Algoritmos e Aplicações de Segurança

Gestão de chaves secretas

Problemas

- Os dados cifrados só são confidenciais se a chave de cifra for secreta
  - A distribuição e salvaguarda das chaves deverá garantir a sua confidencialidade
- Quanto mais imprevisíveis forem as chaves mais difíceis são de adivinhar
  - O valor das chaves deverá ser tão aleatório quanto possível
- Os computadores não são bons geradores aleatórios
  - É preciso descobrir e usar dados e comportamentos aleatórios num sistema
- O uso excessivo das chaves torna-as mais fáceis de descobrir
  - É preciso quantificar e impor limites para o uso das chaves

Gestão de chaves secretas : Objectivos

- Geração de chaves
  - Como e quando devem ser geradas chaves secretas
- Distribuição de chaves
  - Como são distribuídas a um número limitado (tipicamente 2) de interlocutores
- Tempo de vida das chaves
  - Durante quanto tempo devem as chaves ser usadas

Geração de chaves secretas: Princípios

- Usar bons geradores de valores aleatórios
  - Devem ser capazes de produzir qualquer das chaves aceitáveis pelo algoritmo de cifra
    - Imprevisibilidade (de todos os bits da chave)
      - Não devem ser previsíveis mesmo conhecendo toda a história passada e o algoritmo.
    - Equiprobabilidade (de todos os bits da chave)
      - Tal é normalmente feito pelos geradores pseudo-aleatórios
      - Passam os testes de aleatoridade
      - Distribuições de zeros e uns
      - Não devem ser compressíveis
  - As cifras simétricas têm normalmente poucas chaves "inaceitáveis"
    - DES: chaves fracas, semi-fracas e quasi-fracas
- Bons geradores podem ser:
  - Verdadeiramente aleatórios
  - Criptograficamente fortes

Geração de chaves secretas: Dimensão

- Qual a dimensão de uma chave secreta ?
  - Complexidade do algoritmo
    - (se for perfeito não influencia)
  - Tempo de vida
  - Utilização
  - Capacidade do atacante.
- RFC3766
  - 90 bits em 1996
  - 2/3 bits por ano
  - em 2005: 96bits

Distribuição de chaves secretas: Manual (1/2)

- Utilidade
  - Para distribuir chaves pessoais
    - Que autenticam uma pessoa (senha)
  - Para distribuir grandes conjuntos de chaves
    - Para serem usadas durante um período alargado de tempo
- Requisitos usuais
  - As chaves não devem ser reveladas a terceiros
    - Entre a sua geração e sua recepção pelo destinatário correcto
    - Devem ser consideradas todas as entidades que podem ter acesso à chave (administradores de sistemas, distribuidores, etc.)
  - O receptor deverá distinguir claramente se a chave que recebe está correcta e é legítima
    - Somas de controlo
    - Autenticidade do remetente e da mensagem
    - Uso só após confirmação da sua recepção

Distribuição de chaves secretas: Manual (2/2)

- Suporte
  - Em suportes voláteis
    - Apresentação num ecrã de uma nova senha de um utilizador
  - Em "papel"
    - Normalmente usado para transmitir chaves pessoais
      - PIN dos cartões Multibanco ou VISA
      - Cartões telefónicos universais
  - Em suportes alteráveis
    - Diskettes, cartões magnéticos, cartões c/ memória FLASH
- Distribuição
  - Presencial
  - Por várias vias não totalmente confiáveis
    - Mas não colaborantes entre si

Distribuição de chaves secretas:

Com segredos partilhados de longa duração (1/3)

- Utilidade
  - Servem para trocar facilmente segredos efémeros entre entidades que partilham alguma informação secreta
    - Senhas memorizáveis por humanos
    - Chaves de cifra não memorizáveis
- Nomenclatura
  - Segredos partilhados de longa duração
    - Chaves de cifra de chaves
    - (***Key Encrypting Keys,*** **KEK**)
  - Segredos efémeros a partilhar
    - Chaves de sessão (***sessions keys, Ks***)

Distribuição de chaves secretas:

Com segredos partilhados de longa duração (2/3)

- Distribuição
  - Protocolo ANSI X9.17 ou variantes

    $A \rightarrow B: \{K_s\}_{KEK}$
- A distribuição pressupõe autenticação sob certas condições
  - Se B
    - acreditar que apenas A conhece KEK;
    - comprovar que a mensagem é "fresca";
    - verificar que o seu conteúdo é efectivamente $\{K_s\}_{KEK}$,

    então A foi o seu autor
  - A comprovação da "frescura" evita ataques por repetição
    - Basta um contador partilhado para esse fim

Distribuição de chaves secretas:

Com segredos partilhados de longa duração (3/3)

- Aspectos práticos a considerar
  - As KEK devem ser usadas apenas para cifrar chaves de sessão
    - Para dificultar a sua criptanálise
    - Quanto mais chaves de sessão se cifrar mais se compromete a KEK
  - A descoberta de uma KEK revela todas as chaves de sessão trocadas por seu intermédio
    - Não existe **segurança futura perfeita** (*perfect forward secrecy*, PFS)
  - Uma chave de sessão não deve ser usada como KEK
    - Porque, por definição, foi ou será demasiado exposta pelo seu uso intensivo

Distribuição de chaves secretas: Com valores públicos partilhados

- Semelhante à distribuição de chaves com segredos partilhados de longa duração
  - Mas a chave KEK é a chave pública do destinatário
  - Vulgarmente designada como cifra mista

    $A \rightarrow B: \{Ks\}_{K_B}$
  - Exemplo: PGP (com chaves assimétricas RSA)
- A distribuição não pressupõe autenticação
  - Porque é usada a chave pública do destinatário para lhe comunicar um segredo
- Aspectos práticos a considerar
  - A descoberta da chave secreta do destinatário revela todas as chaves de sessão trocadas usando a chave pública correspondente
  - Não existe segurança futura perfeita

Distribuição de chaves secretas: Com valores públicos partilhados

- Qual a dimensão da chave pública/privada
  - Depende da chave simétrica
- RFC3766

Chave simétrica	RSA/DH Dimensão do módulo	DSA Dimensão do subgrupo
70	947	129
80	1228	148
90	1553	167
100	1926	186
150	4575	284
200	8719	383
250	14596	482

Distribuição de chaves secretas: Sem partilhar qualquer valor (1/3)

- Algoritmo de Diffie-Hellman (DH)
  - Na prática tem de se partilhar algo
    - A partilha pode ser efémera ou universal
    - Os valores a partilhar não são secretos ou pessoais
  - Dados α e q públicos:
    - A e B geram valores aleatórios e secretos: a e b
    - A calcula $y_A = \alpha^a \bmod q$
      B calcula $y_B = \alpha^b \bmod q$
    - A e B trocam y_A e y_B (valores públicos de DH)
    - A calcula $K_s = y_B^a \bmod q$
      B calcula $K_s = y_A^b \bmod q$
- A segurança baseia-se na complexidade de certas operações matemáticas
    - Logaritmo modular
    - Dados α, q , y_A e y_B é impossível obter a e b ou calcular K_s

Distribuição de chaves secretas: Sem partilhar qualquer valor (2/3)

- A distribuição não pressupõe autenticação
  - Porque não existe nada partilhado entre os interlocutores
  - Ataques por interposição (*man-in-the-middle*)
- Alternativas para a autenticação
  - Autenticar valores públicos de DH y_A e y_B
  - Autenticar a chave de sessão gerada K_s
- Autenticação com assinaturas digitais
  - De uma autoridade de certificação
    - Para valores públicos de DH de longa duração
  - Pelo próprio
    - Pressupõe a existência de chaves assimétricas (para assinatura) do interlocutor
  - Exemplo: PGP (com chaves assimétricas DH/DSS)

Distribuição de chaves secretas: Sem partilhar qualquer valor (3/3)

- Aspectos práticos a considerar
  - Se ambos os valores secretos forem efémeros então existe segurança futura perfeita
  - Se um dos valores secretos for de longa duração a sua revelação revela todas as chaves que gerou

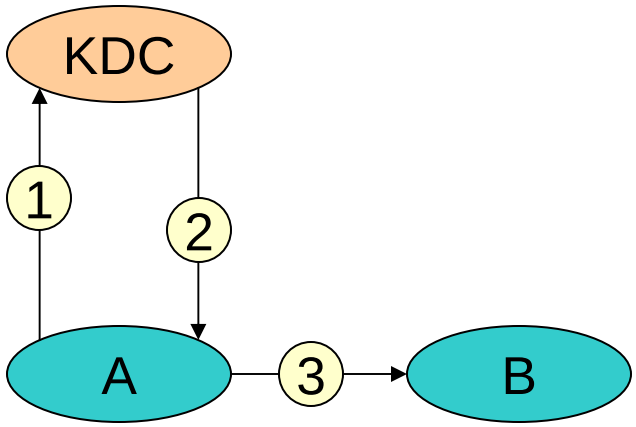
Distribuição de chaves secretas:
Com entidades terceiras confiáveis (1/3)

