Distribuição de Chaves e Certificação

Ricardo C. A. da Rocha

2009

Roteiro

- Gerenciamento de Chaves Públicas
- Certificados Digitais
- X.509
- Infra-estruturas de Chave pública

Gerenciamento de Chaves Públicas

- Criptografia de chave pública depende fortemente da confiança na chave pública de uma entidade.
- Falsificar chave pública possibilita **falsificar identidade**.
- Como distribuir chaves?

Três Modelos de Relações de Confiança

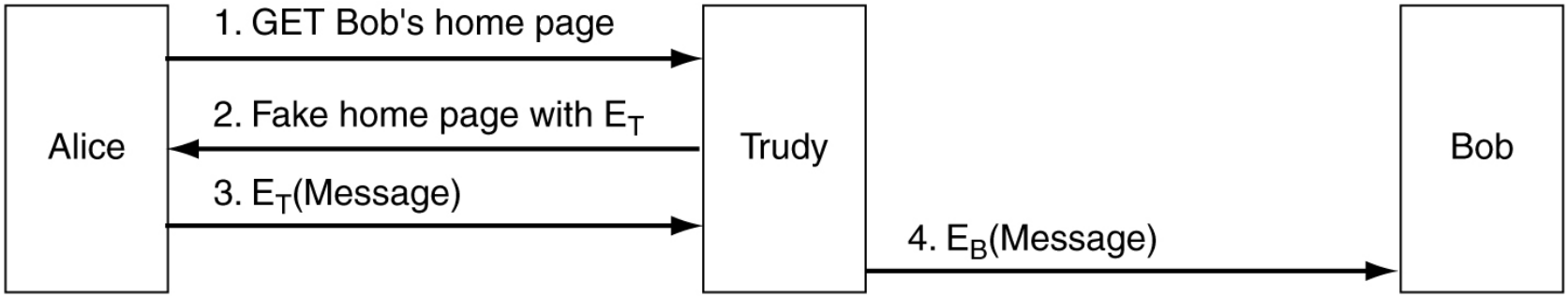
Confiança Direta
- Dois usuários trocam chaves públicas pessoalmente

Teia de Confiança (Web of Trust)
- Se **A** conhece **B** e **B** conhece **C** e **A** e **C** precisam conversar entre si, **B** assina chave de **C** para **A** e a chave de **A** para **C**

Confiança Hierárquica
- Alguns elementos chamados autoridades de certificação são conhecidos por todos e assinam hierarquicamente as chaves dos demais participantes.

Gerenciamento de Chaves Públicas

- Mecanismo simples de distribuição dá margem a ataques triviais.
- Exemplo: Trudy falsifica chave pública de Bob.



Certificado Digital

- Certificado Digital (para chave pública)
  - Documento digital que certifica (assegura) que uma chave pública pertence a uma entidade particular.
- Como documentos do mundo real, exige um intermediário de confiança que assegure a informação indicada.
  - **Chave pública**: **Autoridade Certificadora** (Certification Authority – CA)
  - **Chave privada**: **Central de Distribuição de Chaves** (Key Distribution Center – KDC)

Certificado Digital

```
Eu certifico que a chave pública:
    a7 23 38 36 23 94 d5 5b c8 30 03 ...
pertence a:
    Banco do Brasil S.A.
    www.bancodobrasil.com.br
    Unidade responsável: DITEC

Hash SHA-1 do certificado assinado com chave privada da CA
```

