

Criptografia de chaves públicas

Marcelo Augusto Rauh Schmitt
Maio de 2001

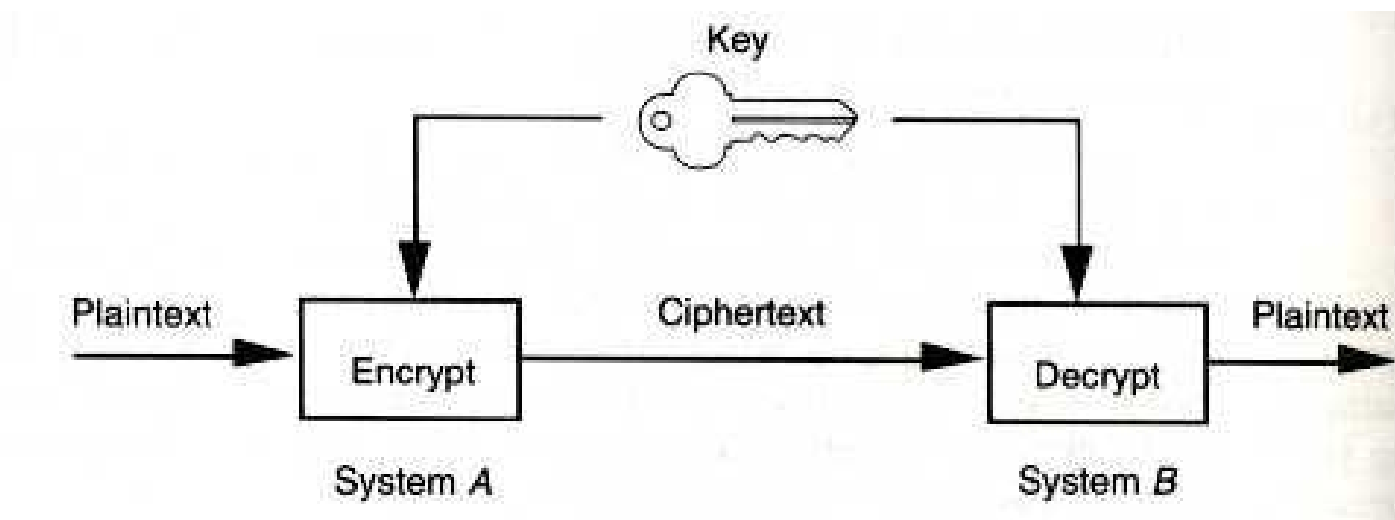
Introdução

- Conceito
 - É a transformação de um texto original em um texto ininteligível (texto cifrado), que pode ser restaurado.
- Funções principais
 - Confidencialidade
 - Autenticação
- Tipos
 - Simétrica
 - Assimétrica (sistemas de chave pública)