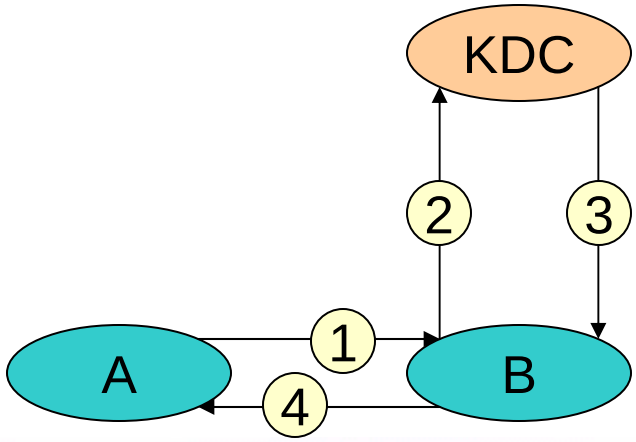
- Entidades terceiras confiáveis (*Key Distribution Centers*)
  - Actuam como mediadores entre os interlocutores
    - Distribuem credenciais para uma interacção segura
  - Simplificam a gestão de segredos partilhados de longa duração
    - Evitam a partilha de segredos entre quaisquer 2 interlocutores
  - Permitem centralizar a autenticação
    - Ponto central de conhecimento de segredos partilhados
- Pressupostos
  - Actuam correctamente
    - Não divulgam nem usam incorrectamente os segredos que conhecem
    - Geram chaves de sessão imprevisíveis
  - São seguras
    - São geridas de forma a proteger da melhor forma os segredos que guardam

Distribuição de chaves secretas:

Com entidades terceiras confiáveis (2/3)

- Distribuição
  - *Pull model*
    - 1: A →KCD: A, B
    - 2: KDC → A: $\{K_s\}_{K_A}$, $\{A, K_s\}_{K_B}$
    - 3: A → B: A, $\{A, K_s\}_{K_B}$
    - A ⇔ B: $\{M\}_{K_s}$
  - *Push model*
    - 1: A →B: A
    - 2: B → KDC: A, B
    - 3: KDC → B: $\{K_s\}_{K_B}$, $\{B, K_s\}_{K_A}$
    - 4: B → A: $\{B, K_s\}_{K_A}$
    - A ⇔ B: $\{M\}_{K_s}$



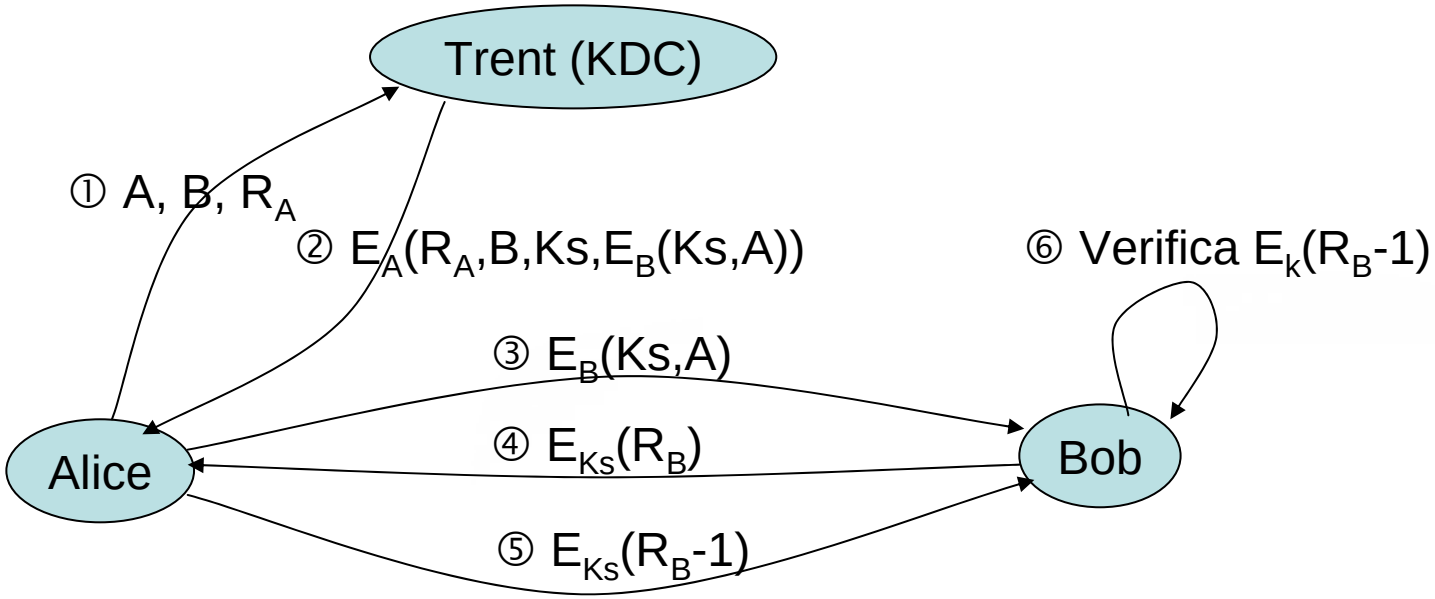


Distribuição de chaves secretas:

Com entidades terceiras confiáveis (3/3)

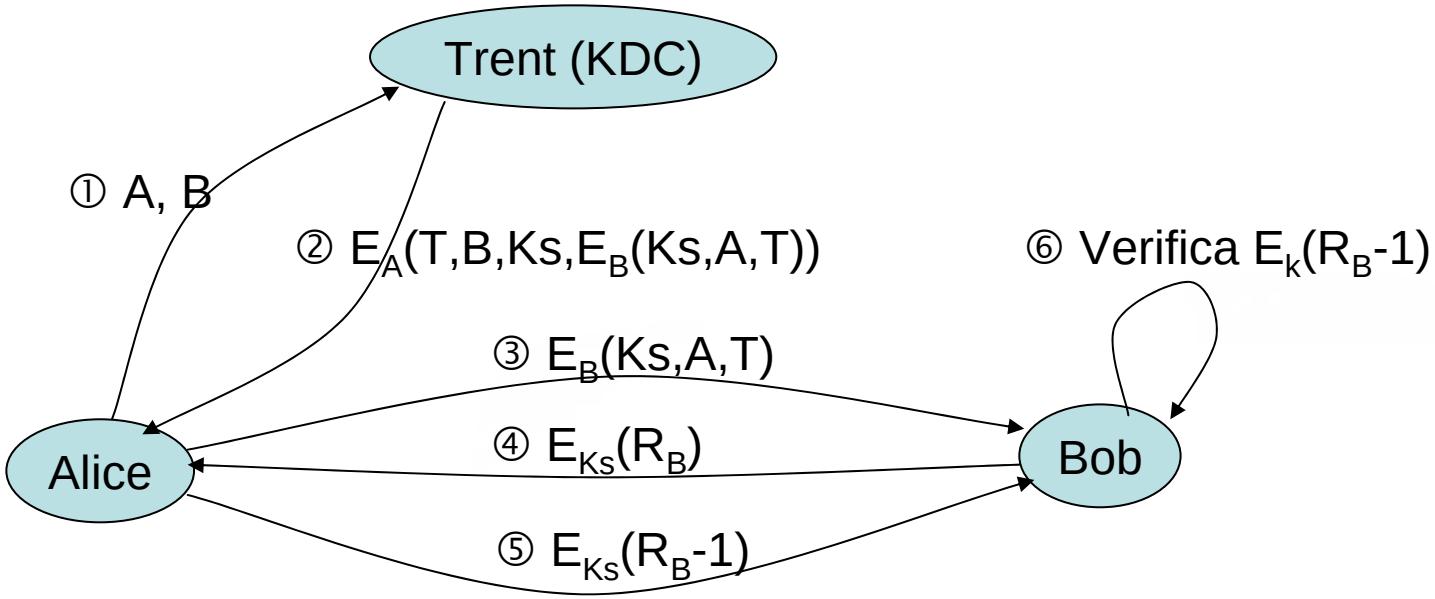
- A distribuição pressupõe autenticação
  - Só quem partilha uma chave com o KDC é que pode obter uma chave de sessão
  - Quando B recebe $\{A, K_s\}_{KB}$ tem a certeza que está a receber uma chave K_s para falar com A
- Problemas a resolver
  - Autenticação das mensagens
    - Origem, conteúdo, frescura
  - Cooperação entre diferentes KDC
    - Facilitar a troca de chaves entre entidades conhecidas por diferentes KDCs
- Aspectos práticos a considerar
  - Não existe segurança futura perfeita

