Gestão de chaves assimétricas

SEGURANÇA INFORMÁTICA E NAS ORGANIZAÇÕES

Problemas a resolver

Assegurar uma geração apropriada dos pares de chaves

- Geração aleatória de valores secretos
- Aumentar eficiência sem reduzir a segurança

Assegurar um uso apropriado dos pares de chaves assimétricas

- Uso/conhecimento exclusivo das chaves privadas
  - Para impedir o repúdio das assinaturas digitais
- Distribuição correta das chaves públicas
  - Para assegurar confidencialidade
  - Para assegurar uma correta validação de assinaturas digitais

Evolução temporal das relações entidade⇔par de chaves

- Para lidar com situações catastróficas
  - ex. perda da chave privada
- Para lidar que requisitos operacionais normais
  - ex. refrescamento de pares de chaves para reduzir riscos de personificação

Gestão de chaves assimétricas: Objetivos

Geração de chaves

- Como e quando devem ser gerados pares de chaves

Uso de chaves privadas

- Como é protegida a sua privacidade

Distribuição de chaves públicas

- Como são distribuídas as chaves públicas correta e universalmente

Tempo de vida das chaves

- Durante quanto tempo devem as chaves ser usadas
- Como se verifica a obsolescência de pares de chaves

Geração de chaves assimétricas: Princípios

Usar bons geradores aleatórios para produzir segredos

- Gerador de Bernoulli com probabilidade ½
  - Gerador sem memória
  - P(b=1) = P(b=0) = ½

Facilitar sem comprometer a segurança

- Chaves públicas eficientes
  - Com poucos bits, tipicamente valores 2k+1 (3, 17, 65537)
  - Permitem acelerar um dos cálculos sem perda de segurança

A chave privada deve ser gerada pelo próprio

- Para assegurar ao máximo a sua privacidade
- Este princípio pode ser relaxado se não se pretender assinaturas digitais

Utilização de chaves privadas: Cuidados a ter

Uso correto

- A chave privada representa o próprio
  - O seu comprometimento tem que ser minimizado
  - Cópias de salvaguarda fisicamente seguras
- O caminho de acesso à chave privada deverá ser controlado
  - Proteção com senha
  - Correção das aplicações que a usam

Confinamento

- Salvaguarda e uso da chave privada num dispositivo autónomo (ex. smartcard)
  - O dispositivo gera pares de chaves
  - O dispositivo apenas envia para o exterior a chave pública
    - E nunca a privada
  - O dispositivo cifra/decifra dados com a chave privada

Distribuição de chaves públicas

Distribuição aos remetentes de dados confidenciais

- Manual
- Usando um segredo partilhado
- Distribuição ad hoc usando certificados digitais

Distribuição aos receptores de assinaturas digitais

- Distribuição ad hoc usando certificados digitais

Disseminação confiável da chave para terceiros

- Caminhos / grafos de confiança
  - Se A confia em KX+, e B confia em A, então B confia em KX+
- Hierarquias / grafos de certificação

Certificados digitais de chaves públicas

Documentos emitidos por uma Entidade Certificadora

- Certification Authority (CA)
- Associam uma chave (pública) a uma entidade
  - Pessoa, servidor, serviço
- São documentos públicos
  - Não contêm informação privada, apenas pública
- São criptograficamente seguros
  - Assinados digitalmente pelo emissor, não podem ser alterados

Úteis para a distribuição confiável de chaves públicas

- O recetor do certificado pode validar o mesmo
  - Usando a chave pública da CA
- Se confiar no assinante (CA) e a assinatura estiver correta, pode confiar na chave pública certificada
  - Como a CA confia na K+ certificada, se confiar em KCA+ pode confiar em K+

Certificados digitais de chaves públicas

Padrão X.509v3

- Campos obrigatórios
  - Versão
  - Sujeito (subject)
  - Chave pública
  - Datas (de emissão, de validade)
  - Emissor (issuer)
  - Assinatura
  - etc.
- Extensões

