Introdução à Criptografia

Assinatura e Certificado Digital

Prof. Rodrigo Minetto
rminetto@dainf.ct.utfpr.edu.br
Universidade Tecnológica Federal do Paraná
Baseado em: Understanding Cryptography by Paar e Pelzl

Sumário

Introdução

Definição: **assinatura digital** é em essência uma sequência numérica, derivada de um documento eletrônico de origem, e criada com o uso de uma função matemática de **criptografia assimétrica**. A assinatura digital é capaz de atestar a originalidade de uma mensagem ou documento (validade jurídica). O algoritmo RSA é amplamente utilizado para este propósito.

Introdução

Observe a diferença de uma **assinatura digital**, que é única para cada documento assinado, para uma **assinatura formal**, que é uma marca personalíssima, gravada de forma idêntica em todos os documentos produzidos por seu autor. Também não confunda uma assinatura digital com uma **assinatura digitalizada** (mera transposição do sinal físico para um sinal eletrônico).

Introdução

As assinaturas digitais tem o mesmo objetivo que as assinaturas convencionais em papel tentam alcançar, que são, **autenticação do remetente**, **não-repúdio** e **garantia da integridade da mensagem**. A integridade garante que qualquer alteração da mensagem faz com que a assinatura não corresponda mais ao documento. Sem estes predicados, por exemplo, não seria possível realizar o comércio eletrônico seguro na Internet.

Introdução

Cenário 1: autenticidade (garante a identidade de quem está enviando a mensagem).

Introdução

Cenário 1: autenticidade (garante a identidade de quem está enviando a mensagem).

Comprar 500 kg de ouro $\longrightarrow$

Introdução

Cenário 1: autenticidade (garante a identidade de quem está enviando a mensagem).

Comprar 500 kg de ouro $\longrightarrow$

Introdução

Cenário 2: não-repúdio ou irretratabilidade (o emissor não pode negar a autenticidade da mensagem).

Introdução

Cenário 2: não-repúdio ou irretratabilidade (o emissor não pode negar a autenticidade da mensagem).

Comprar 500 kg de ouro $\longrightarrow$

Introdução

Cenário 2: não-repúdio ou irretratabilidade (o emissor não pode negar a autenticidade da mensagem).

Comprar 500 kg de ouro $\longrightarrow$

Introdução

Cenário 2: não-repúdio ou irretratabilidade (o emissor não pode negar a autenticidade da mensagem).

Comprar 500 kg de ouro $\longrightarrow$

Introdução

Cenário 3: integridade (garante que o conteúdo da mensagem não foi alterado pelo receptor).

Introdução

Cenário 3: integridade (garante que o conteúdo da mensagem não foi alterado pelo receptor).

Comprar 500 kg de ouro $\longrightarrow$

Introdução

Cenário 3: integridade (garante que o conteúdo da mensagem não foi alterado pelo receptor).

Comprar 500 kg de ouro $\longrightarrow$

Introdução

Cenário 3: integridade (garante que o conteúdo da mensagem não foi alterado pelo receptor).

Comprar 500 kg de ouro $\longrightarrow$

Introdução

Cenário 3: integridade (garante que o conteúdo da mensagem não foi alterado pelo receptor).