Geração de Certificado de Chave Pública

Autoridade Certificadora

CA

CHAVE PRIVADA

Certificado X509

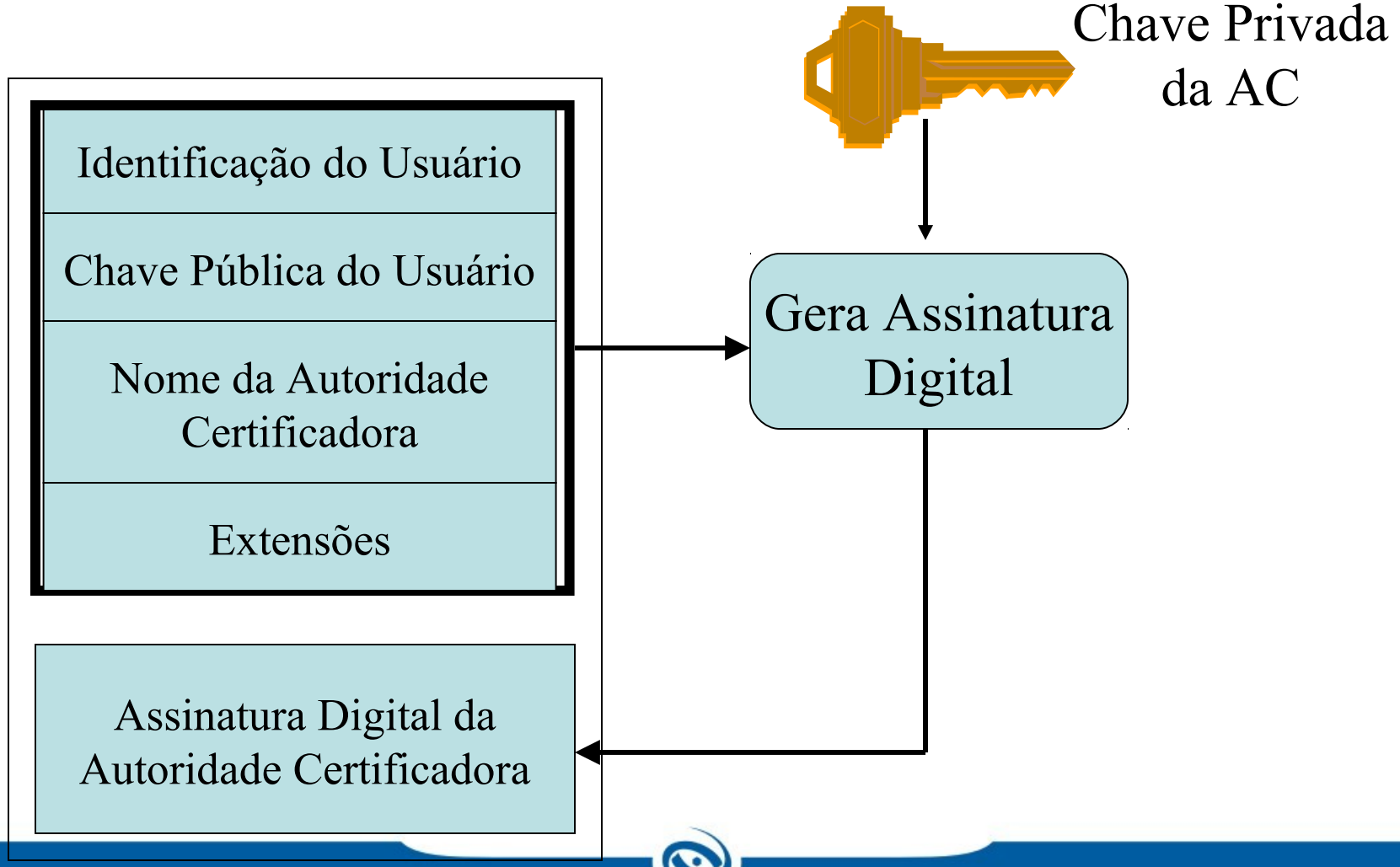
	I.D. do Proprietário	I.D. da CA	Assinatura Digital

Chave pública (e.g., Banco do Brasil)

www.bancodobrasil.com.br
Banco do Brasil S.A.
Brasília, DF, Brasil

www.verisign.com
Verisign, Inc.

Geração de Certificado Digital



Geração de Certificado de Chave Pública

- Usa assinatura digital usando criptografia assimétrica.
- Certificado é assinado pela CA, utilizando a sua chave privada.
- Chave pública de CA deve ser bem conhecida
  - Controle rigoroso da chave pública
  - Garantir consistência das chaves públicas de um conjunto limitado e bem conhecido de CAs é mais simples.