Criptografia simétrica

• Conceito

- A mesma chave criptografa e decriptografa

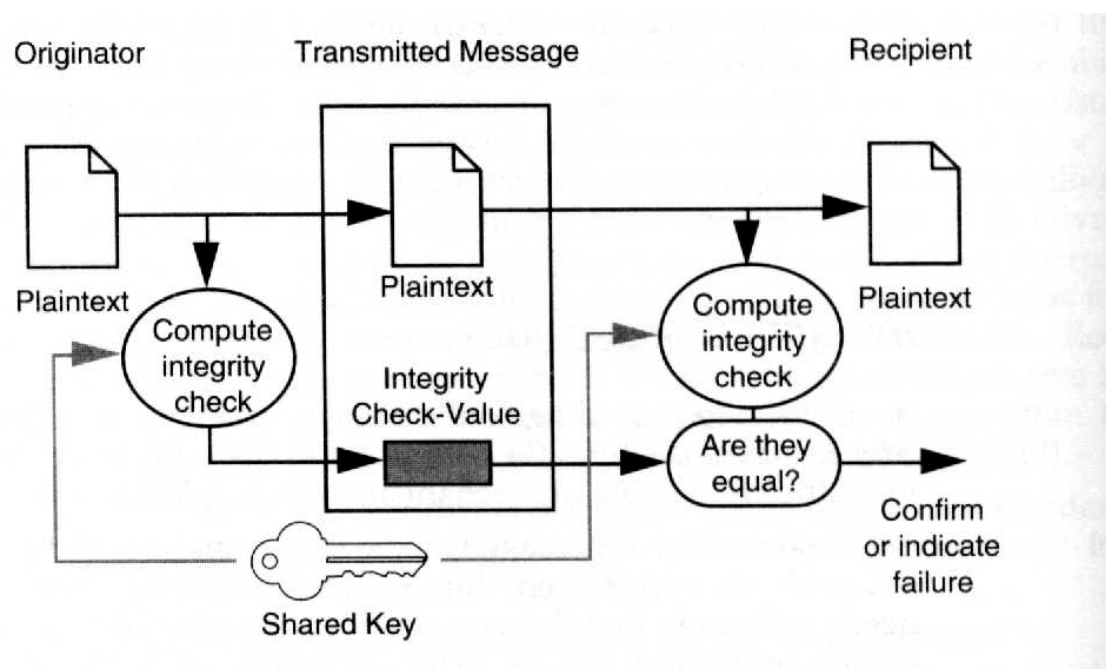


• Exemplos

- DES
- Triple DES
- IDEA
- RC2, RC4 e RC5 (RSA)

Criptografia simétrica

Autenticação



Problema: compartilhamento das chaves

Criptografia assimétrica

Criação

- Whitfield Diffie & Martin Hellman (Stanford University - 1976)

Funcionamento

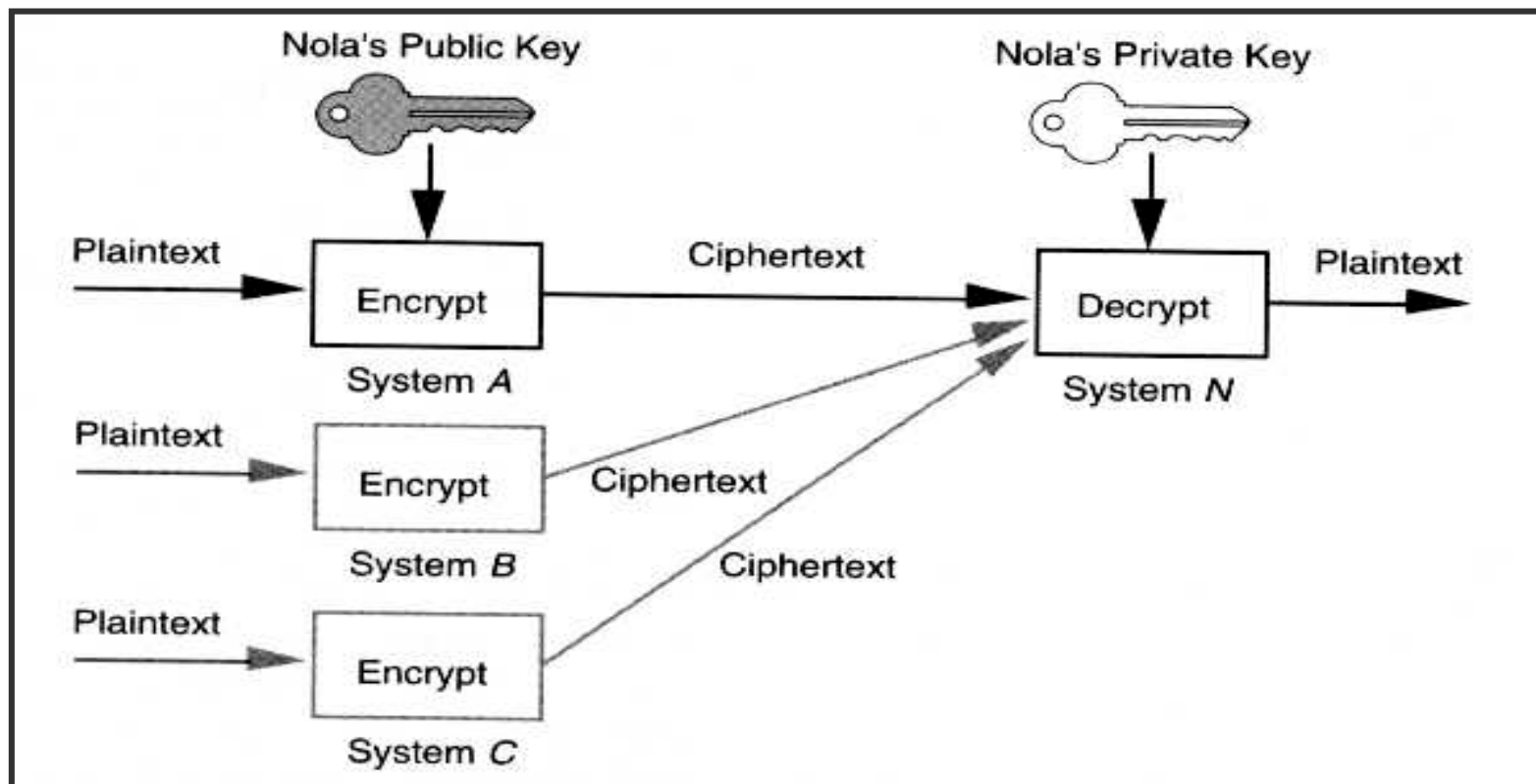
- Duas chaves
 - chave pública - publicada
 - chave privada - mantida em segredo
- É possível gerar a chave pública a partir do conhecimento da chave privada
- Não é possível gerar a chave privada a partir do conhecimento da chave pública
 - A dificuldade de quebra está no tempo necessário para determinar a chave privada a partir da chave pública
- O texto criptografado por uma é decriptografado pela outra.