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 Mail)
- Codificações de X.509 em base64

Entidades Certificadoras

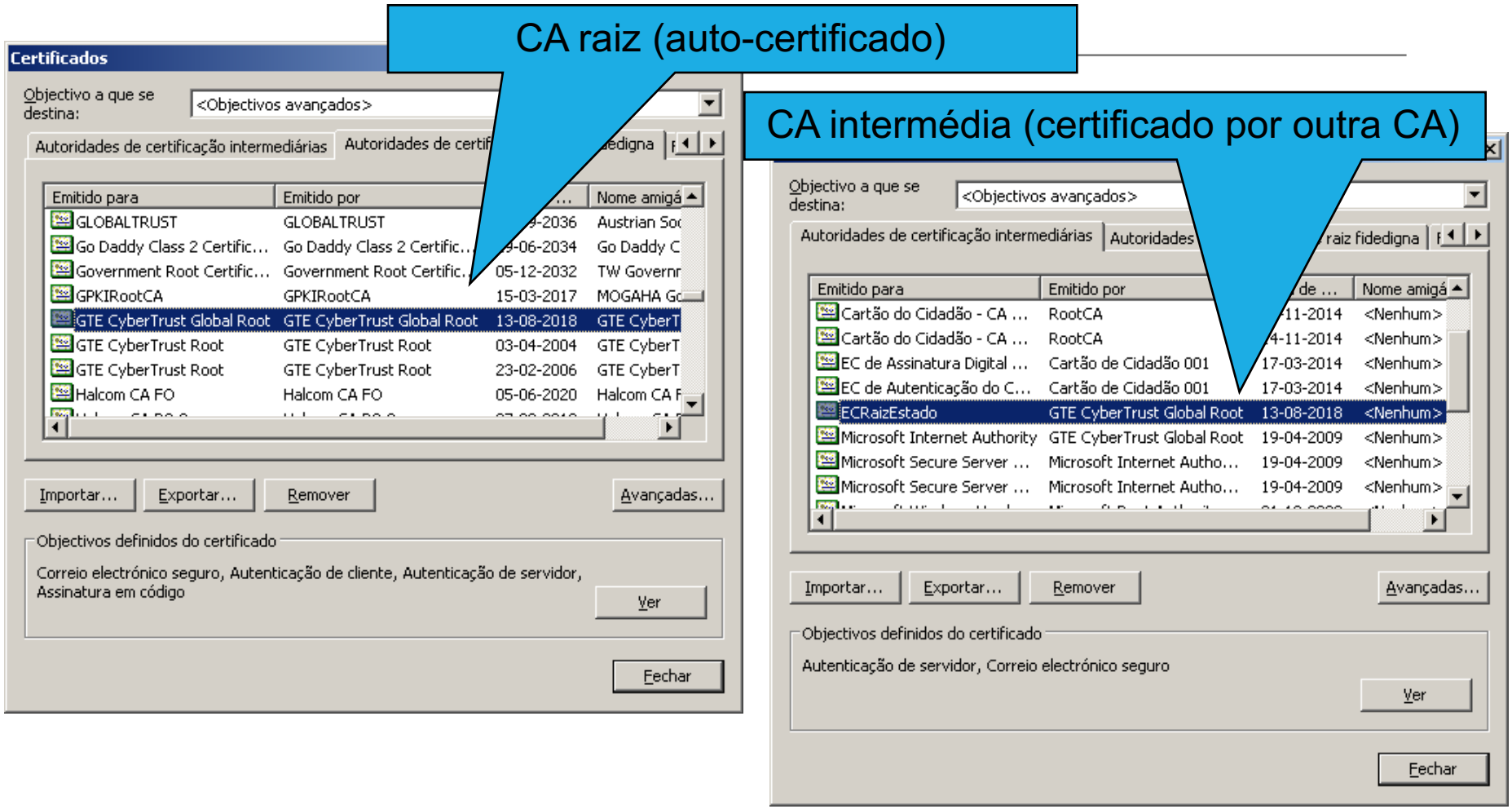
Organizações que gerem certificados

- Definem políticas e mecanismos para
  - Emitir certificados
  - Revogar certificados
  - Distribuir certificados
  - Emitir e distribuir as chaves privadas correspondentes
- Gerem listas de revogação de certificados
  - Listas de identificares de certificados revogados

