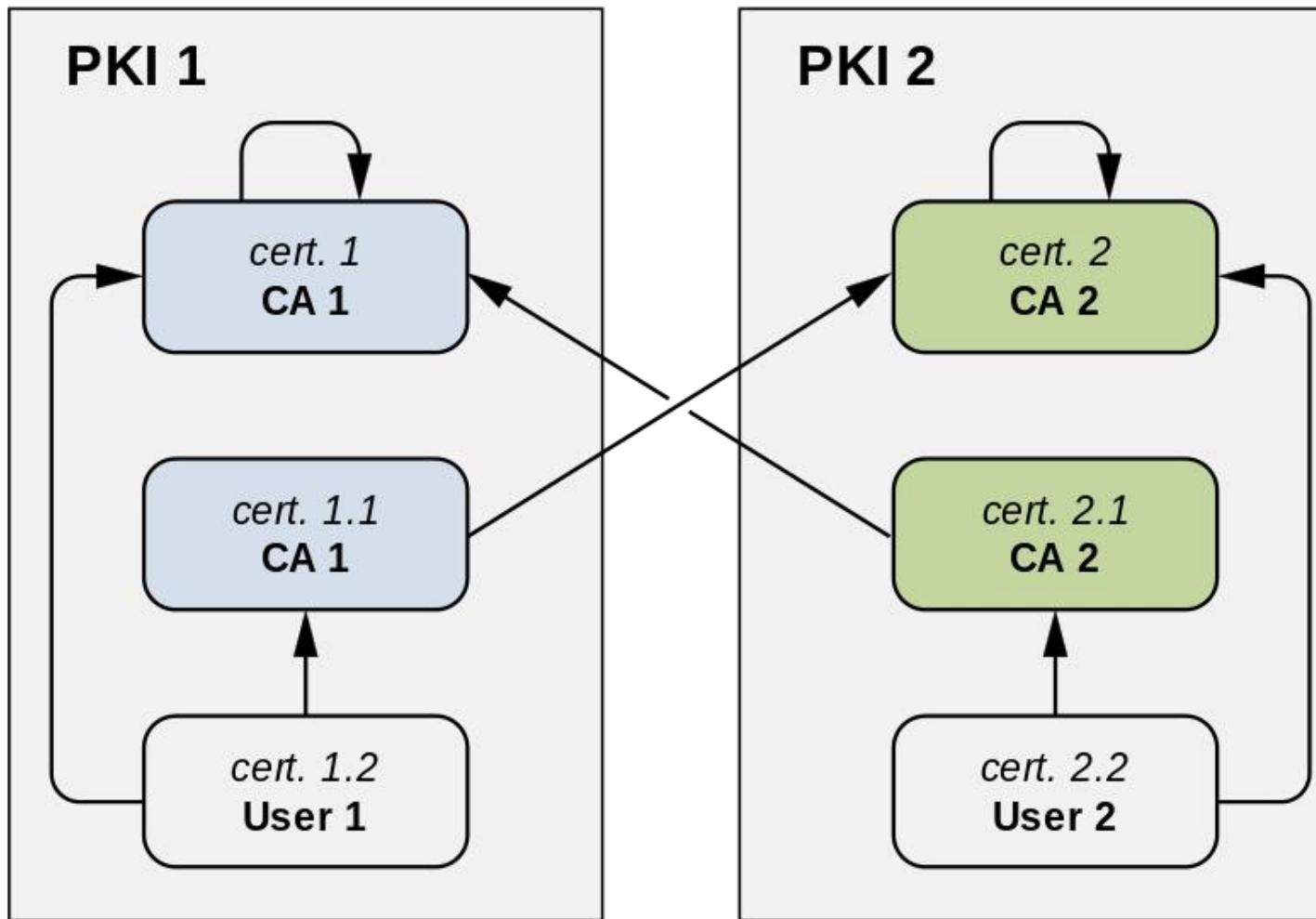
- **Subscrição**
  - Em locais próprios, pessoal
- **Vários pares de chaves por pessoa**
  - Um para autenticação
  - Uma para assinaturas qualificadas
  - Gerados no cartão, não exportáveis
  - Requerem um PIN em cada operação
- **Uso autorizado dos certificados**
  - Autenticação
    - SSL Client Certificate, Email (Netscape cert. type)
    - Signing, Key Agreement (key usage)
- **Assinatura**
  - Email (**Netscape cert. type**)
  - Non-repudiation (**key usage**)
- **Caminho de certificação**
  - Raiz bem conhecida e divulgada
    - GTE Cyber Trust Global Root
    - Baltimore CyberTrust Root
    - MULTICERT Root Certification Authority 01
  - CA raiz PT debaixo da GTE/Baltimore/Multicert
  - CA raiz CC debaixo de CA raiz PT
  - CAs Autenticação CC e Assinatura CC debaixo CA raiz CC
- **CRLs**
  - Certific. de assinatura pré-revogados
    - Removida se o dono explicitamente requerer o uso de assinaturas
  - Todos os certificados são removidos a pedido do dono
    - Mediante a apresentação de um PIN de revogação
  - Pontos de distribuição das CRL indicados em cada certificado

<https://censys.io/certificates/01c2a9b0fc202e34d471011d1b246fb106d3be5faf4c3eba6ca4b8283aa2bc4d>

# PKI: Relações de Confiança

- Um PKI estabelece relações de confiança de duas formas
  - Emitindo certificados de chaves públicas de outras CAs
    - Abaixo na hierarquia; ou
    - Não relacionadas hierarquicamente
  - Requerendo a certificação da sua chave pública a outras CAs
    - Acima na hierarquia; ou
    - Não relacionadas hierarquicamente
- Relações de confiança características
  - Hierárquicas
  - Cruzadas (A certifica B e vice-versa)
  - Ad-hoc (meshed)
    - Grafos mais ou menos complexos de certificação

# PKI: Certificação Hierárquica e Cruzada



Créditos: Wikimedia Foundation

# Fixação de Certificados (Pinning)

- **Se um atacante possui acesso a uma raiz de confiança, ele pode emitir qualquer certificado para qualquer entidade**
  - Manipular a CA para que ela emita um certificado (difícil)
  - Injetar raízes adicionais nos sistemas da vítima (mais fácil)
- **Certificate Pinning: Adicionar uma impressão digital da chave pública ao código**
  - Impressão Digital usa SHA256
  - Associada a um pedido HTTP específico
- **Processo de validação normal + verificação de impressão digital**
  - Certificado tem de ser assinado por uma raiz de confiança
  - Certificado tem de ter uma chave pública com a impressão digital especificada

# Transparência de Certificação (RFC 6962 )

- **Problemas**
  - CAs podem ser comprometidas (Ex, DigiNotar)
    - Por atacantes maliciosos
    - Por governos, etc...
  - Comprometimento é difícil de detetar
    - Resulta na alteração das regras de funcionamento da PKI
    - Dono legítimo dificilmente saberá
- **Definição: Sistema que regista todos os certificados públicos emitidos**
  - Garante que só são publicados certificados que levam a raízes legítimas
  - Armazena toda a cadeia de certificação de cada certificado
  - Apresenta esta informação para auditoria
    - Organizações ou ad-hoc pelos utilizadores