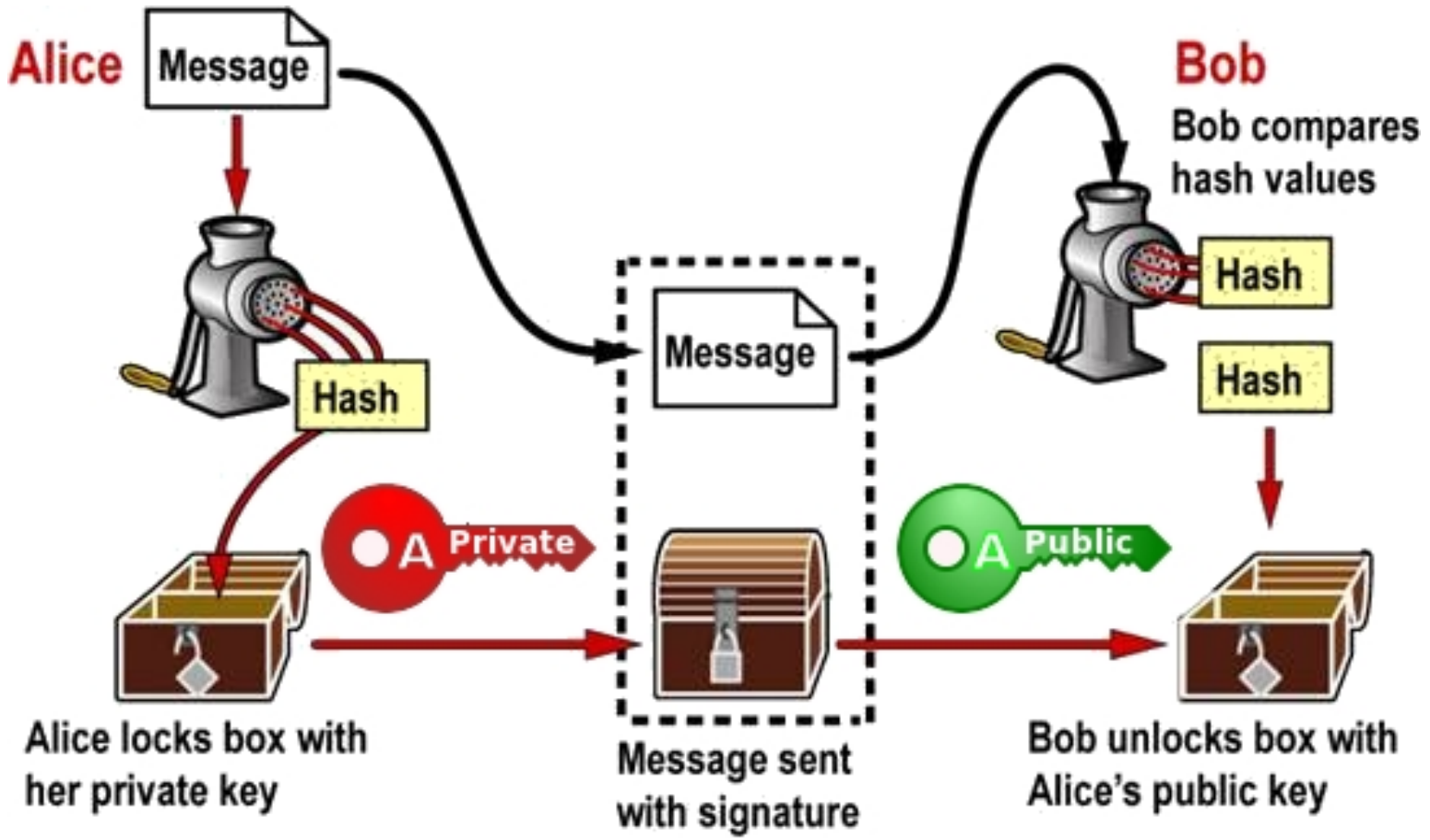
Ordem de **10** kg de ouro

Introdução

A assinatura digital se baseia no conceito de **chave privada** e **chave pública**. Se a **chave privada**, de conhecimento exclusivo do autor, é utilizada para codificar uma informação, então apenas seu dono poderia ter feito isto. Portanto, é possível "provar para um terceiro (juiz em um tribunal) que só o proprietário da chave privada poderia ter gerado a mensagem", alcançando assim as finalidades da assinatura formal. A verificação da assinatura é feita com o uso da **chave pública**, pois se o texto foi codificado com a chave privada, somente a chave pública correspondente pode decodificá-lo.

Assinatura Digital com RSA

Devido a baixa performance da criptografia assimétrica, a assinatura digital é realizada sobre um resumo da mensagem (hash) de tamanho fixo e reduzido.



Sumário

RSA

Geração de chaves

1. Selecione dois primos grandes p e q;
2. Calcule $\mathbf{n} = p \times q$;
3. Calcule $\phi(\mathbf{n}) = (p-1) \times (q-1)$;
4. Escolha $0 < \boldsymbol{e} < \phi(\mathbf{n})$ tal que

   $\textbf{MDC-}\textsc{Euclides-Estendido}(\phi, \boldsymbol{e}, a, \mathbf{b}) = 1$

   Enquanto $(\mathbf{b} < 0)$ { $\mathbf{b} = \mathbf{b} + \phi(\mathbf{n})$; }
5. Calcule $\mathbf{d} = \mathbf{b} \bmod \phi(\mathbf{n})$; $(\mathbf{b} = \boldsymbol{e}^{-1})$
6. Publique a chave $k_{\text{pub}} = (\boldsymbol{e}, \mathbf{n})$;
7. Proteja a chave $k_{\text{priv}} = (\mathbf{d}, \mathbf{n})$;

RSA

Seja a chave pública $k_{\text{pub}} = (\boldsymbol{e}, \mathbf{n})$ e o texto em claro $\mathbf{x}$, a função de ciframento é definida por:

Ciframento

$$\mathbf{y} = \mathbf{x}^{\boldsymbol{e}} \bmod \mathbf{n}$$

onde $x, y \in \mathbb{Z}_n$.

RSA

Seja a chave privada $k_{\text{priv}} = (\mathbf{d}, \mathbf{n})$ e o texto cifrado $\mathbf{y}$, a função de deciframento é definida por:

Deciframento

$$\mathbf{x} = \mathbf{y}^{\mathbf{d}} \bmod \mathbf{n}$$

onde $x, y \in \mathbb{Z}_n$.

RSA

Exemplo de cifragem e decifragem:

RSA

Exemplo de cifragem e decifragem:

Alice $\leftarrow$ Bob

$k_{\text{pub}} = (\mathbf{e}, \mathbf{n})$

Exemplo de cifragem e decifragem:

Alice

Bob

$\leftarrow \quad k_{\text{pub}} = (\mathbf{3}, \mathbf{33})$

RSA

Exemplo de cifragem e decifragem:

Alice

Bob

$\leftarrow \quad k_{\text{pub}} = (3, 33)$

$x = 4$

RSA

Exemplo de cifragem e decifragem:

Alice $\leftarrow$ Bob

$k_{\text{pub}} = (\mathbf{3}, \mathbf{33})$

$\mathbf{x} = \mathbf{4}$

$\mathbf{y} = \mathbf{x}^{e} \bmod \mathbf{n}$

RSA

Exemplo de cifragem e decifragem:

Alice $\leftarrow$ Bob

Bob: $k_{\text{pub}} = (\mathbf{3}, \mathbf{33})$

$\mathbf{x} = \mathbf{4}$

$\mathbf{y} = \mathbf{x}^{e} \bmod \mathbf{n}$

$\mathbf{y} = \mathbf{4}^{\mathbf{3}} \bmod \mathbf{33}$

RSA

Exemplo de cifragem e decifragem:

Alice $\leftarrow$ Bob

Bob: $k_{\text{pub}} = (\mathbf{3}, \mathbf{33})$

$\mathbf{x} = \mathbf{4}$

$\mathbf{y} = \mathbf{x}^{e} \bmod \mathbf{n}$

$\mathbf{y} = \mathbf{4}^{\mathbf{3}} \bmod \mathbf{33}$

$\mathbf{y} = \mathbf{31} \rightarrow$

RSA

Exemplo de cifragem e decifragem:

Alice		Bob
	$\leftarrow$	$k_{\text{pub}} = (\mathbf{3}, \mathbf{33})$
$\mathbf{x} = \mathbf{4}$		
$\mathbf{y} = \mathbf{x}^{e} \bmod \mathbf{n}$		
$\mathbf{y} = \mathbf{4}^{\mathbf{3}} \bmod \mathbf{33}$		
$\mathbf{y} = \mathbf{31}$	$\rightarrow$	
		$k_{\text{priv}} = (\mathbf{d}, \mathbf{n})$

RSA

Exemplo de cifragem e decifragem:

Alice

Bob

$\leftarrow \quad k_{\text{pub}} = (\mathbf{3}, \mathbf{33})$

$\mathbf{x} = \mathbf{4}$

$\mathbf{y} = \mathbf{x}^{e} \bmod \mathbf{n}$

$\mathbf{y} = \mathbf{4}^{\mathbf{3}} \bmod \mathbf{33}$

$\mathbf{y} = \mathbf{31} \quad \rightarrow$

$k_{\text{priv}} = (\mathbf{7}, \mathbf{33})$

RSA

Exemplo de cifragem e decifragem:

Alice		Bob
	$\leftarrow$	$k_{\text{pub}} = (\mathbf{3}, \mathbf{33})$
$\mathbf{x} = \mathbf{4}$		
$\mathbf{y} = \mathbf{x}^{e} \bmod \mathbf{n}$		
$\mathbf{y} = \mathbf{4}^{\mathbf{3}} \bmod \mathbf{33}$		
$\mathbf{y} = \mathbf{31}$	$\rightarrow$	
		$k_{\text{priv}} = (\mathbf{7}, \mathbf{33})$
		$\mathbf{x} = \mathbf{y}^{\mathbf{d}} \bmod \mathbf{n}$

RSA

Exemplo de cifragem e decifragem:

Alice		Bob
	$\leftarrow$	$k_{\text{pub}} = (3, 33)$
$x = 4$		
$y = x^e \bmod n$		
$y = 4^3 \bmod 33$		
$y = 31$	$\rightarrow$	
		$k_{\text{priv}} = (7, 33)$
		$x = y^d \bmod n$
		$x = 31^7 \bmod 33$

Exemplo de cifragem e decifragem:

Alice		Bob
	$\leftarrow$	$k_{\text{pub}} = (\mathbf{3}, \mathbf{33})$
$\mathbf{x} = \mathbf{4}$		
$\mathbf{y} = \mathbf{x}^{e} \bmod \mathbf{n}$		
$\mathbf{y} = \mathbf{4}^{\mathbf{3}} \bmod \mathbf{33}$		
$\mathbf{y} = \mathbf{31}$	$\rightarrow$	
		$k_{\text{priv}} = (\mathbf{7}, \mathbf{33})$
		$\mathbf{x} = \mathbf{y}^{\mathbf{d}} \bmod \mathbf{n}$
		$\mathbf{x} = \mathbf{31}^{\mathbf{7}} \bmod \mathbf{33}$
		$\mathbf{x} = \mathbf{4}$

RSA

Seja o processo de cifragem e decifragem:

$$\mathbf{y} = \mathbf{x}^{e} \bmod \mathbf{n} \qquad \mathbf{x} = \mathbf{y}^{\mathbf{d}} \bmod \mathbf{n}$$

portanto temos que

$$\begin{aligned} \mathbf{x} &= \mathbf{y}^{\mathbf{d}} \bmod \mathbf{n} \\ \mathbf{x} &= (\mathbf{x}^{e})^{\mathbf{d}} \bmod \mathbf{n} \\ \mathbf{x} &= (\mathbf{x}^{\mathbf{d}})^{e} \bmod \mathbf{n} \end{aligned}$$

onde $(\mathbf{x}^{e})^{\mathbf{d}} = \mathbf{x}^{e \times \mathbf{d}} = \mathbf{x}^{\mathbf{d} \times e} = (\mathbf{x}^{\mathbf{d}})^{e}$.

Sumário

Assinatura Digital com RSA

Alice

Bob

Assinatura Digital com RSA

Alice

Bob

$k_{\text{priv}} = (\mathbf{d}, \mathbf{n})$

$\leftarrow \quad k_{\text{pub}} = (\mathbf{e}, \mathbf{n})$

Assinatura Digital com RSA

Alice		Bob
		$k_{\text{priv}} = (\mathbf{d}, \mathbf{n})$
$k_{\text{pub}} = (\mathbf{e}, \mathbf{n})$	$\leftarrow$	$k_{\text{pub}} = (\mathbf{e}, \mathbf{n})$

Assinatura Digital com RSA

Alice		Bob
		$k_{\text{priv}} = (\mathbf{7}, \mathbf{33})$
$k_{\text{pub}} = (\mathbf{3}, \mathbf{33})$	$\leftarrow$	$k_{\text{pub}} = (\mathbf{3}, \mathbf{33})$

Assinatura Digital com RSA

Alice		Bob
		$k_{\text{priv}} = (\mathbf{7}, \mathbf{33})$
$k_{\text{pub}} = (\mathbf{3}, \mathbf{33})$	$\leftarrow$	$k_{\text{pub}} = (\mathbf{3}, \mathbf{33})$
		$\mathbf{x} = \mathbf{4}$

Assinatura Digital com RSA

Alice		Bob
		$k_{\text{priv}} = (\mathbf{7}, \mathbf{33})$
$k_{\text{pub}} = (\mathbf{3}, \mathbf{33})$	$\leftarrow$	$k_{\text{pub}} = (\mathbf{3}, \mathbf{33})$
		$\mathbf{x} = \mathbf{4}$
		$\mathbf{s}_b = \mathbf{4}^{\mathbf{d}} \mathbf{mod}\ \mathbf{33}$

Assinatura Digital com RSA

Alice		Bob
		$k_{\text{priv}} = (7, 33)$
$k_{\text{pub}} = (3, 33)$	$\leftarrow$	$k_{\text{pub}} = (3, 33)$
		$x = 4$
		$s_b = 4^7 \bmod 33$

Assinatura Digital com RSA

Alice		Bob
		$k_{\text{priv}} = (\mathbf{7}, \mathbf{33})$
$k_{\text{pub}} = (\mathbf{3}, \mathbf{33})$	$\leftarrow$	$k_{\text{pub}} = (\mathbf{3}, \mathbf{33})$
		$\mathbf{x} = \mathbf{4}$
		$\mathbf{s}_b = \mathbf{4}^{\mathbf{7}} \text{mod } \mathbf{33}$
		$\mathbf{s}_b$ é a assinatura

Assinatura Digital com RSA

Alice		Bob
		$k_{\text{priv}} = (7, 33)$
$k_{\text{pub}} = (3, 33)$	$\leftarrow$	$k_{\text{pub}} = (3, 33)$
		$x = 4$
		$s_b = 4^7 \bmod 33$
		$s_b = 16$