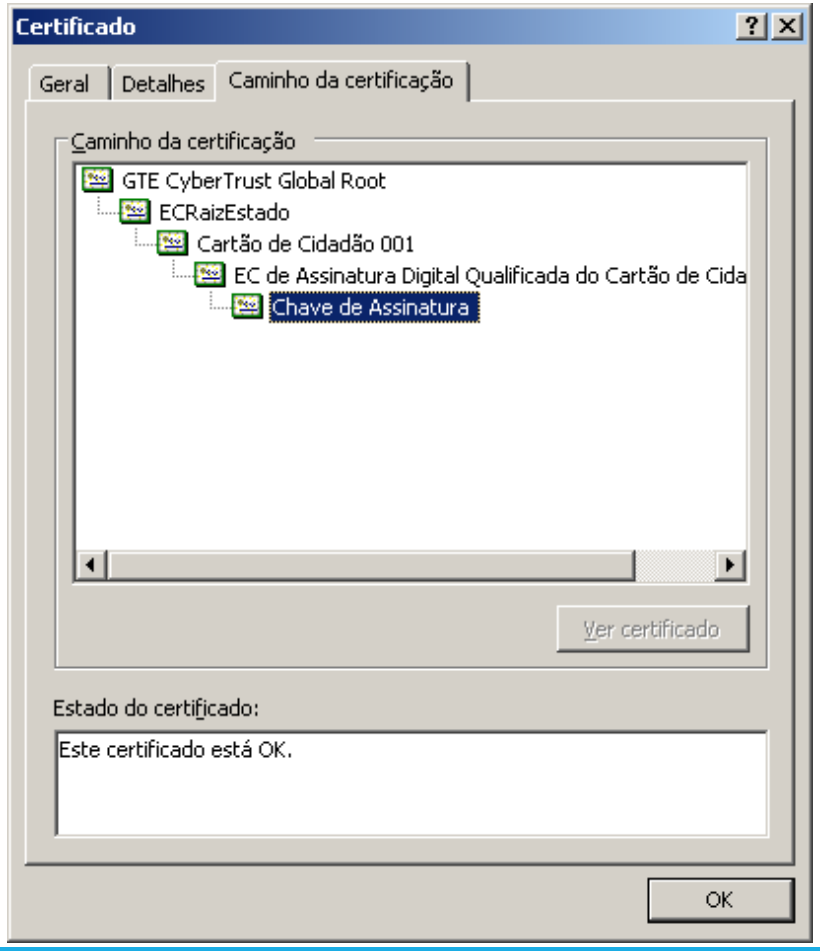
CAs confiáveis

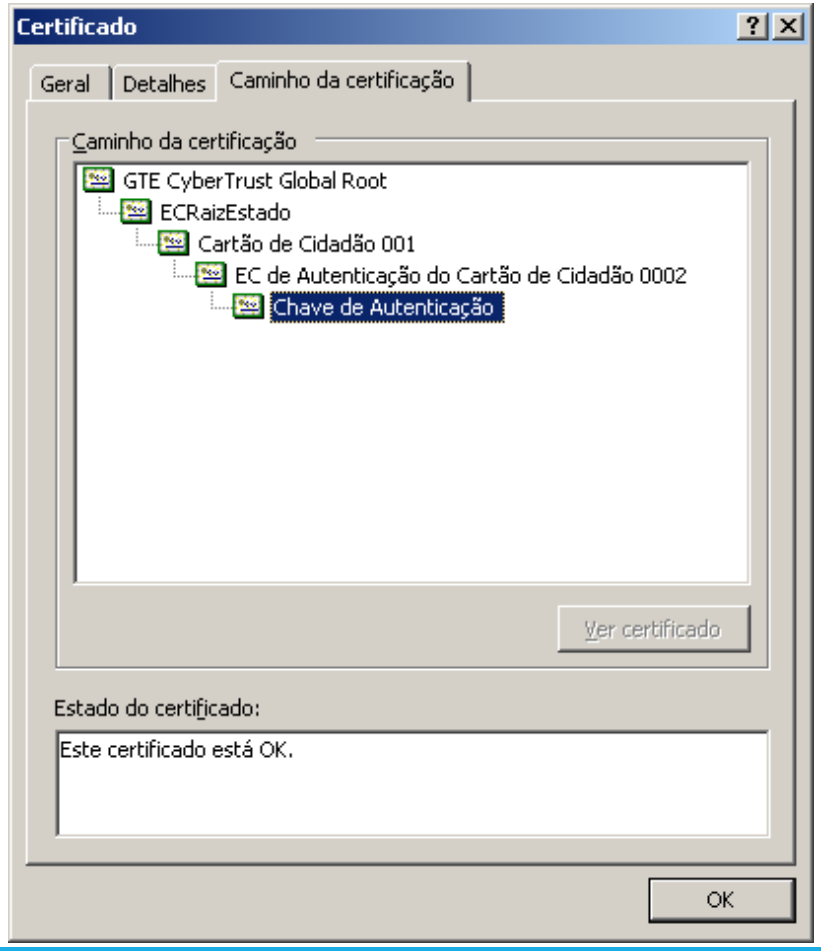
- CAs para as quais se possui uma chave pública confiável
  - Âncora de confiança
    - Normalmente concretizada através de certificados autoassinados (ou autocertificados, sujeito=emissor)
  - Distribuição manual das suas chaves públicas
    - ex. em navegadores (Internet Explorer, Netscape, etc.)
- CAs certificadas por outras CAs
  - Certificados de chaves públicas de CAs
  - Hierarquias de certificação

Distribuição manual de chaves públicas confiáveis (como certificados raiz): Exemplo Internet Explorer



Hierarquias (ou caminhos) de certificação: Exemplo do Cartão de Cidadão





Renovação de pares de chaves assimétricas

Os pares de chaves devem ter um período de validade limitado

- Porque as chaves privadas podem-se perder / ser descobertas
- Para lidar com políticas de alteração regular de chaves assimétricas

Problema

- Os certificados podem ser reproduzidos sem qualquer controlo
- Não se conhece o universo de detentores de um certificado que se pretende eliminar
  - Portanto, não se podem contactar para eliminar determinados certificados

Soluções

- Certificados com prazos de validade
- Listas de revogação de certificados
  - Para certificados revogados antes do termo do seu prazo de validade

Listas de certificados revogados

Certificate Revocation Lists (CRL)

- Base ou delta

São listas assinadas de identificadores de certificados revogados antecipadamente

- Devem ser consultadas regularmente pelos detentores de certificados
- Protocolo OCSP para certificados X.509 individuais
  - RFC 2560
- Podem indicar a justificação da revogação