Needham-Schroeder



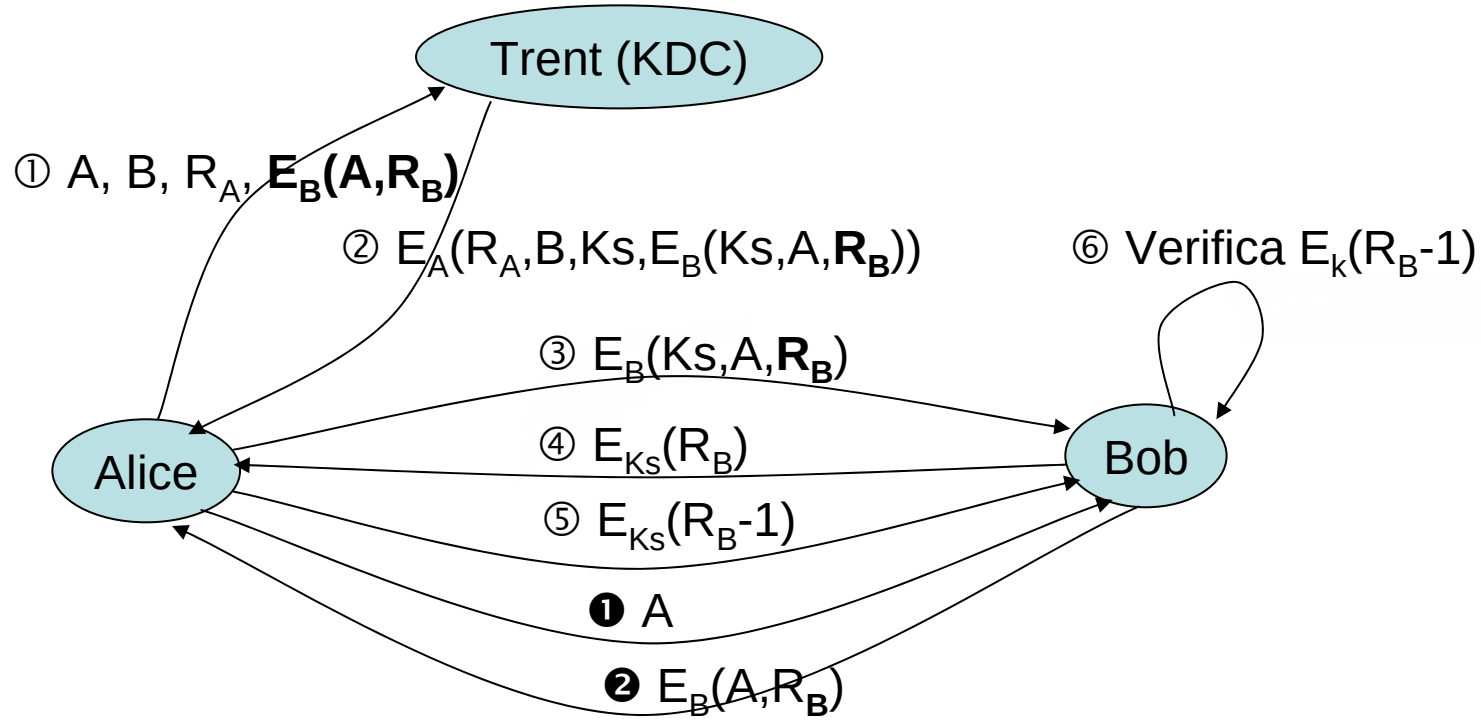
- A mensagem 3 pode ser enviada directamente para o Bob pelo Trent?
- Para que servem as mensagens 4 e 5?
- O que é que acontece se alguém conseguir obter uma chave de sessão?

NS com marcas temporais



- Alteração proposta por Dorothy Denning
- Bob só aceita 3 se estiver dentro da janela temporal.
- A janela para obtenção da chave de sessão é menor.

NS revisitado



- Alteração proposta por Needham e Schroeder
- Não necessita de sincronização de relógios

Ataques de repetição (Replay attacks)

- Messagens copiadas e reenviadas posteriormente
- Frescura das mensagens
  - Números sequenciais
  - Marcas temporais
  - Desafio/resposta

Ataques de repetição I

- Números sequenciais
  - Não é prático
  - Participantes têm que manter contadores sincronizados
  - Difícil quando existem perdas de mensagens e duplicações

Ataques de repetição II

- Marcas temporais
  - As mensagens contêm uma marca temporal
  - Só são aceites mensagens com marcas dentro de certos limites
  - Muito utilizados (kerberos) mas têm problemas
    - Os relógios têm que estar sincronizados
    - Tolerância a atrasos na rede.

Ataques de repetição III

- Desafio/resposta
  - O iniciador envia um nonce (number used only one-time) e espera que esse nonce (ou uma sua transformação) venha na resposta.
  - Fácil de implementar
  - Utiliza mais mensagens
  - Necessita que ambas as partes sejam activas
    - Não é aplicável a comunicações sem ligação.

Renovação de chaves (1/2)

- Objectivo
  - Minimizar o risco de criptanálise
  - Aplicável a chaves de sessão e de longa duração
    - Exemplo: alteração periódica de senhas de utilizadores
- Critérios
  - Após um determinado intervalo temporal
    - Para evitar a sua descoberta durante o período de vida útil
    - Tal permitiria alterar deterministicamente os criptograma
  - Após um determinado volume de dados cifrados
    - Para evitar um uso excessivo da chave
    - Exemplo: WEP

Renovação de chaves (2/2)

- Método de renovação
  - Usando um protocolo de alteração de chaves de longa duração
  - Usando chaves KEK para distribuir novas chaves de sessão
  - Usando chaves de sessão como chaves KEK
    - Exemplo: distribuição de chaves nos autenticadores Kerberos
    - Neste caso as chaves de sessão nunca são usadas como tal, mas sim como KEK temporárias
- Segurança futura perfeita
  - A menos que se use DH com valores privados efémeros a renovação não garante segurança futura perfeita

Algoritmos e Aplicações de Segurança

Gestão de chaves públicas

Problemas

- A gestão deverá assegurar a correcção no seu uso
  - A gestão de chaves privadas deverá garantir a sua privacidade
    - Para evitar o repúdio de assinaturas digitais
  - A gestão de chaves públicas deverá garantir a sua correcta distribuição
    - Para garantir confidencialidade
    - Para garantir a correcta validação de assinaturas digitais
- Evolução temporal do mapeamento entidade ⇔ par de chaves
  - Para lidar com situações de catástrofe (perda da chave privada)
  - Para lidar com situações de gestão correntes (renovação para assegurar maior segurança)
- Imprevisibilidade das chaves dificulta a sua descoberta
  - A geração das chaves assimétricas deverá usar bons geradores de valores "aleatórios"

Gestão de chaves assimétricas: Objectivos

- Geração de chaves
  - Como e quando devem ser geradas chaves assimétricas
- Uso de chaves privadas
  - Como é protegida a sua privacidade
- Distribuição de chaves públicas
  - Como são distribuídas as chaves públicas correcta e universalmente
- Tempo de vida das chaves
  - Durante quanto tempo devem as chaves ser usadas
  - Consulta de chaves obsoletas

Geração de chaves assimétricas: Princípios

- Usar bons geradores
  - Devem ser capazes de produzir qualquer das chaves aceitáveis pelo algoritmo de cifra
    - Imprevisibilidade (de todos os bits da chave)
    - Equiprobabilidade (de todos os bits da chave)
- Facilitar sem comprometer a segurança
  - Gerar chaves públicas eficientes
    - Normalmente significa chaves públicas com poucos bits
    - Permite acelerar um dos sentidos de cálculo sem perda de segurança
- A chave privada deve ser gerada pelo próprio
  - Para assegurar ao máximo a sua privacidade

Utilização de chaves privadas: Cuidados a ter

- Uso correcto
  - 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
    - Protecção com senha (ex. PGP)
    - Correcção das aplicações que a usam
- Confinamento
  - Salvaguarda e uso da chave privada num dispositivo autónomo (ex. *smart card*)
    - O dispositivo gera pares de chaves
    - O dispositivo cifra/decifra dados com o par de chaves mediante controlo externo próprio

Distribuição de chaves públicas

- Técnicas
  - Manual
    - Não é prático
  - Usando um segredo partilhado
    - Se já existe um segredo partilhado !!!
  - Anúncio público
  - Directório público
  - Distribuição centralizada
  - Distribuição pública usando certificados digitais

Anúncio Público

- Publicar a chave pública por vários meios
  - via newsgroups, listas de emais, sitios pessoas, etc.
  - Alguém pode publicar essa chave dizendo que é de outra pessoas