Assinatura Digital com RSA

Alice		Bob
		$k_{\text{priv}} = (\mathbf{7}, \mathbf{33})$
$k_{\text{pub}} = (\mathbf{3}, \mathbf{33})$	$\leftarrow$	$k_{\text{pub}} = (\mathbf{3}, \mathbf{33})$
		$\mathbf{x} = \mathbf{4}$
		$\mathbf{s}_b = \mathbf{4}^{\mathbf{7}} \text{mod } \mathbf{33}$
		$\mathbf{s}_b = \mathbf{16}$
	$\leftarrow$	**Envia** $\mathbf{x}$ e $\mathbf{s}_b$

Assinatura Digital com RSA

Alice		Bob
		$k_{\text{priv}} = (7, 33)$
$k_{\text{pub}} = (3, 33)$	$\leftarrow$	$k_{\text{pub}} = (3, 33)$
		$x = 4$
		$s_b = 4^7 \bmod 33$
		$s_b = 16$
$x = 4$ e $s_b = 16$	$\leftarrow$	**Envia** x e s_b

Assinatura Digital com RSA

Alice		Bob
		$k_{\text{priv}} = (7, 33)$
$k_{\text{pub}} = (3, 33)$	$\leftarrow$	$k_{\text{pub}} = (3, 33)$
		$x = 4$
		$s_b = 4^7 \bmod 33$
		$s_b = 16$
$x = 4$ e $s_b = 16$	$\leftarrow$	**Envia** x e s_b
$x' = s_b^e \bmod n$		

Assinatura Digital com RSA

Alice		Bob
		$k_{\text{priv}} = (7, 33)$
$k_{\text{pub}} = (3, 33)$	$\leftarrow$	$k_{\text{pub}} = (3, 33)$
		$x = 4$
		$s_b = 4^7 \bmod 33$
		$s_b = 16$
$x = 4$ e $s_b = 16$	$\leftarrow$	**Envia** x e s_b
$x' = 16^3 \bmod 33$		

Assinatura Digital com RSA

Alice		Bob
		$k_{\text{priv}} = (7, 33)$
$k_{\text{pub}} = (3, 33)$	$\leftarrow$	$k_{\text{pub}} = (3, 33)$
		$x = 4$
		$s_b = 4^7 \bmod 33$
		$s_b = 16$
$x = 4$ e $s_b = 16$	$\leftarrow$	**Envia** x e s_b
$x' = 16^3 \bmod 33$		
$x' = 4$		

Assinatura Digital com RSA

Alice		Bob
		$k_{\text{priv}} = (7, 33)$
$k_{\text{pub}} = (3, 33)$	$\leftarrow$	$k_{\text{pub}} = (3, 33)$
		$x = 4$
		$s_b = 4^7 \bmod 33$
		$s_b = 16$
$x = 4$ e $s_b = 16$	$\leftarrow$	**Envia** x e s_b
$x' = 16^3 \bmod 33$		
$x' = 4$		
$x' = x$?		

Introdução

Note que no esquema de assinaturas digitais, o papel das chaves pública e privada são trocados, para assinar ciframos com a chave privada e para verificar uma assinatura, deciframos com a chave pública. Note também que as **assinaturas digitais** não são reutilizáveis (a assinatura digital de um documento qualquer não pode ser transferida para qualquer outro documento) e não garantem confidencialidade do documento.

Sumário

Questões:

1) Como obter chaves públicas?

2) Como certificar-se de que a chave recebida é realmente da parte intencionada?

Resposta: certificação digital!

Introdução

A **certificação digital** pode ser vista como um conjunto de técnicas, processos e normas estabelecidas ou adotadas, que visam propiciar mais segurança às comunicações e transações eletrônicas, proporcionando a autenticidade e integridade das informações que tramitam de forma eletrônica.

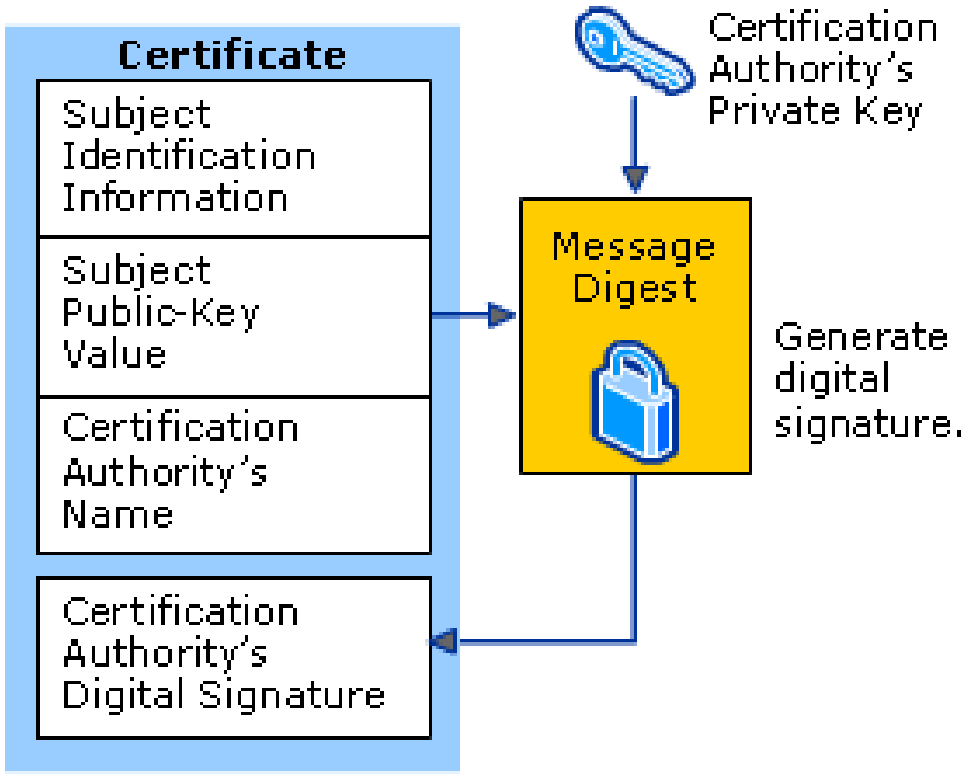
Certificado digital

Certificado digital: é um documento eletrônico no formato de arquivo, com um conjunto de informações que têm como objetivo associar o nome de uma entidade/pessoa com sua correspondente chave pública. Os certificados digitais são usados para evitar as tentativas de substituição da chave pública de uma pessoa por outra.