Manutenção e divulgação das CRL

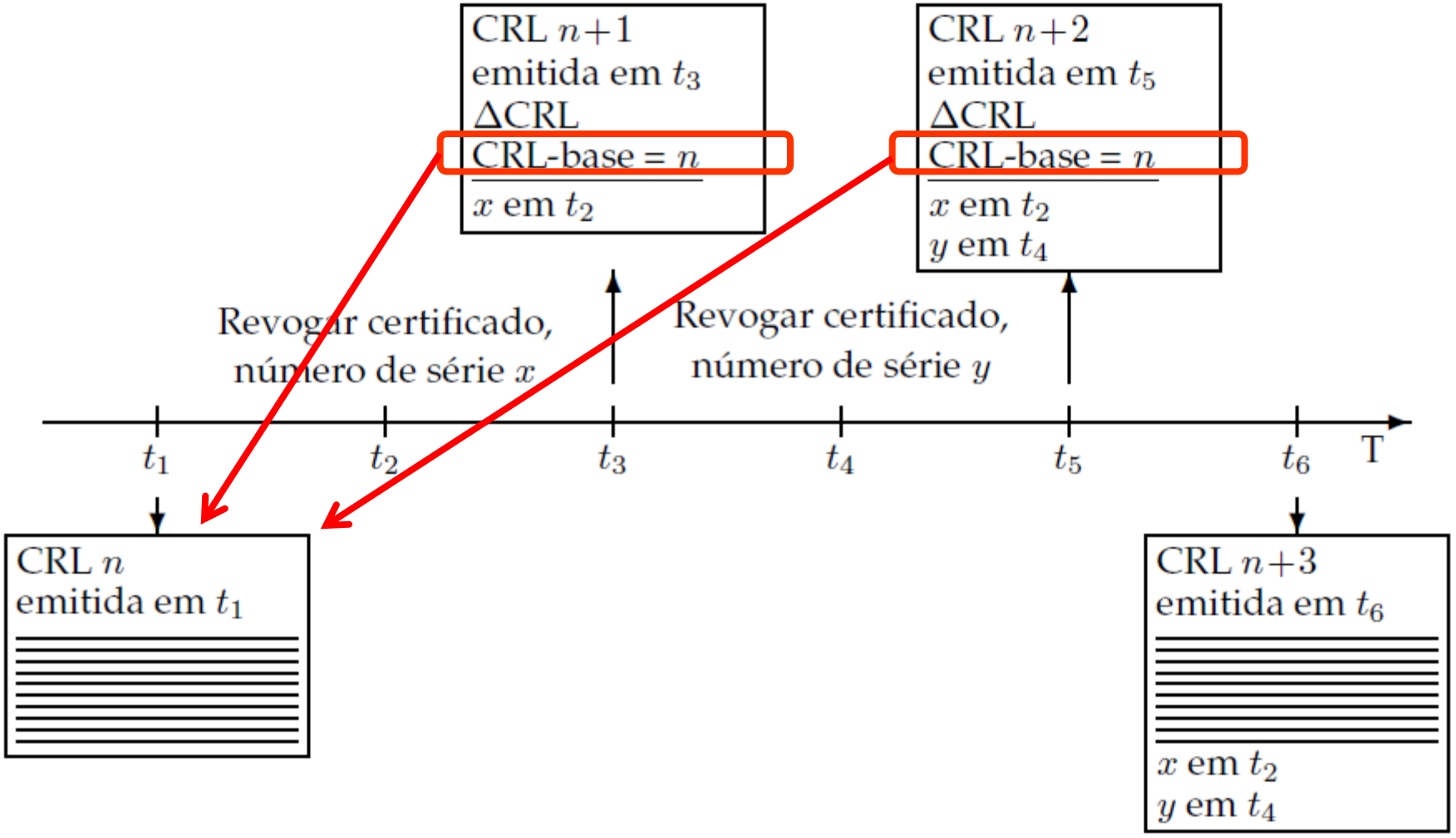
- Cada CA mantém e permite a consulta da sua CRL
- As CAs trocam listas entre si para facilitar o conhecimento das CRL

RFC 3280

unspecified (0)
keyCompromise (1)
CACompromise (2)
affiliationChanged (3)
superseded (4)
cessationOfOperation (5)
certificateHold (6)

removeFromCRL (8)
privilegeWithdrawn (9)
AACompromise (10)

CRL e Delta CRL



Distribuição de certificados de chave pública

Transparente (integrada com sistemas ou aplicações)