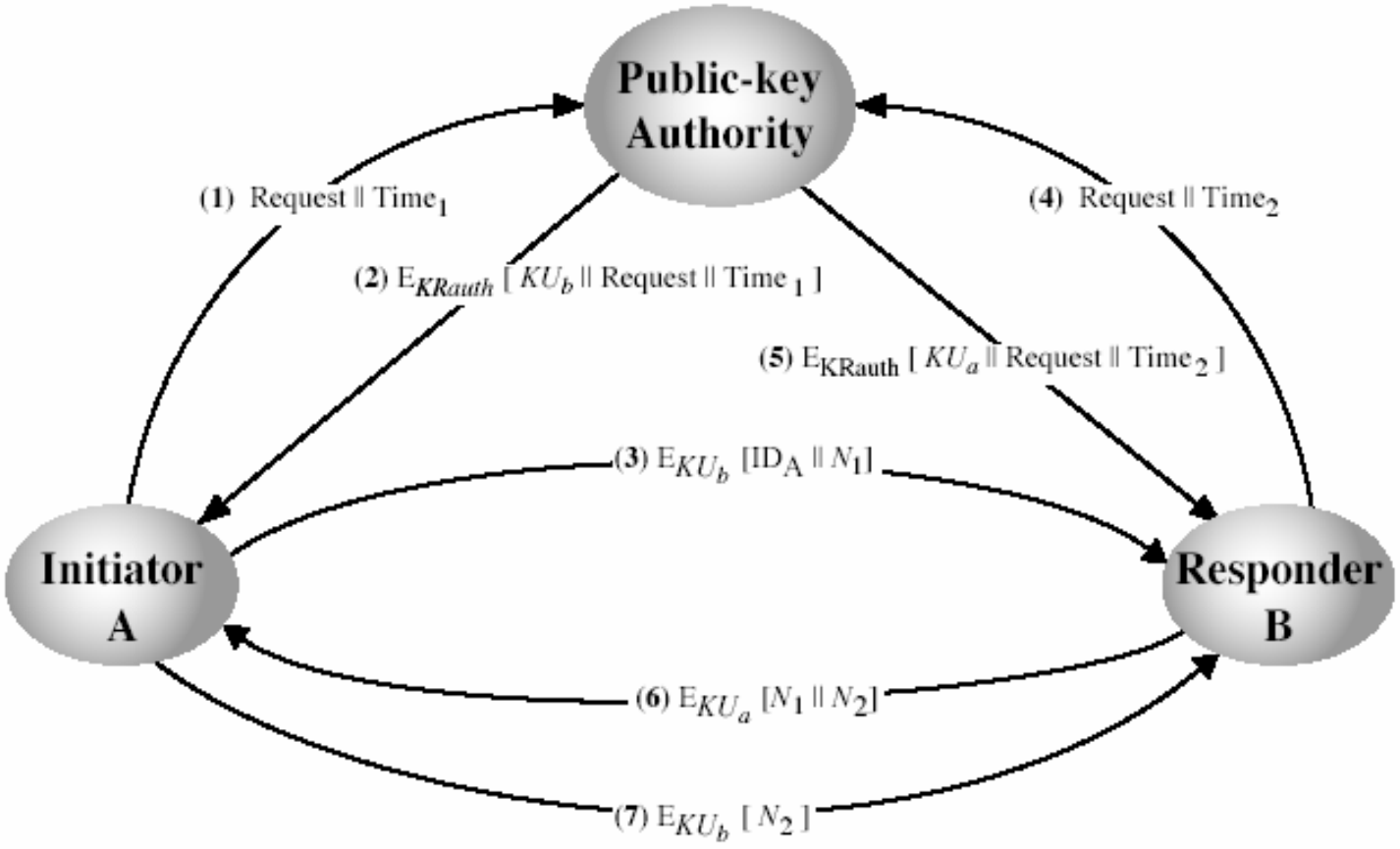
Directório público

- Existe um directório com pares de {nome, chave pública}
- A escrita é controlada
  - Administrador confiável
- Administração difícil
  - Ponto central de administração

Gestão descentralizada de directório público

- Semelhante ao directóro públcio mas:
  - Utilizadores obtêm as chaves públicas de forma segura
  - Necessita de acesso online ao directório
  - Os utilizadores têm que saber a chave pública do directório
- O directório contém pares {nome, chave pública}
  - Permissão para escrita é restricta para cada par a quem provar que tem a chave privada correspondente.

PROTOCOLO


Public-key Authority
(1) Request || Time1
(2) EKRauth [KUb || Request || Time 1]
(4) Request || Time2
(5) EKRauth [KUa || Request || Time 2]
(3) EKUb [IDA || N1]
Initiator A
Responder B
(6) EKUa [N1 || N2]
(7) EKUb [N2]

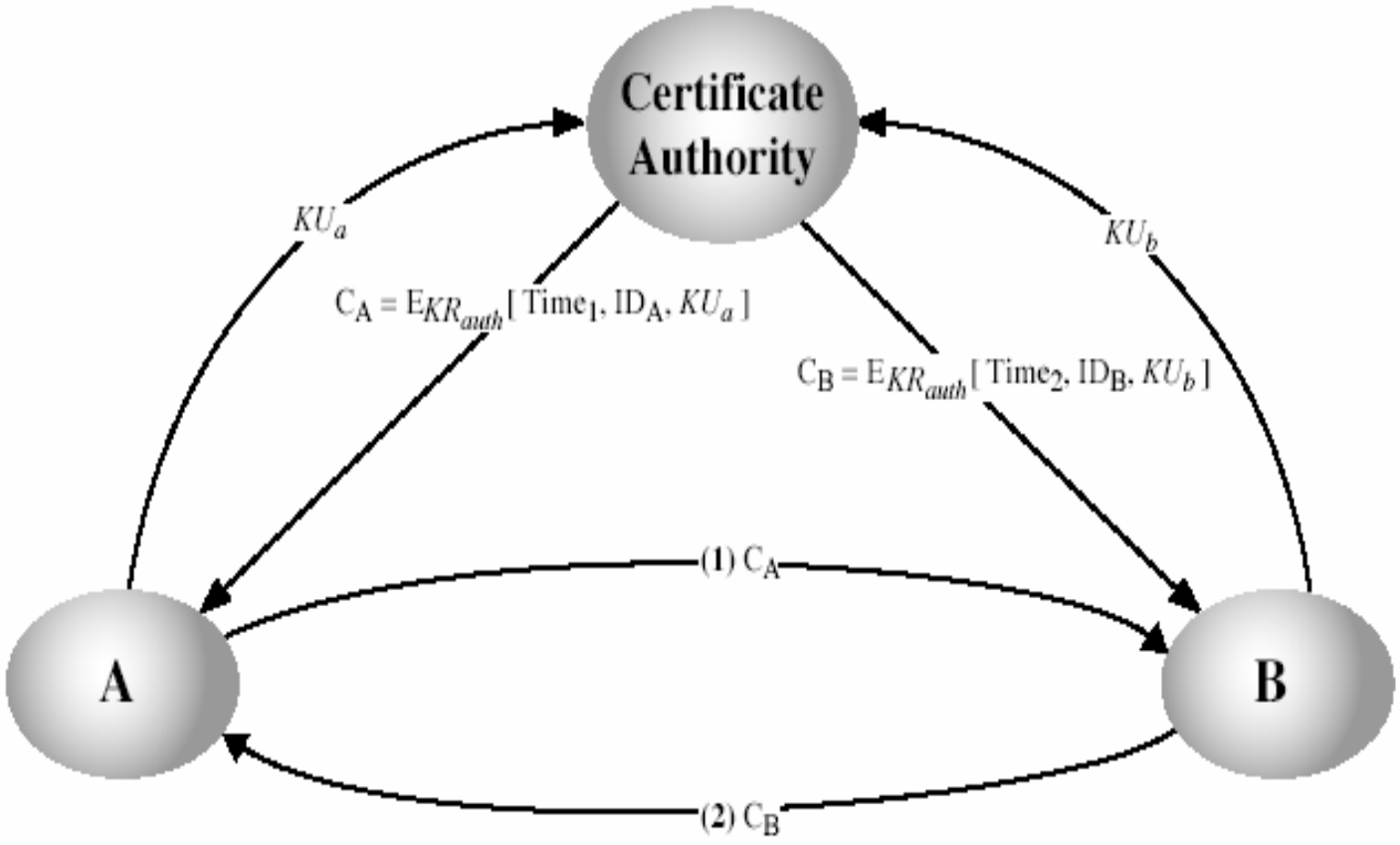
Directório Público com gestão descentralizada

- Desvantagens
  - O directório é uma entidade activa que pode provocar perdas de desempenho
  - O directório deve ser mantido seguro para evitar alterações não autorizadas
  - O problema do registo das chaves públicas não é resolvido

Certificados digitais de chaves públicas

- São documentos assinados por uma entidade certificadora
  - Autoridade de Certificação (CA)
  - São documentos públicos criptográficamente seguros
    - Podem ser distribuídos com segurança através de canais inseguros
- Servem para distribuir chaves públicas de forma confiável
  - O receptor do certificado pode validar a assinatura do certificado usando a chave pública da CA
  - Se confiar no assinante (CA) e a assinatura estiver correcta pode confiar na chave pública certificada
- Estrutura de um certificado
  - Padrão X.509
  - PKCS #7 Cryptographic Message Syntax Standard

Public-Key Certificates



X.509 v3 Digital Certificate (RFC3280)