Certificado digital

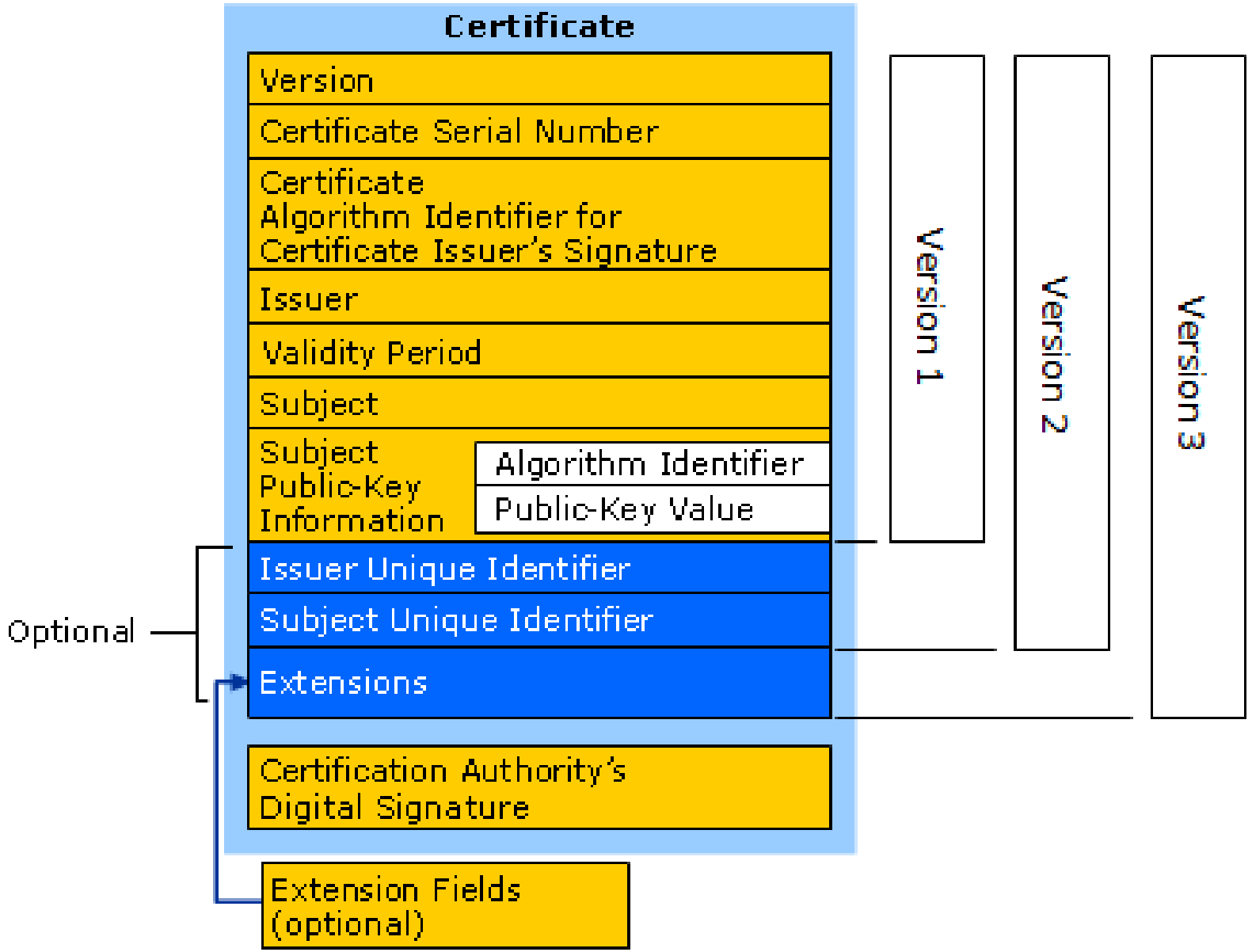
Um certificado digital é composto por:

- informações de identidade do usuário
- chave pública do dono do certificado;
- dados referentes à autoridade certificadora