Criptografia assimétrica

• Algoritmos

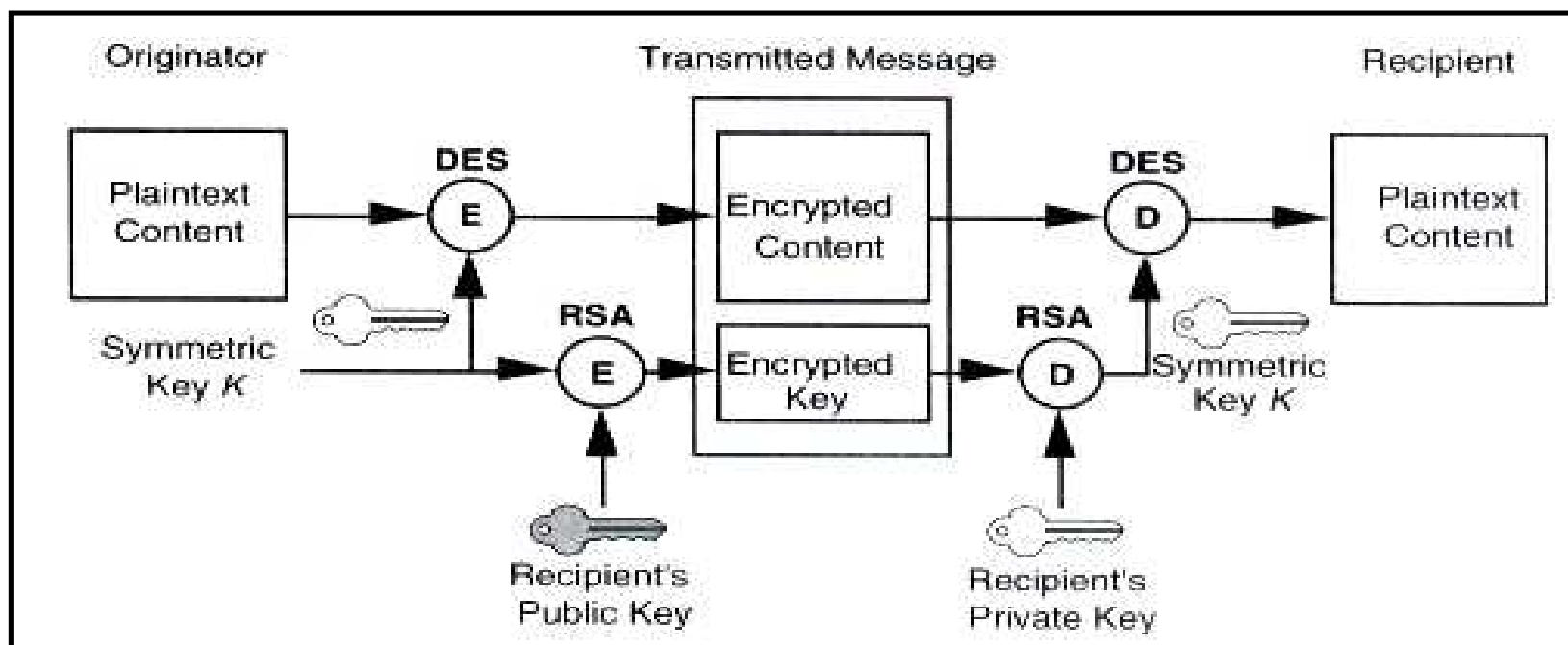
- RSA (Ron Rivest, Adi Shamir e Len Adleman - MIT)
 - Módulo público - parte da chave pública.
 - Obtido a partir de 2 números primos que fazem parte da chave privada.
 - Dificuldade de fatorar o produto. Aumentando em 3 dígitos dobra a dificuldade de fatoração.
 - 1024 bits é considerado um bom número para os próximos anos.
- DSA (Digital Signature Algorithm)
- Diffie-Hellman