- Structure
  - Version
  - Serial Number (p/ CA)
  - Algorithm ID (ex.: DSA c/ SHA-1)
  - Issuer
  - Validity
    - Not Before
    - Not After
  - Subject
  - Subject Public Key Info
    - Public Key Algorithm
    - Subject Public Key
  - Extensions (Optional)
  - Signature Algorithm
  - Signature Value
- Extensions
  - Issuer Unique Identifier (v2)
  - Subject Unique Identifier (v2)
  - Authority Key Identifier
  - Subject Key Identifier
  - Key Usage
    - digitalSignature
    - nonRepudiation
    - keyEncipherment
    - dataEncipherment
    - keyAgreement
    - keyCertSign
    - CRLSign
    - encipherOnly
    - decipherOnly
  - Extended Key usage
  - CRL Distribution Points
  - Private Key usage period

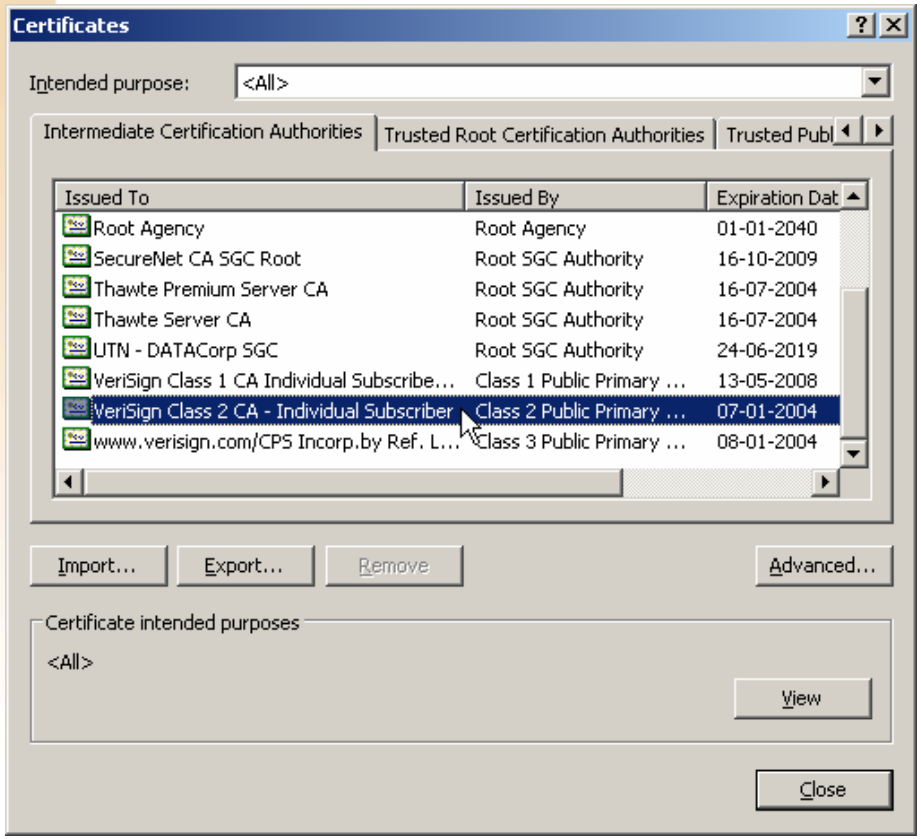
Formatos e Extensões

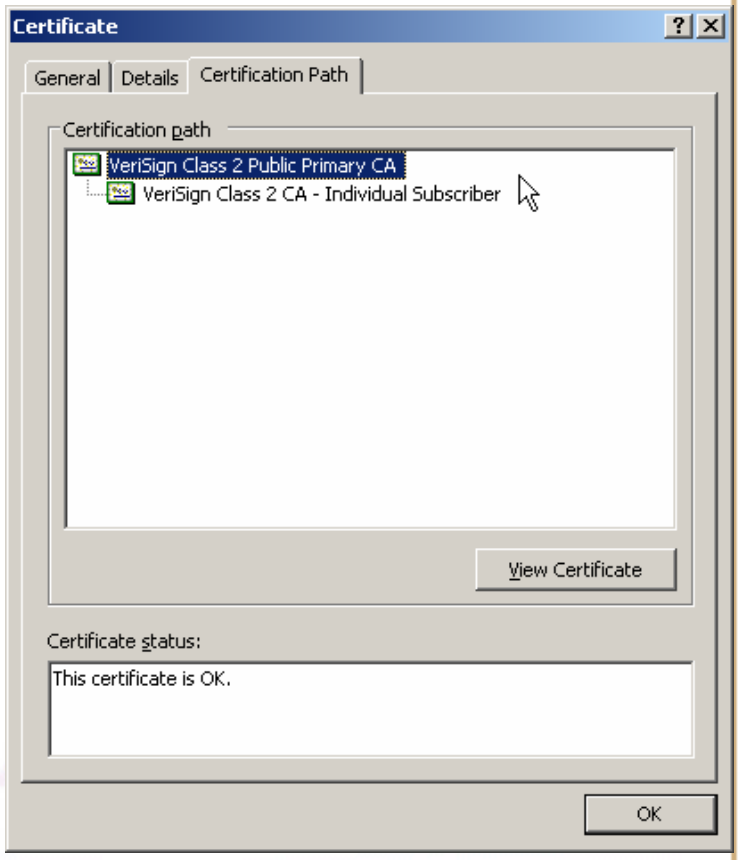
- .DER – certificado no formato DER
- .CER – conjunto de certificatos no formato DER,
- .PEM – certificado no formato Base64
  - "-----BEGIN CERTIFICATE-----"
  - "-----END CERTIFICATE-----"
- .P7B e .P7C - PKCS#7 mensagem assinada,
  - usualmente sem dados
  - Só o certificado
- .PFX e .P12 - PKCS#12, vários certificados e chave privada (protegida com senha)

Autoridades de Certificação

- Organizações que gerem certificados
  - Definem políticas e mecanismos de geração e distribuição de certificados
  - Gerem listas de revogação de certificados
- Confiança nas CAs
  - Distribuição manual das suas chaves públicas
    - Certificação centralizada (só com uma CA)
    - Certificação ad-hoc (ex. PGP)
  - Hierarquia de certificação
    - Certificados de chaves públicas de CAs
    - Distribuição manual das chaves públicas das CA raiz
      - ex. em navegadores (Internet Explorer, Netscape, etc.)

Distribuição manual de certificados: Internet Explorer





Hierarquias de certificação: Modelo PEM (*Privacy Enhanced Mail*)

- Distribuição de certificados para e-mail seguro PEM
  - Hierarquia à escala mundial
    - Uma única raiz (IPRA)
    - Várias PCA (*Policy Creation Authorities*) abaixo da raiz
    - Várias CA abaixo de cada PCA
      - Tipicamente de organizações ou empresas
  - Caminhos de certificação
- O modelo nunca chegou a ser concretizado
  - O que existe é uma floresta de CAs sem raiz PCA
    - Hierarquias privadas com raiz numa CA
  - Cada CA tenta que a sua chave pública seja distribuída com as aplicações que usam chaves públicas
    - ex. navegadores

Hierarquias de certificação: Modelo PGP (*Pretty Good Privacy*)

- Teia de confiança (*Web of Trust*)
  - Não existem autoridades centrais de certificação
    - Cada pessoa é um potencial certificador
    - Basta assinar uma chave pública e exportar a assinatura para terceiros
  - Os utilizadores usam dois tipos de confiança
    - Nas chaves públicas que conhecem
      - Validação por vias alternativas (FAX, telefone, etc.)
    - Na capacidade dos seus detentores serem bons assinantes
      - Assinam sabendo o que fazem
- Confiança transitiva
  - Se

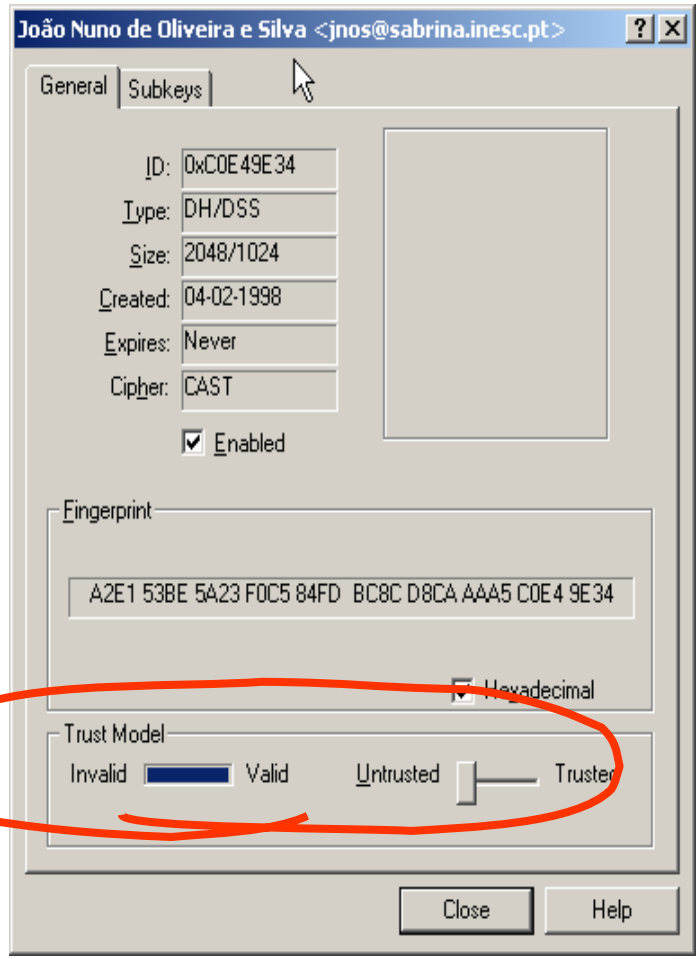
    A confia que B é um bom certificador, e