Certificado digital

Estrutura do certificado X.509



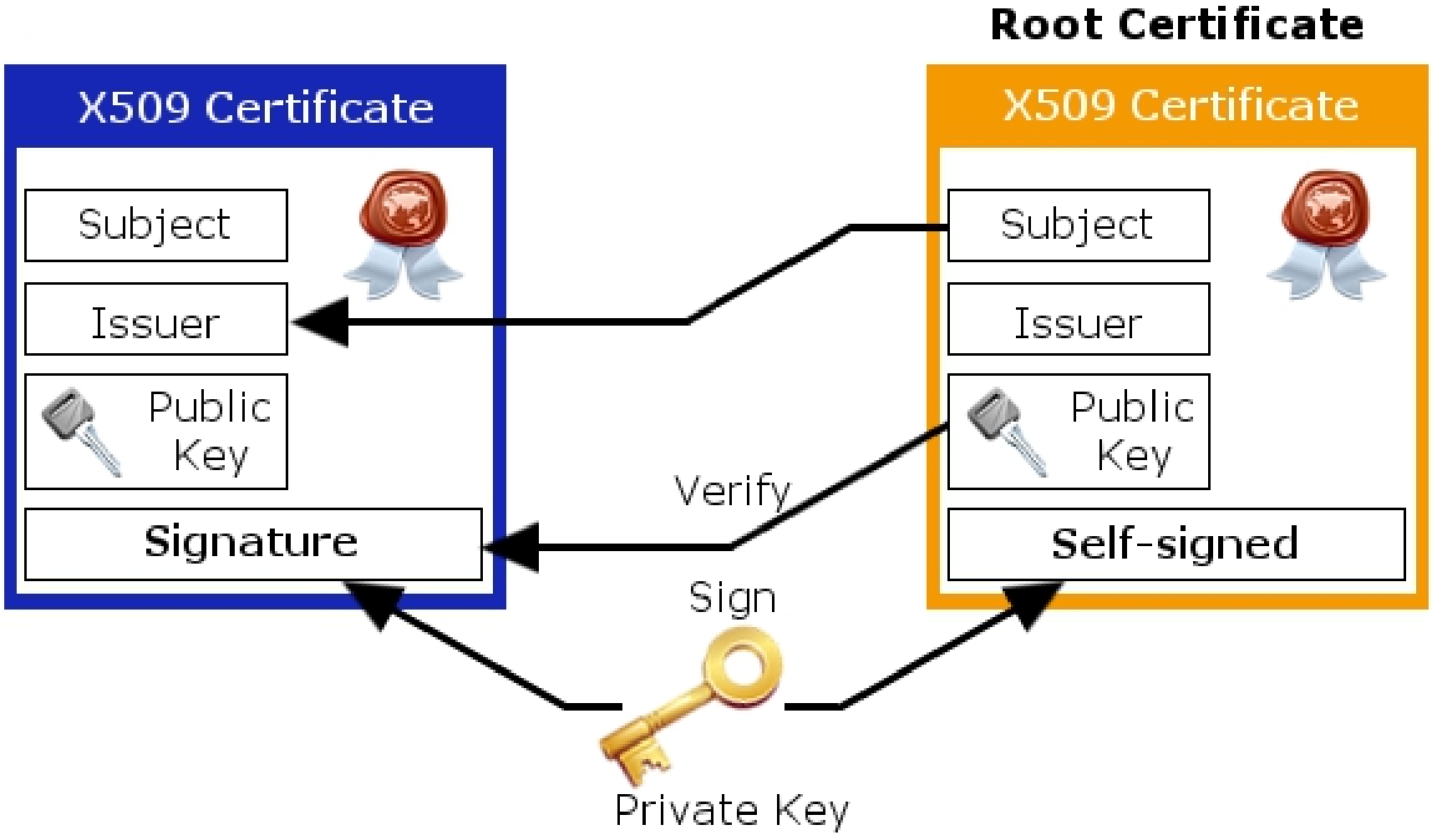
Certificado digital

Exemplo de um certificado X.509

```
    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:
                66:36:d0:8e:56:12:44:ba:75:eb:e8:1c:9c:5b:66:
                70:33:52:14:c9:ec:4f:91:51:70:39:de:53:85:17:
                16:94:6e:ee:f4:d5:6f:d5:ca:b3:47:5e:1b:0c:7b:
                c5:cc:2b:6b:c1:90:c3:16:31:0d:bf:7a:c7:47:77:
                8f:a0:21:c7:4c:d0:16:65:00:c1:0f:d7:b8:80:e3:
                d2:75:6b:c1:ea:9e:5c:5c:ea:7d:c1:a1:10:bc:b8:
                e8:35:1c:9e:27:52:7e:41:8f
            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:
```

Certificado digital

Assinatura de um certificado X.509



Sumário

Infraestrutura de Chaves Públicas

Uma **Infraestrutura de Chaves Públicas** (ICP), do inglês Public Key Infrastructure (PKI), é um órgão (iniciativa pública ou privada) que tem como objetivo manter uma estrutura de emissão de chaves públicas, baseando-se no princípio da terceira parte confiável, oferecendo uma mediação de credibilidade e confiança em transações entre partes que utilizam certificados digitais.

Infraestrutura de Chaves Públicas

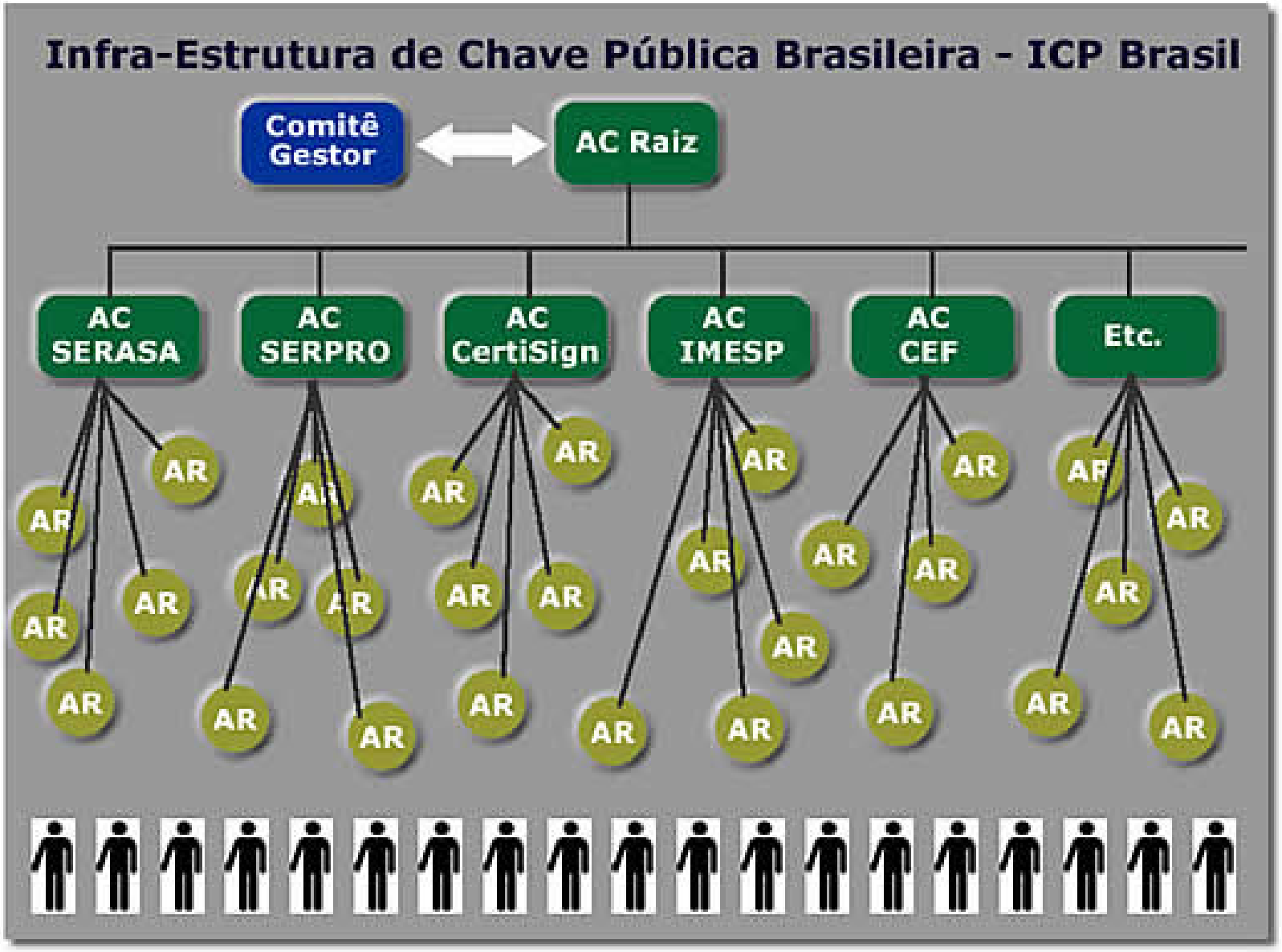
O **certificado digital** não é emitido pelas próprias pessoas e sim por terceiros de confiança. Por exemplo, o passaporte é emitido pela Receita Federal, instituição que atua como terceiro confiável para o mundo inteiro; o CPF é emitido pela Receita Federal, já o reconhecimento de assinaturas é realizado por cartórios, instituições que atuam como terceiro confiável para a Federação Brasileira.