Confidencialidade



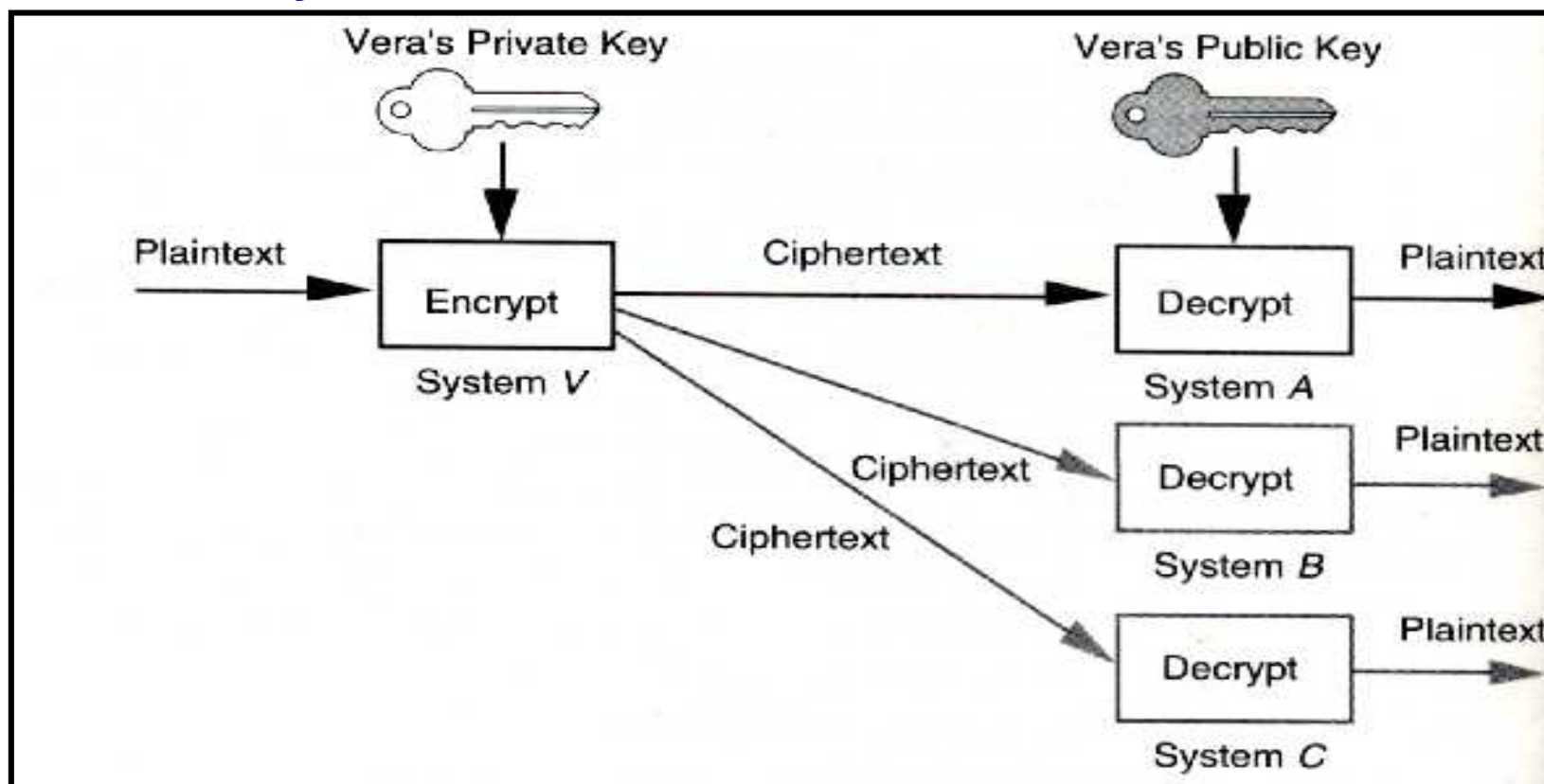
Problema: custo de processamento

Confidencialidade



Primeiro o texto é criptografado com um algoritmo simétrico; após a chave simétrica é criptografada com a chave pública do destinatário.

Autenticação