Certificado X.509

Padrão de certificados digitais proposto inicialmente pela ITU e adotado pelo IETF (RFC 3280 e 1422).

- Codificado por meio da sintaxe ASN.1 (Abstract Syntax Notation 1)
- Endereços X.500

  /C=<*país*>/O=<*organização*>/OU=<*unidade*>
  /CN=<*nome comum*>/

  /C=BR/ST=Distrito Federal/L=Brasilia/O=Banco do Brasil S.A./OU=DITEC/CN=www2.bancobrasil.com.br

Atributos de Certificados X.509

- **`Version`**: do X.509
- **`Serial number`**: gerado pela CA
- **`Signature`** (algoritmo e ID): algoritmo utilizado na assinatura
- **`Issuer name`**: nome X.500 da CA
- **`Validity period`**
- **`Subject name`**: entidade sendo certificada
- **`Subject public key`** (e ID do algoritmo): algoritmo associado chave pública

Exemplo

```
Certificate:
   Data:
       Version: 1 (0x0)
       Serial Number: 7829 (0x1e95)
       Signature Algorithm: md5WithRSAEncryption
       Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
               OU=Certification Services Division,
               CN=Thawte Server CA/emailAddress=server-certs@thawte.com
       Validity
           Not Before: Jul  9 16:04:02 1998 GMT
           Not After : Jul  9 16:04:02 1999 GMT
       Subject: C=US, ST=Maryland, L=Pasadena, O=Brent Baccala,
                OU=FreeSoft, CN=www.freesoft.org/emailAddress=baccala@freesoft.org
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
           RSA Public Key: (1024 bit)
               Modulus (1024 bit):
                   00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb:
                   33:35:19:d5:0c:64:b9:3d:41:b2:96:fc:f3:31:e1:
                   ...
               Exponent: 65537 (0x10001)
   Signature Algorithm: md5WithRSAEncryption
       93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:
       92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:2f:92:
       ...
```

Uso de Certificados X.509

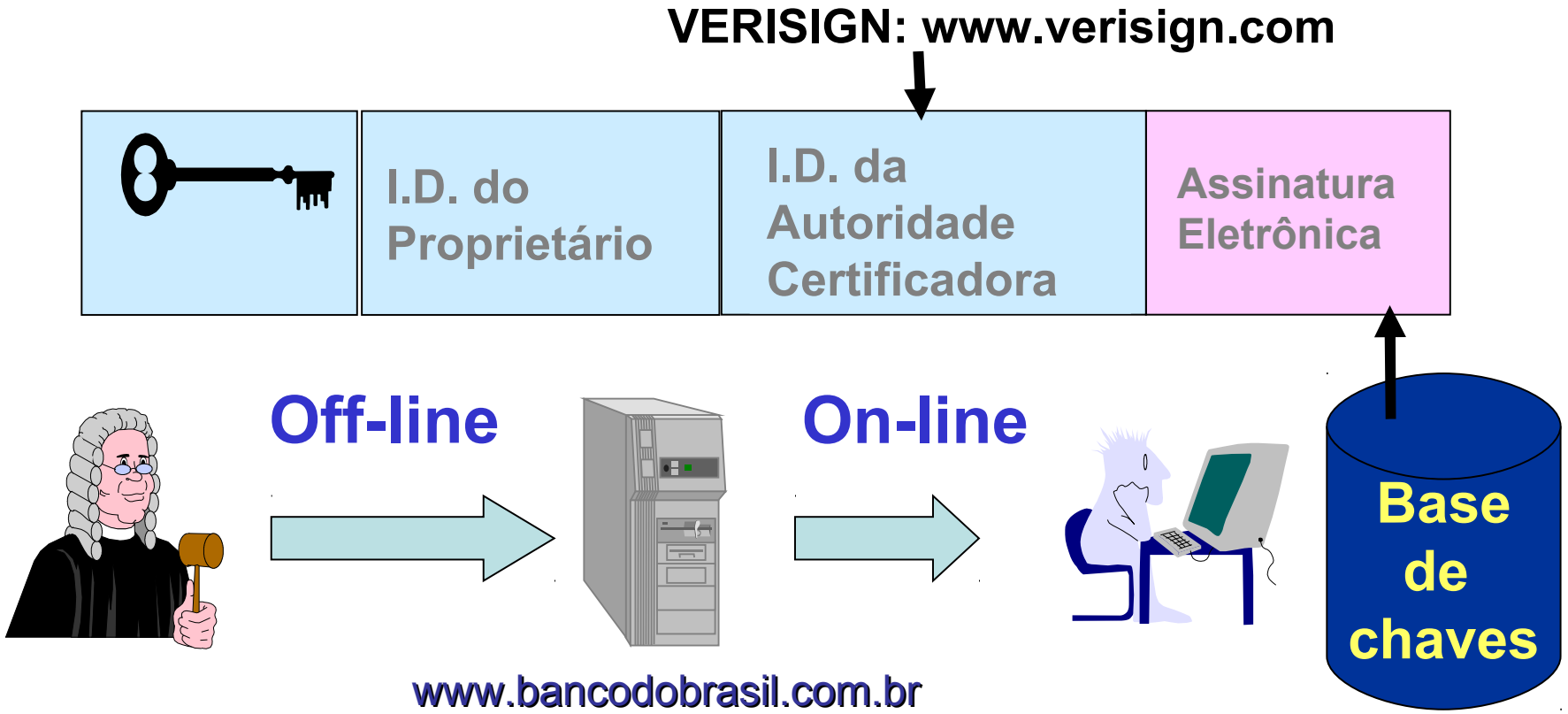
- Transport Layer Security (SSL/TLS)
- IPSec
- S/MIME
- SSH
- Smartcard
- HTTPS
- LDAPv3