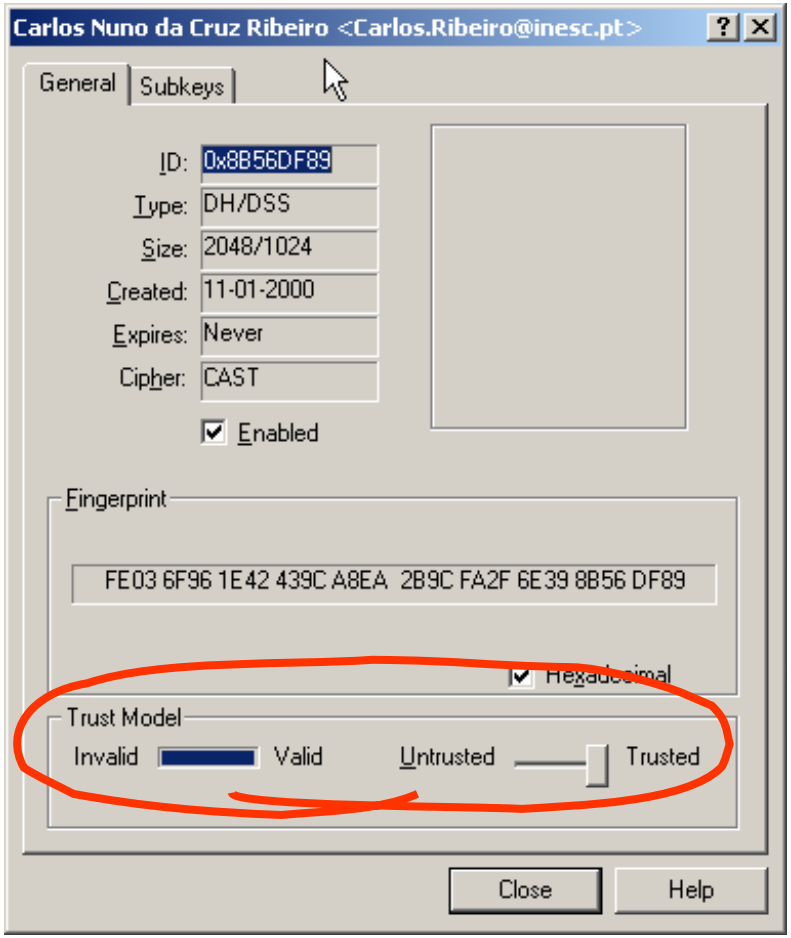
    B certificou a chave pública de C,
  - então

    A confia na chave pública de C

Certificados de chaves públicas PGP:

Diferença entre validade e confiança





Renovação de pares de chaves assimétricas

- As chaves assimétricas devem ter um período de validade limitado
  - Porque as chaves privadas podem-se perder ou ser comprometidas
  - 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
- Soluções
  - Certificados com prazos de validade
  - Listas de revogação de certificados
    - Com certificados revogados antes da expiração do prazo de validade

Listas de certificados revogados

- São listas de certificados fora de uso
  - Devem ser consultadas regularmente pelos detentores de certificados
- Manutenção e divulgação de listas de certificados revogados
  - Certificação institucional
    - Cada CAs mantém e permite a consulta da lista que conhece
    - As CAs trocam listas entre si para facilitar o conhecimento de todos os certificados revogados
  - Certificação ad-hoc
    - A entidade detentora da chave pública revogada tem que criar e divulgar o melhor que puder um certificado de revogação

Distribuição de certificados

- Transparente
  - Sistemas de directório
    - De grande escala
      - ex. X.500
    - Organizacionais
      - ex. Windows 2000 Active Directory
  - On-line
    - No âmbito de protocolos que deles necessitam
      - ex. protocolos de comunicação segura
- Interactiva
  - É enviado um pedido a um serviço específico quando se detecta a necessidade de obter um dado certificado
    - Pedido por e-mail, consulta de página HTTP, finger, etc.

PKI (*Public Key Infrastructure*)

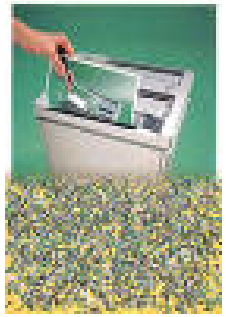
- Infra-estrutura de apoio ao uso de chaves públicas
  - Criação segura de pares de chaves assimétricas
  - Criação e distribuição de certificados de chaves públicas
  - Definição e uso de cadeias de certificação
  - Actualização, publicação e consulta de listas de certificados revogados
  - Uso de estruturas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

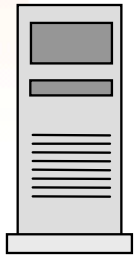
Entidades da PKI

Certification Authority (CA)
Entidade Confiável que cria e publica os certificados no repositório.

Subscritor
- Gera um par de chaves
- Pede um certificado para a sua chave pública
- Recebe o certificado
- Usa a sua chave privada

Certification Revocation List Authority (CRLA)
Entidade Confiável que cria e publica os certificados de revogação no repositório.





Repositório

Verificador
- Descobre certificados no repositório
- Valida os certificdos de modo a construir uma cadeia de certificados
- Usa a chave pública do subscritor

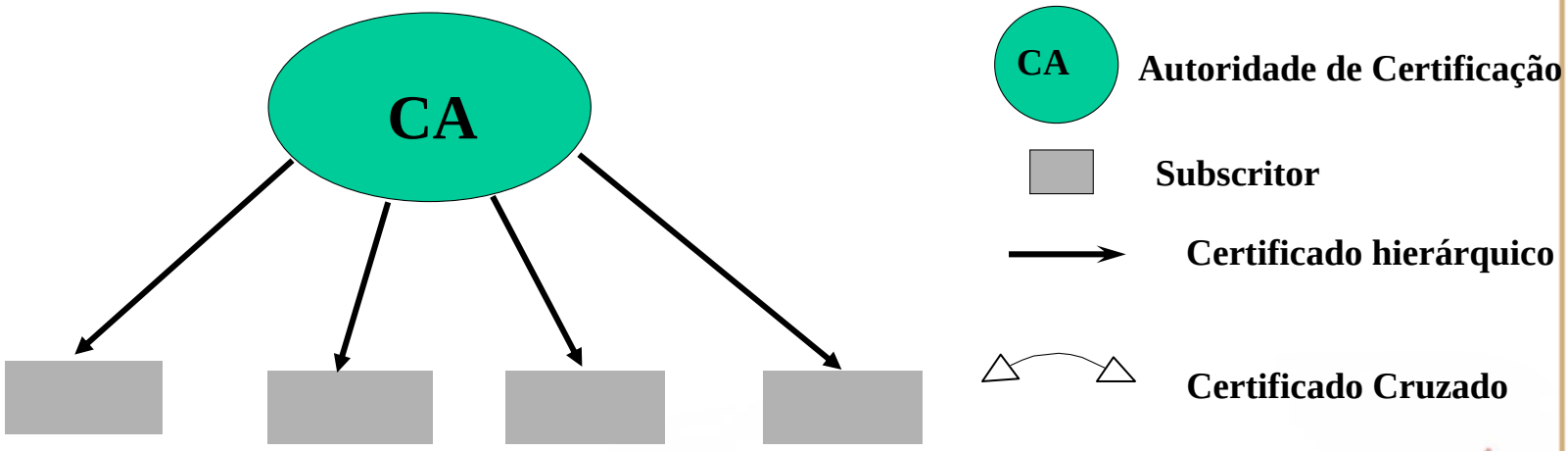
PKI: Pares de chaves assimétricas

- Chaves para garantir confidencialidade
  - A chave pública de X é usada por emissores para garantir a confidencialidade de dados enviados para X
    - E a chave privada de X é usada para decifrar informação confidencial que lhe chega
  - Estas chaves podem ser refrescadas frequentemente
    - No pior caso repete-se o envio da informação
- Chaves para garantir autenticidade
  - A chave privada de X é usada para assinar conteúdos
    - E a pública correspondente para validar as assinaturas
  - Estas chaves não devem ser refrescadas frequentemente
    - Para simplificar os processos de validação de assinaturas