Infraestrutura de Chaves Públicas

A Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil) é uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais. A Autoridade Certificadora (AC) Raiz, assina digitalmente os certificados das ACs de primeiro nível, que por sua vez assinam os de segundo nível. As ACs são responsáveis pelos certificados emitidos pelas Autoridades de Registro (AR). As ARs fazem o serviço de atendimento direto ao cidadão. AC Raiz, também, tem o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos.

Infraestrutura de Chaves Públicas

ICP-Brasil



Tipos de certificados da ICP-Brasil

Tipo de certificado	Chave criptográfica			Validade máxima (anos)
	Tamanho (bits)	Processo de geração	Mídia armazenadora	
A1 e S2	1024	Software	Arquivo	1
A2 e S2	1024	Sofware	Smart card ou token, sem capacidade de geração de chave	2
A3 e S3	1024	Hardware	Smart card ou token, com capacidade de geração de chave	3
A4 e S4	2048	Hardware	Smart card ou token, com capacidade de geração de chave	3

A = AUTENTICAÇÃO

S = SIGILO

Requisição de certificado:

Infraestrutura de Chaves Públicas

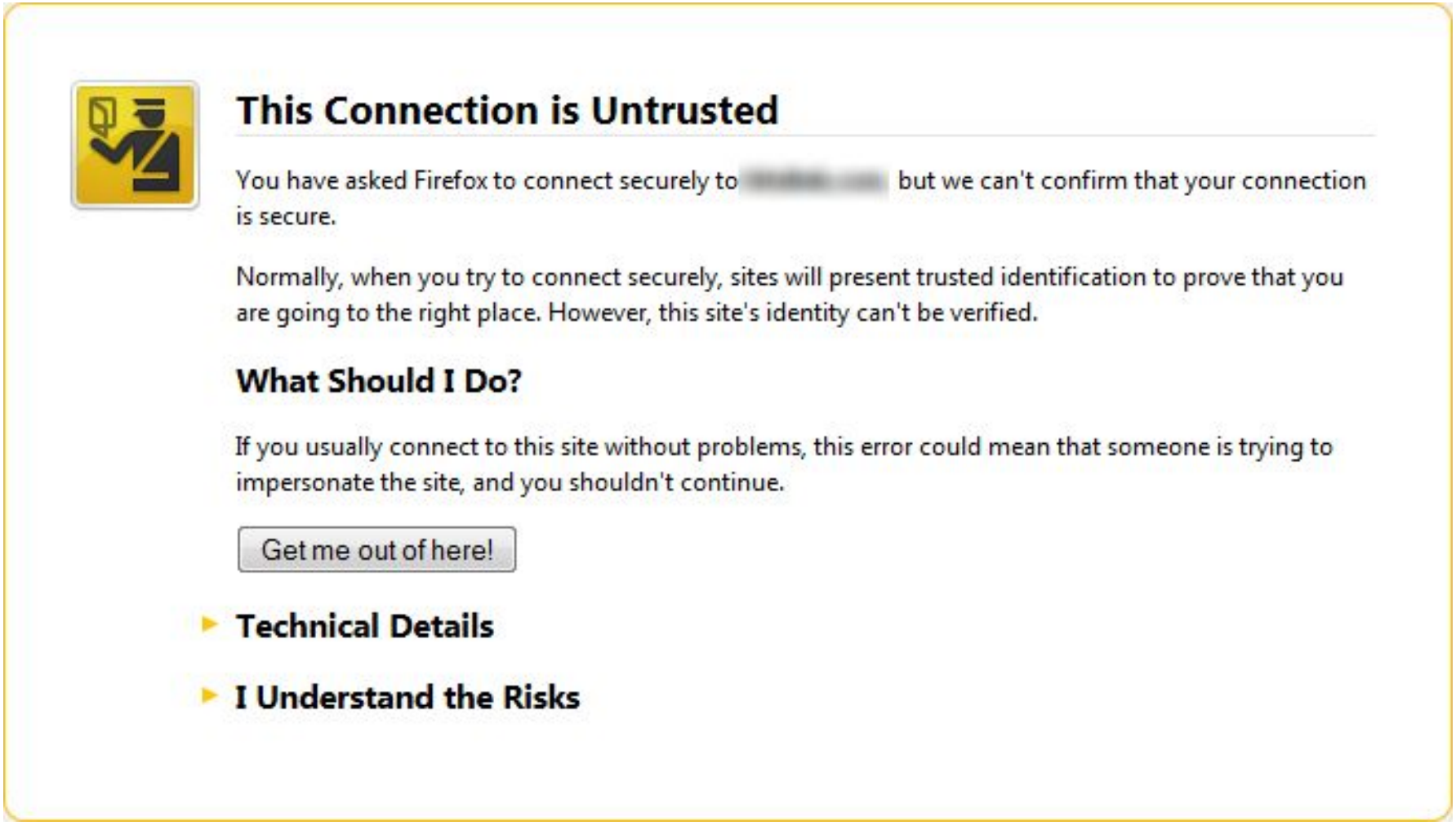
Quando um certificado digital é roubado ou quando não se deseja mais utilizá-lo é necessário uma **revocação de certificado** junto a uma autoridade de registro (AR). Após a revogação o certificado irá pertencer a lista de certificados revogados. A cada vez que um documento é assinado digitalmente o cliente realiza uma conexão na internet para verificar se o certificado da pessoa que está tentando assinar está presente nesta lista.