Autenticação

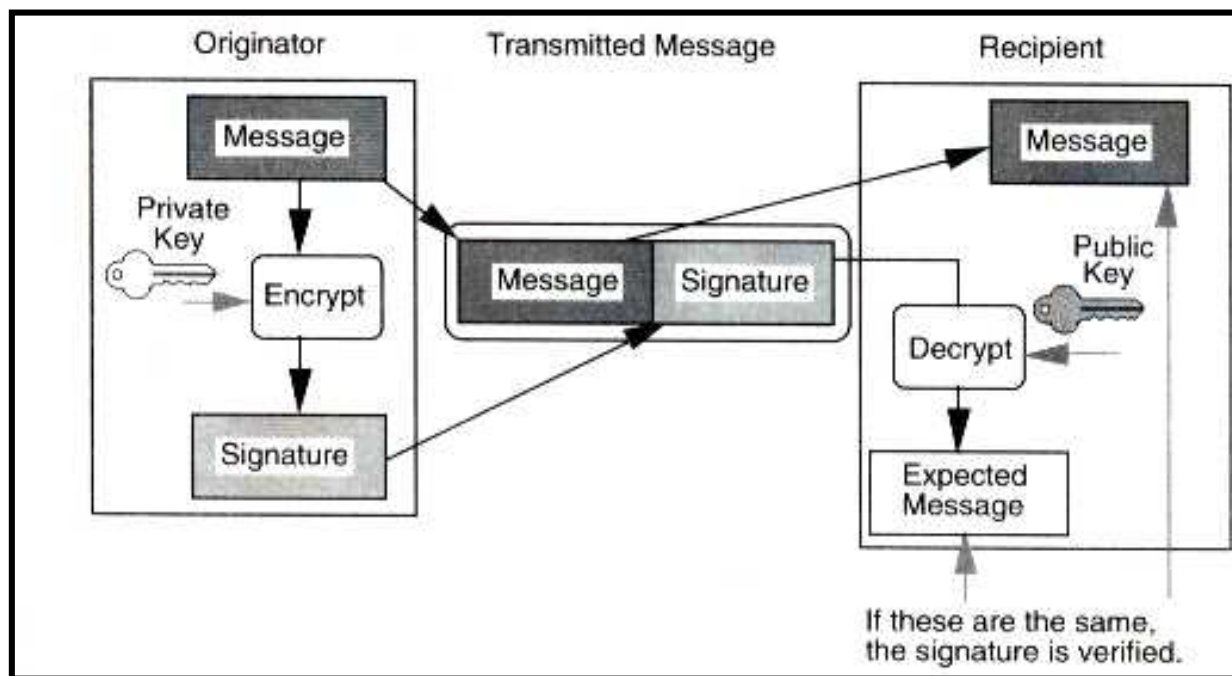
Assinatura digital

Uma assinatura digital é um item que acompanha um determinado dado e que tem duas funções:

- confirmar a origem do dado;
- certificar que o dado não foi modificado;
- impedir a negação de origem.