PKI: Relações de confiança

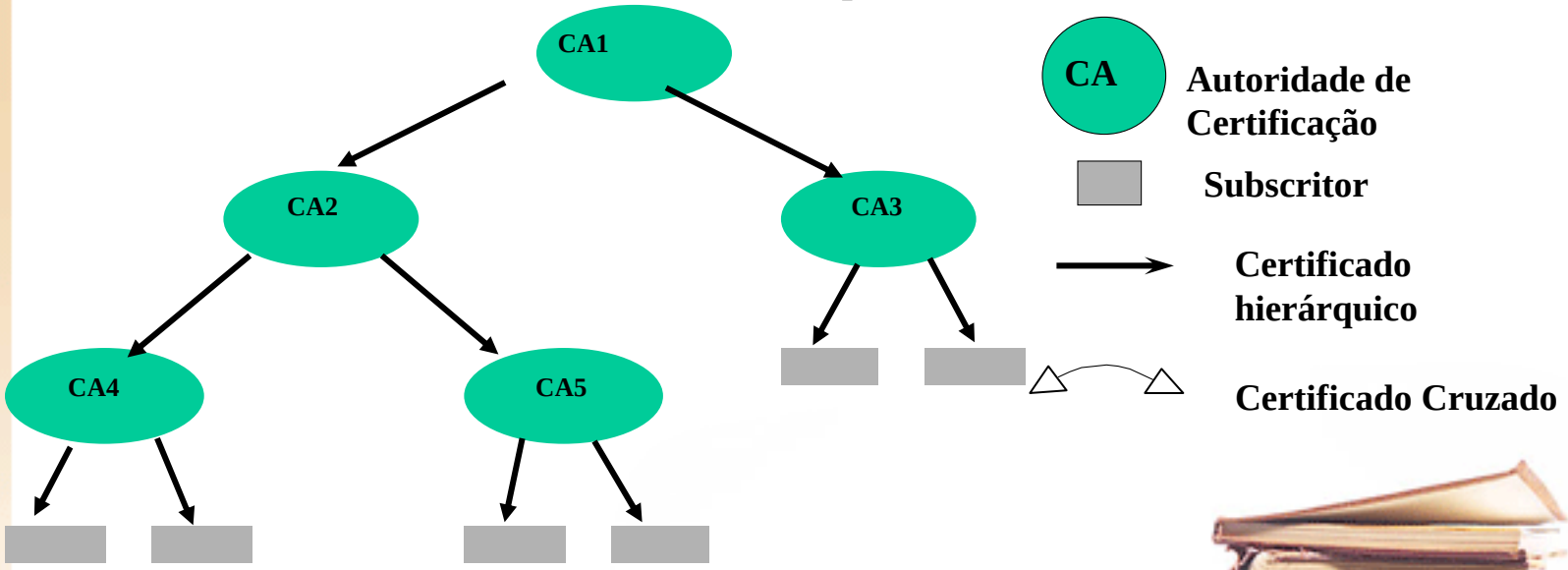
- Um PKI estabelece relações de confiança de duas formas
  - Emitindo certificados de chaves públicas de outras CAs
    - Abaixo na hierarquia; ou
    - Não relacionadas hierarquicamente
  - Requerendo a certificação da sua chave pública a outras CAs
    - Acima na hierarquia; ou
    - Não relacionadas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

Plano



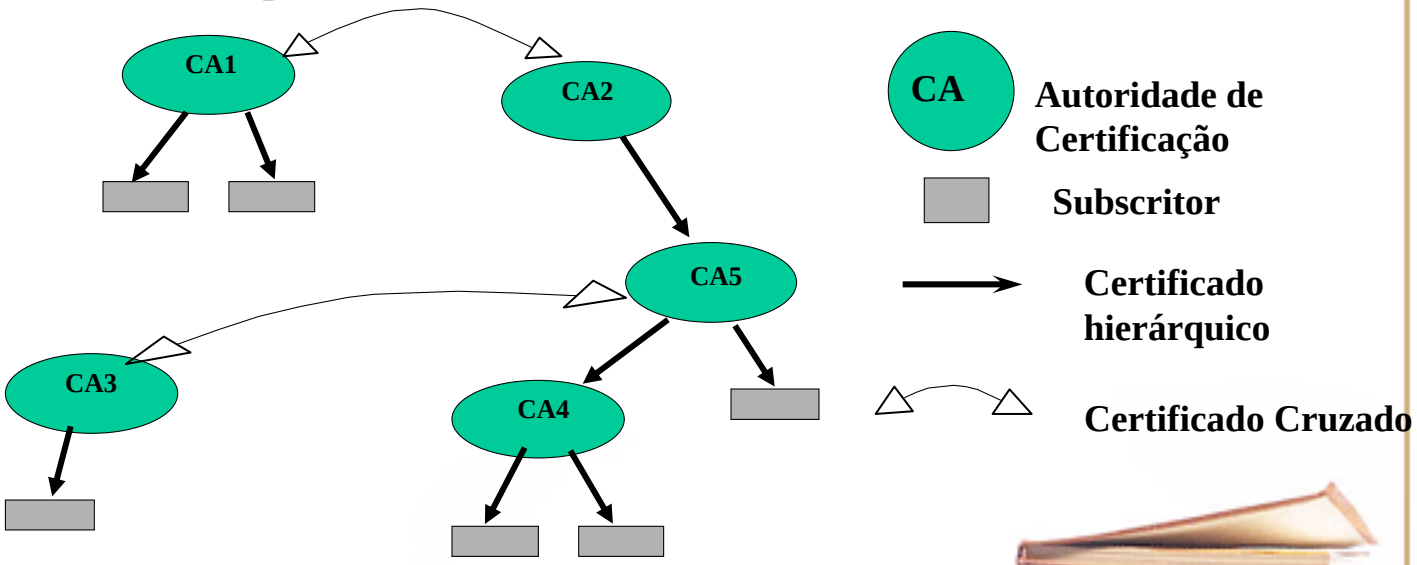
- As entidades verificadores confiam na chave pública de uma CA única e bem conhecida (*trusted single root*)
- Subscritores obtém um certificado assinado pela chave privada da CA.
- As entidades verificadores verificam a validade dos certificados com a chave pública da CA

Hierárquico



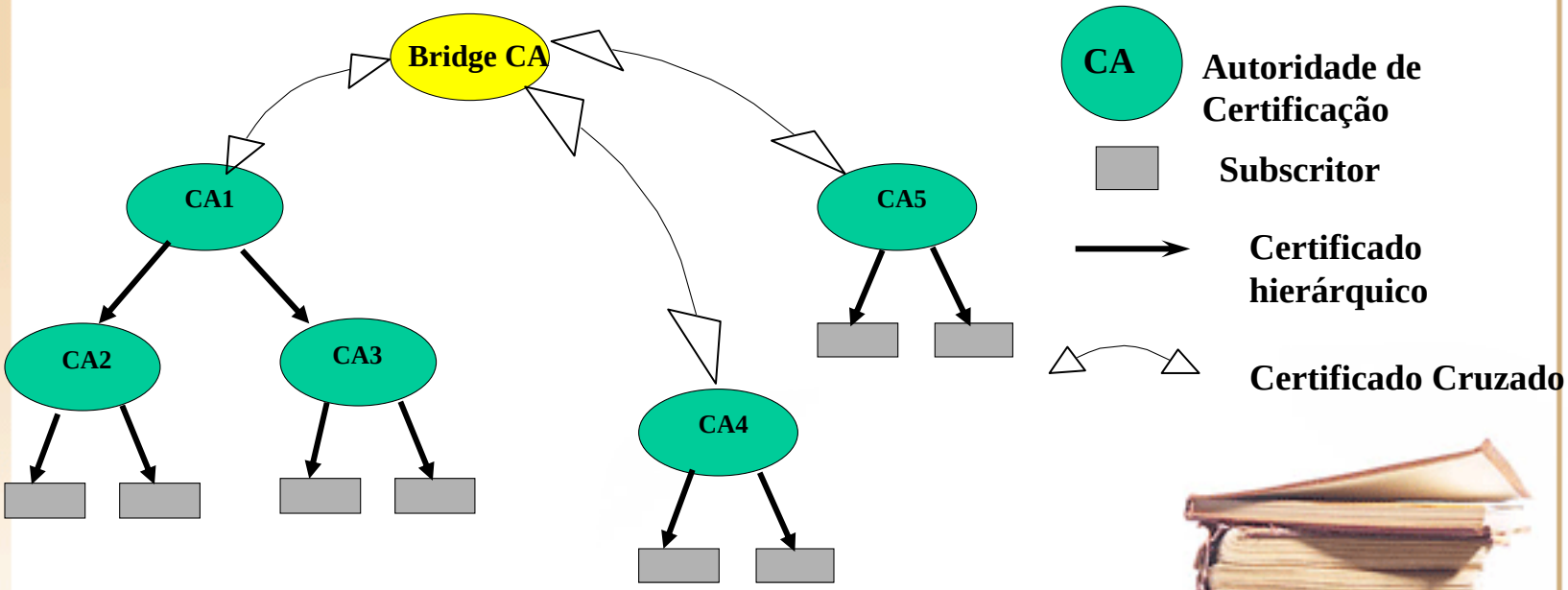
- Uma árvore de autoridades de certificação
- As entidades verificadores confiam na chave da CA1
- As CAs emitem certificados para subscritores e para outras CAs
- As entidades verificadores verificam os certificados dos subscritores por verificação sucessiva de certificados até à raiz da árvore