- Sistemas de diretório
  - De grande escala
    - ex. X.500 via LDAP
  - Organizacionais
    - ex. Windows 2000 Active Directory (AD)
- On-line
  - No âmbito de protocolos que deles necessitam para autenticar o interlocutor
    - ex. protocolos de comunicação segura (SSL, IPSec, etc.)
    - ex. Assinaturas digitais em mensagens de mail MIME
    - ex. Assinaturas digitais em documentos

Explícita (voluntariamente iniciada pelos utentes)

- É enviado um pedido a um serviço específico quando se deteta a necessidade de obter um dado certificado
  - ex. pedido por e-mail
  - ex. consulta de página HTTP

PKI (Public Key Infrastructure)

Infraestrutura de apoio ao uso de chaves públicas

- Criação segura de pares de chaves assimétricas
- Criação e distribuição de certificados de chaves públicas
- Definição e uso de cadeias de certificação
- Atualização, publicação e consulta de listas de certificados revogados
- Uso de estruturas de dados e protocolos que permitem a interoperação entre componentes

PKI:
Exemplo: políticas do Cartão de Cidadão

Inscrição
- Em locais próprios, pessoal

Vários pares de chaves por pessoa
- Um para autenticação
- Uma para assinaturas qualificadas
- Ambos gerados dentro do cartão, não exportáveis
- Ambos 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 amplamente divulgada
  - GTE Cyber Trust Global Root
- CA raiz PT debaixo da GTE
- CA raiz CC debaixo de CA raiz PT
- CAs Autenticação CC e Assinatura CC debaixo CA raiz CC

CRLs
- Certificados de assinatura pré-revogados por omissão
  - A revogação é removida se o dono do CC explicitamente requerer o uso de assinaturas digitais
- Todos os certificados são removidos a pedido do dono
  - Mediante a apresentação de um PIN de revogação
- Os pontos de distribuição das CRL estão explicitamente indicados em cada certificado