Autenticação

Assinatura digital



Problemas

- custo de processamento
- custo de comunicação

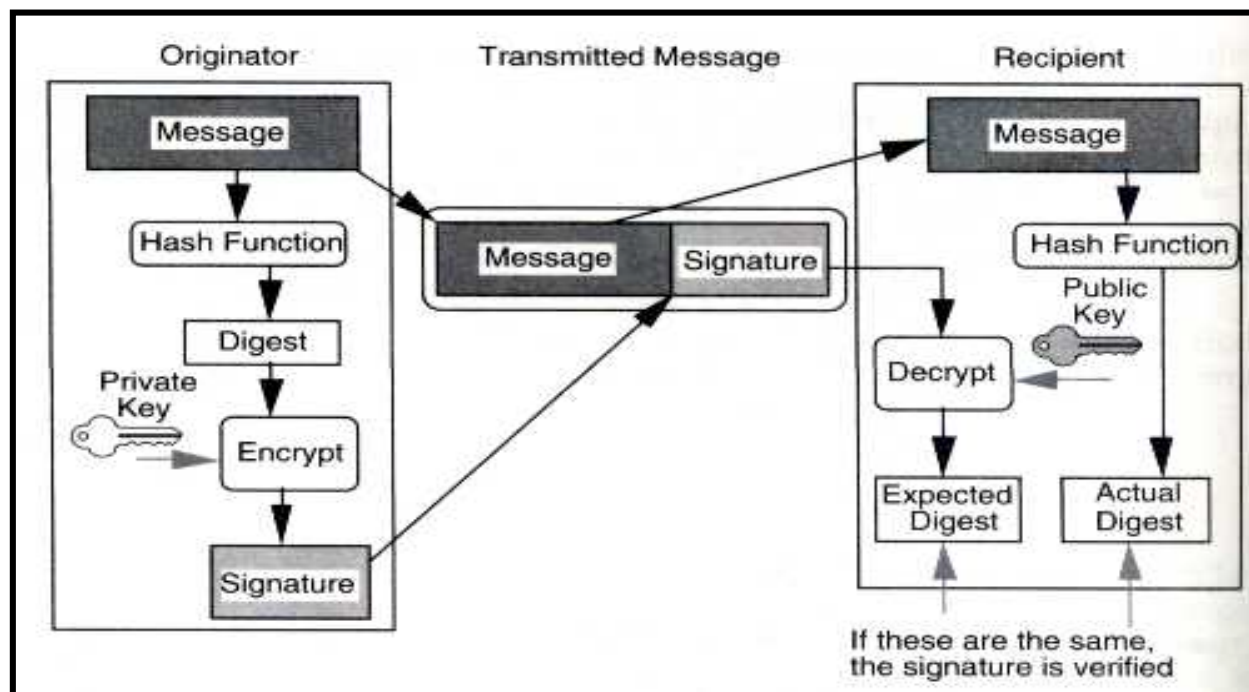
Autenticação

Hash function

- Conceito
 - “Função que tem apenas um sentido e que mapeia valores de um grande domínio em um pequeno domínio.” (FORD & BAUM)
 - Uma modificação mínima na entrada causará a geração de uma saída diferente (impossível construir duas mensagens que gerem a mesma saída).
 - Fácil de computar mas difícil de reverter (sentido único)
- O resultado da função é conhecido como “*message digest*”.
- Algoritmos
 - SHA-1 (saída de 160 bits)
 - MD5

Autenticação

Hash function



- É gerado o MD.
- O MD é criptografado com a chave privada do originador.