Certificação cruzada: MESH



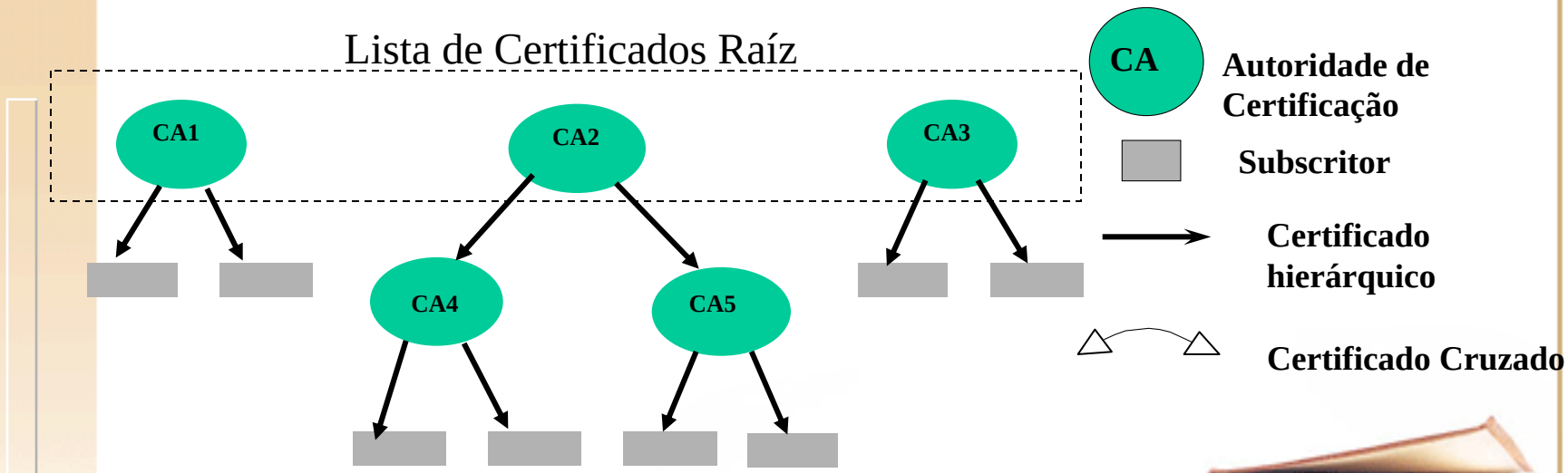
- A rede de confiança é formada pela criação de certificados cruzados entre CAs
- As entidades verificadoras confiam nas suas CAs locais
- Os subscritores podem ser certificados por CAs remotas
- As entidades de verificação verificam uma cadeia de certificação que vai desde a sua CA local até ao subscritor.

Interligação por Ponte



- Duas ou mais PKIs emitem certificados cruzados para um CA "Ponte"
- As entidades verificadores criam as cadeias de certificação através da CA ponte.

Lista de Certificados



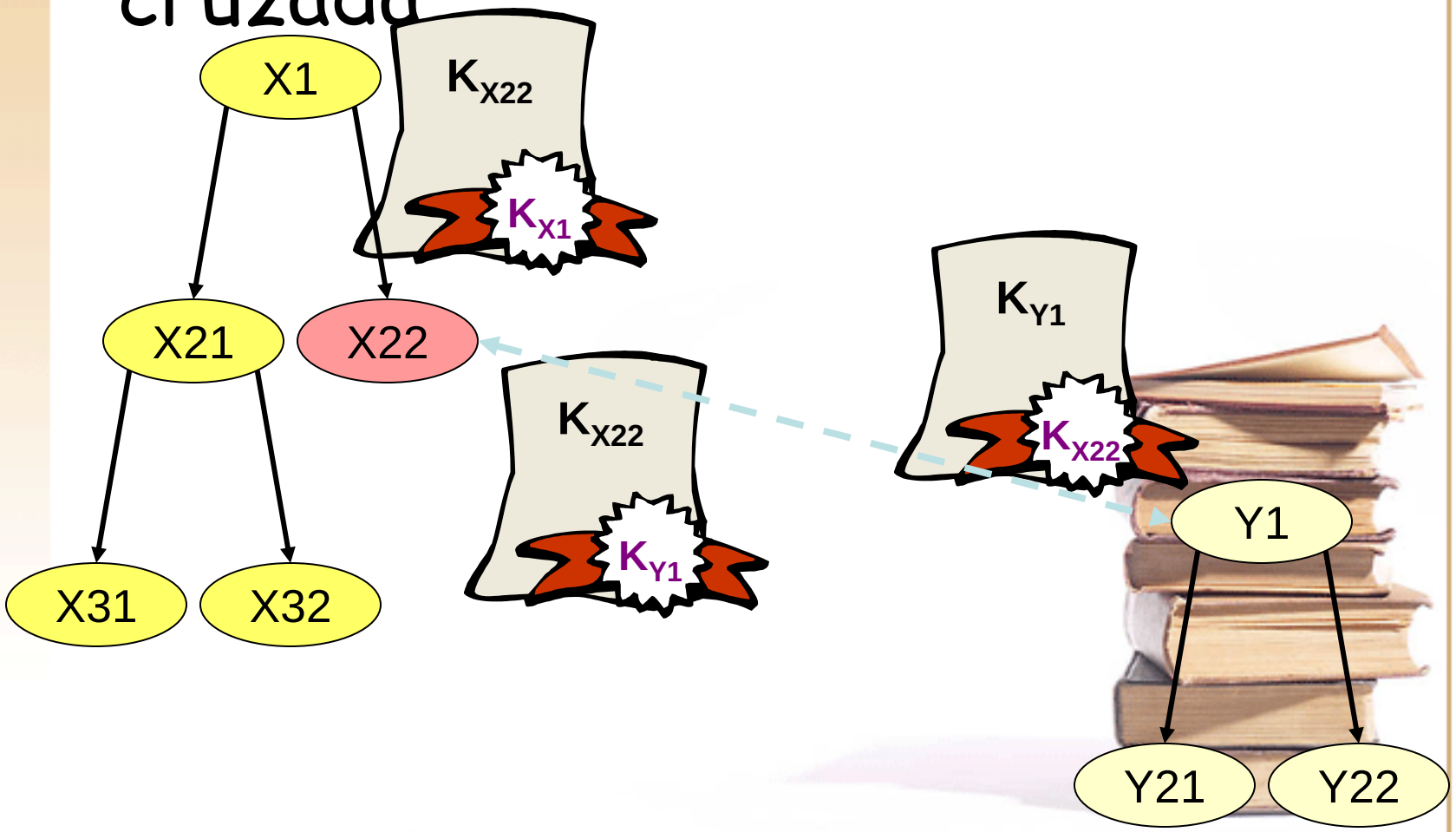
- As entidades verificadores confiam em chaves de várias CAs
- As entidades verificadoras validam as cadeias de certificam que conduzam a qualquer uma das CAs

Que estrutura utilizar?

- Planas e lista de raízes
  - Muito comuns
- Hierárquicas
  - Difíceis de construir incrementalmente
- Ponte e Mesh
  - Muita raras
  - Facilitam a construção incremental
  - Produzem ciclos e caminhos sem saída nas cadeias de certificados.

PKI:

Certificação hierarquica e cruzada



Processo de validação (1/3)

- Construção da cadeia
- Validação básica dos certificados da cadeia
- Processamento das extensões dos certificados
  - Extensões do sujeito e do emissor
  - Extensões das chaves
  - Extensões das políticas
  - Restrições ao caminho
- Verificação da não revogação
  - Obtenção de dados de revogação
  - Processamento dos dados

Processo de validação (2/3)

- Construção das cadeias
  - Rede não trivial de atravessar
- Validação das cadeias
  - Difícil verificação das extensões
- Validação das cadeias de revogação
  - Obtenção e verificação complexa
- Existem servidores expecializados
  - Online Certificate Status Protocol
  - Online Certificate Status Protocol v2
  - Simple Certificate Validation Protocol (SCVP)
  - Data Validation and Certification Server (DVCS)

Processo de validação (2/3)

- OCSP Version 2
  - **Online Revocation Status (ORS)**
    - fornece informação actual sobre revogações.
  - **Delegated Path Validation (DPV)**
    - Delega validações complicadas para o servidor especializado
  - **Delegated Path Discovery (DPD)**
    - Delega construções de cadeias complexas para um servidor especializado.

DVDS

- Validação
  - SCVP
- Construção de cadeias
  - Do raiz para o cliente
  - Do cliente para a raiz
- Validação dos CRLs

Documentação adicional

- Internet X.509 Public Key Infrastructure: Certificate and CRL Profile

  RFC 3280 de 2002 substitui o RFC 2459 de 1999

- Outros RFCs
  - 2510, 2511, 2527, 2528, 2559, 2560, 2585, 2587
  - 3029, 3039, 3161