PKI: Relações de confiança

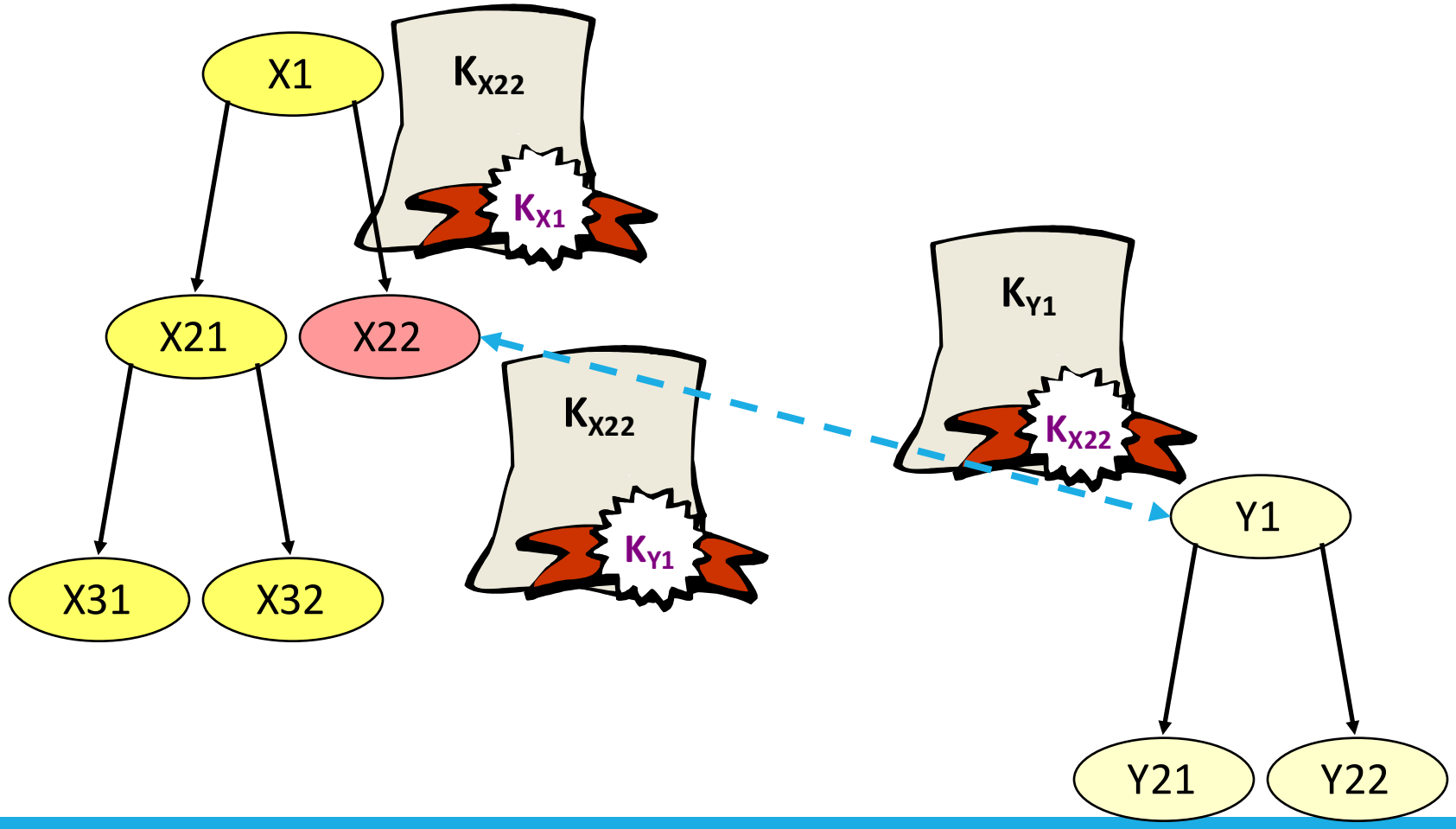
Um PKI estabelece relações de confiança de duas formas