Sumário

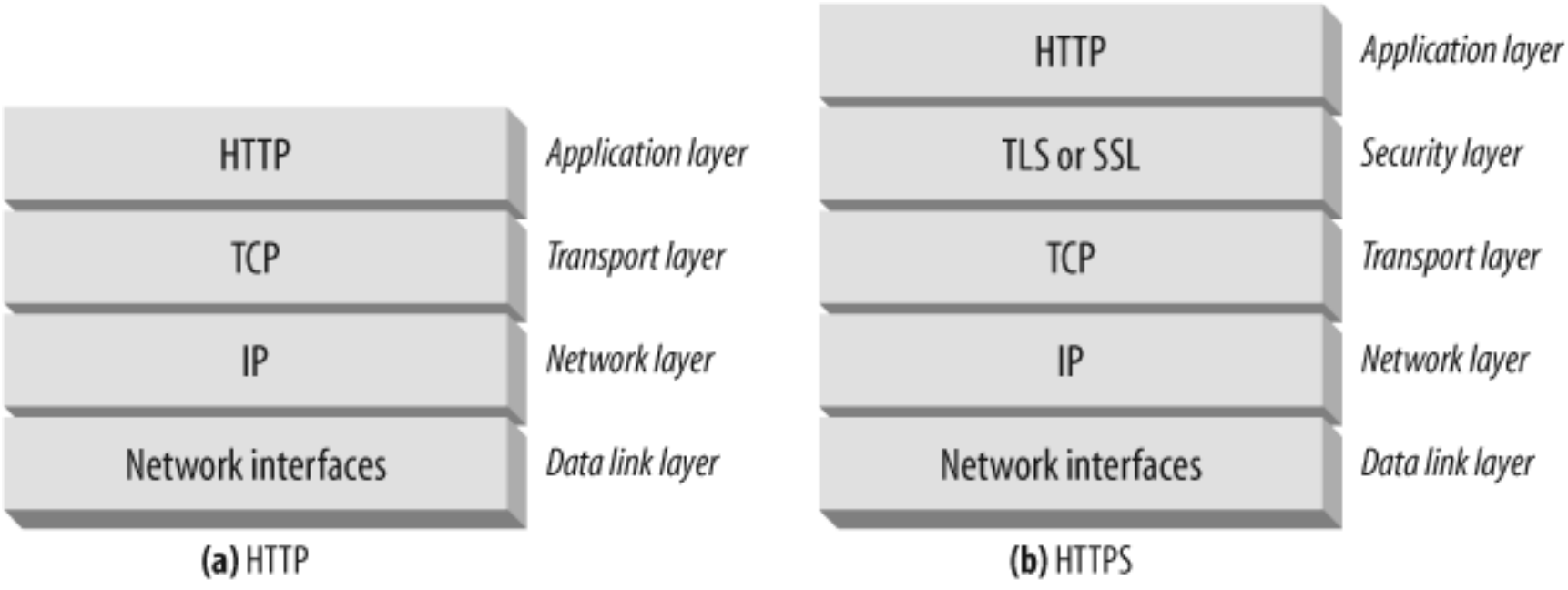
SSL

Quando você visita um website cujo endereço começa com https, é esperado que sua comunicação com este site seja cifrada. Antes de iniciar a comunicação cifrada, o website apresentará ao browser um certificado para se identificar. Se existir um problema com o certificado (se ele não existir, estiver fora da validade ou estiver revogado) uma página de alerta será exibida.

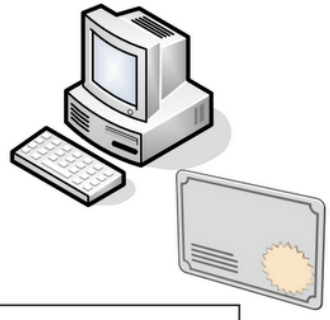
SSL


This Connection is Untrusted
You have asked Firefox to connect securely to [redacted] but we can't confirm that your connection is secure.
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.
What Should I Do?
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.
Get me out of here!
Technical Details
I Understand the Risks

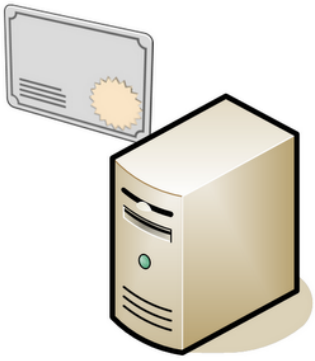
SSL


HTTP
TCP
IP
Network interfaces
Application layer
Transport layer
Network layer
Data link layer
(a) HTTP
HTTP
TLS or SSL
TCP
IP
Network interfaces
Application layer
Security layer
Transport layer
Network layer
Data link layer
(b) HTTPS

SSL



1) Client requests HTTPS session



2) Certificate sent back (with Public Key)

3) Client creates random session key

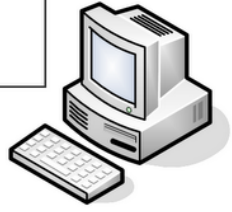
4) Session key encrypted with public key

At this point, only client knows session key

6) Session key decrypted with private key

At this point, both client and server know session key

5) Encrypted session key sent to server



7) Session encrypted with symmetric session key

Sumário

Outros algoritmos

Existem ainda outros algoritmos para assinaturas digitais:

- Elgamal Digital Signature;
- Digital Signature Algorithm (DSA): baseado no padrão Elgamal, padrão livre de patentes, só serve para assinaturas e não para criptografia (facilidade de exportação).
- Curvas elípticas (assinaturas pequenas).

Smart card

- a chave privada é gerada no módulo de criptografia que reside no cartão;
- uso de um PIN para acessar o cartão (bloqueio após n tentativas);
- a chave é altamente segura pois ela nunca "deixa" o cartão, o resumo criptográfico é enviado ao cartão para assinatura, e a assinatura é o retorno do cartão;
- o cartão permite mobilidade e pode ser acoplado a qualquer sistema.