entre outros.

Extensões de Arquivos de Certificados

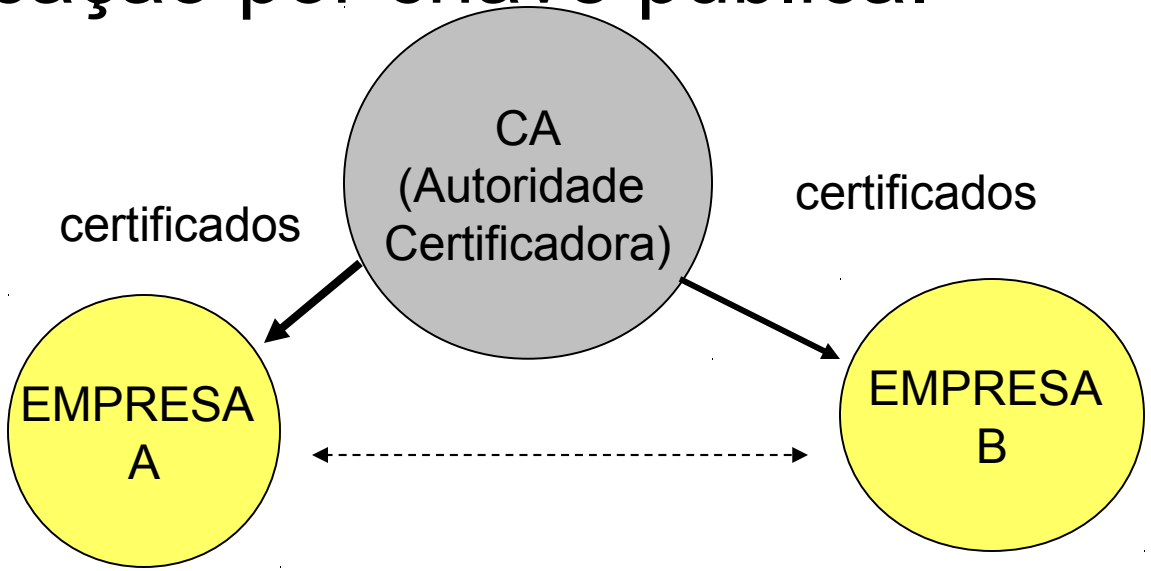
- `.DER`: codificação DER da ISO/ITU
- `.PEM`: Base64 de Privacy Enhanced Mail
- `.cer`, `.crt`: formato binário ou base64
- `.P7B`, `.P7C`: formato definido pela RSA
- `.PFX`, `.P12`: formato definido pela RSA, que sucede o PFX da MS.