- 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

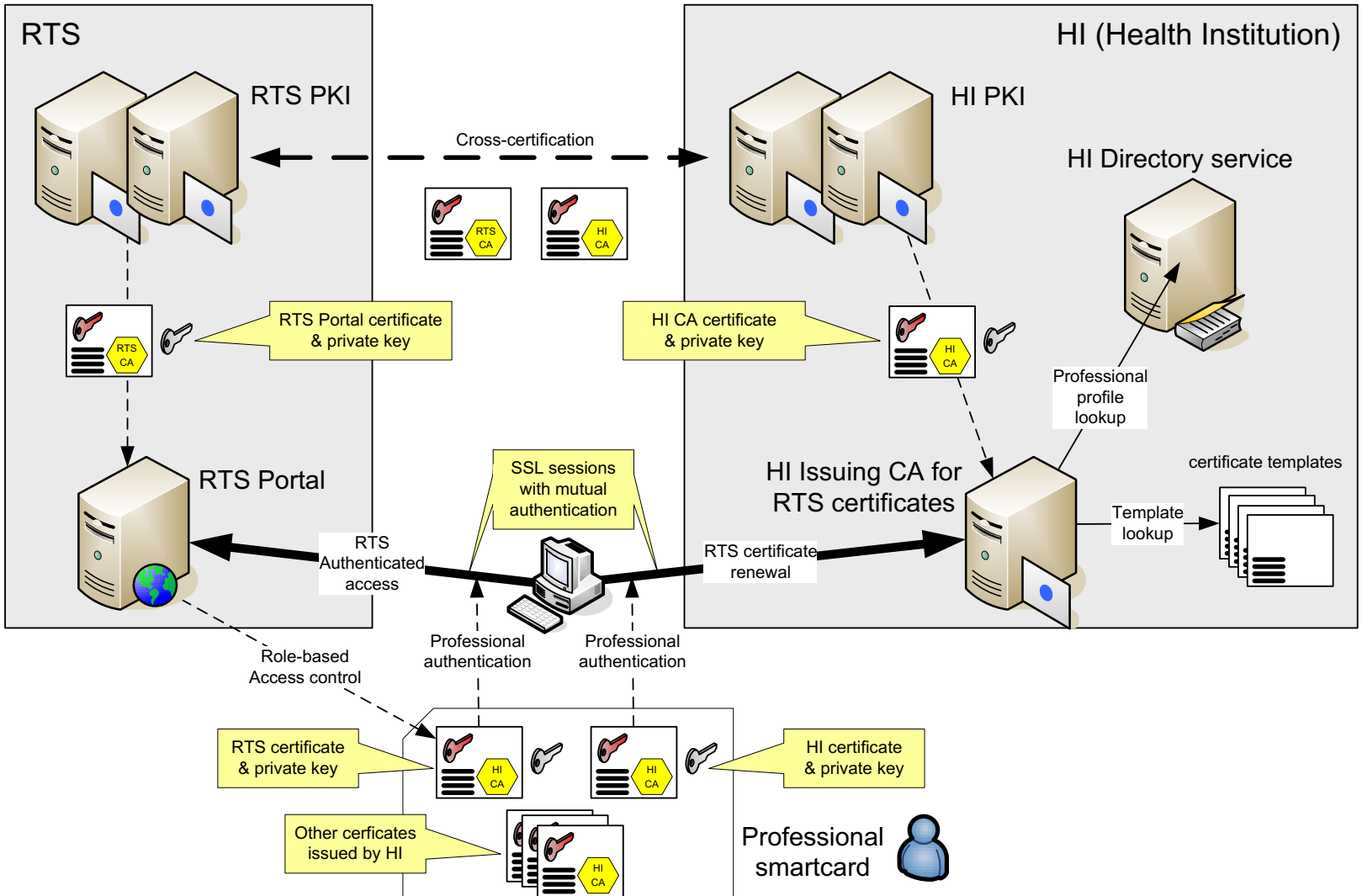
Relações de confiança características

- Hierárquicas
- Cruzadas (A certifica B e vice-versa)
- Ad-hoc (meshed)
  - Grafos mais ou menos complexos de certificação

PKI:
Certificação hierárquica e cruzada



Certificação cruzada entre PKIs: Um exemplo prático



Documentação adicional

[RFC 3280] Internet X.509 Public Key Infrastructure: Certificate and CRL Profile

Outros RFC

- [RFC 2510] Internet X.509 PKI Certificate Management Protocols.
- [RFC 2511] Internet X.509 Certificate Request Message Format.
- [RFC 2559] Internet X.509 PKI Operational Protocols - LDAPv2.
- [RFC 2560] X.509 Internet PKI Online Certificate Status Protocol - OCSP.
- [RFC 2585] Internet X.509 PKI Operational Protocols: FTP and HTTP.
- [RFC 2587] Internet X.509 PKI LDAPv2 Schema.
- [RFC 3029] Internet X.509 PKI Data Validation and Certification Server Protocols.
- [RFC 3161] Internet X.509 PKI Time-Stamp Protocol (TSP).
- [RFC 3279] Algorithms and Identifiers for the Internet X.509 PKI Certificate and Certificate Revocation List (CRL) Profile.
- [RFC 3281] An Internet Attribute Certificate Profile for Authorization.
- [RFC 3647] Internet X.509 PKI Certificate Policy and Certification Practices Framework.
- [RFC 3709] Internet X.509 PKI: Logotypes in X.509 Certificates.
- [RFC 3739] Internet X.509 PKI: Qualified Certificates Profile.
- [RFC 3779] X.509 Extensions for IP Addresses and AS Identifiers.
- [RFC 3820] Internet X.509 PKI Proxy Certificate Profile.