Estratégias de Certificação



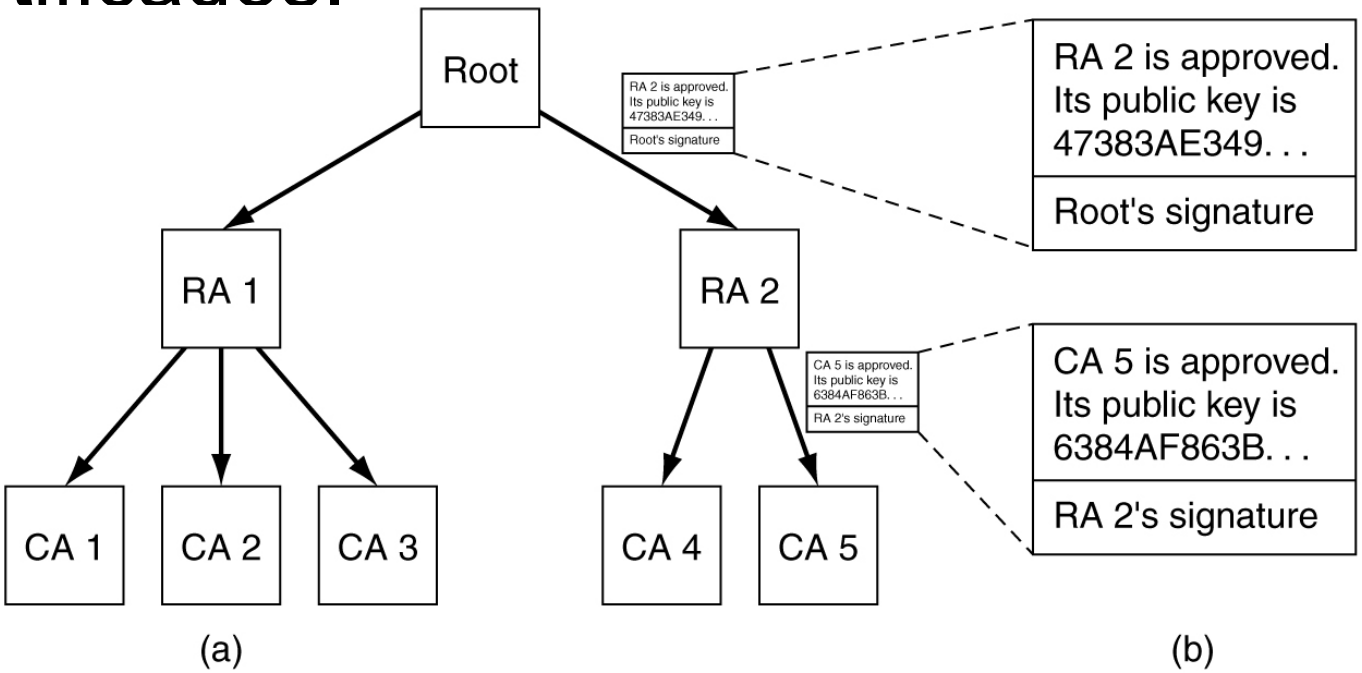
PKI – Infra-estrutura de chave pública

Conjunto de elementos necessários para implementar um mecanismo de certificação por chave pública.



Infra-estrutura de chave pública

Infra-estrutura hierárquica com cadeia de certificados.



Componentes de uma PKI (RFC 2459)

- **Entidade final**: usuária do certificado
- **CA** (Certification Authority): responsável por gerar certificados
- **RA** (Registration Authority): faz registros de certificados sob delegação de uma CA
- **Repository**: BD de certificados
- **Caminho de certificação**
- **Lista de revogação**: lista de certificados que devem ser considerados inválidos

Componentes de uma PKI

Protocolos operacionais: necessário para distribuição de certificados

Protocolos de gerenciamento: define como os certificados serão gerados

Exemplos de CAs