Correio eletrônico

✉ Utilização

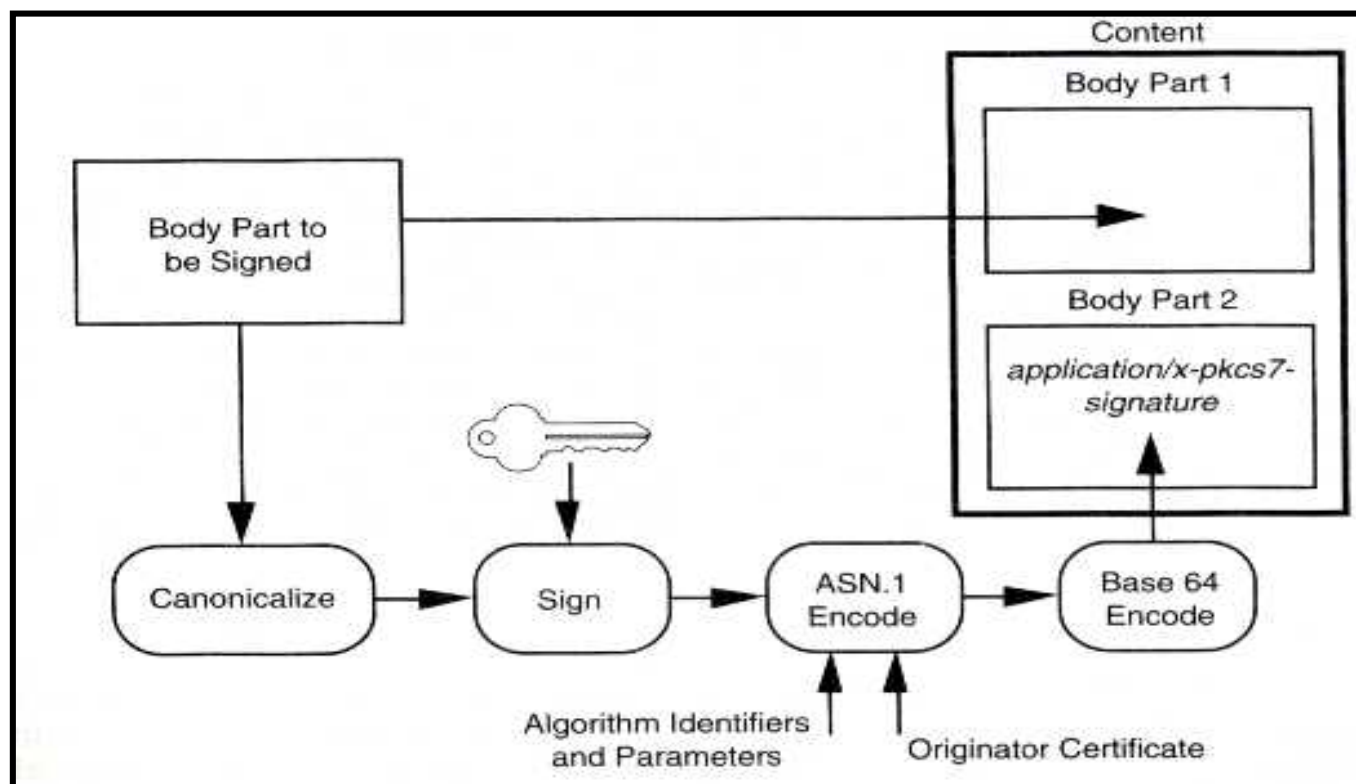
- Autenticação de origem
- Integridade do conteúdo
- Confidencialidade
- Não repudição

✉ Protocolos

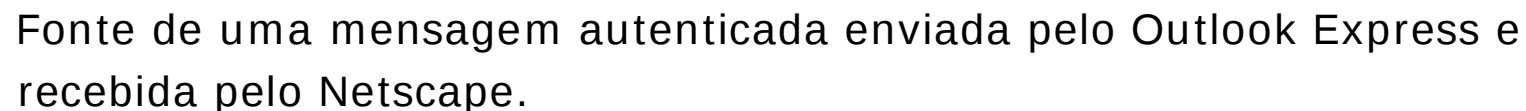
- PEM (Public Enhanced Mail)
- Security Multiparts for MIME/MOSS
- S/ MIME(colocar figura e exemplo 161)
- PGP
- X.400

Correio eletrônico

Autenticação / SMIME

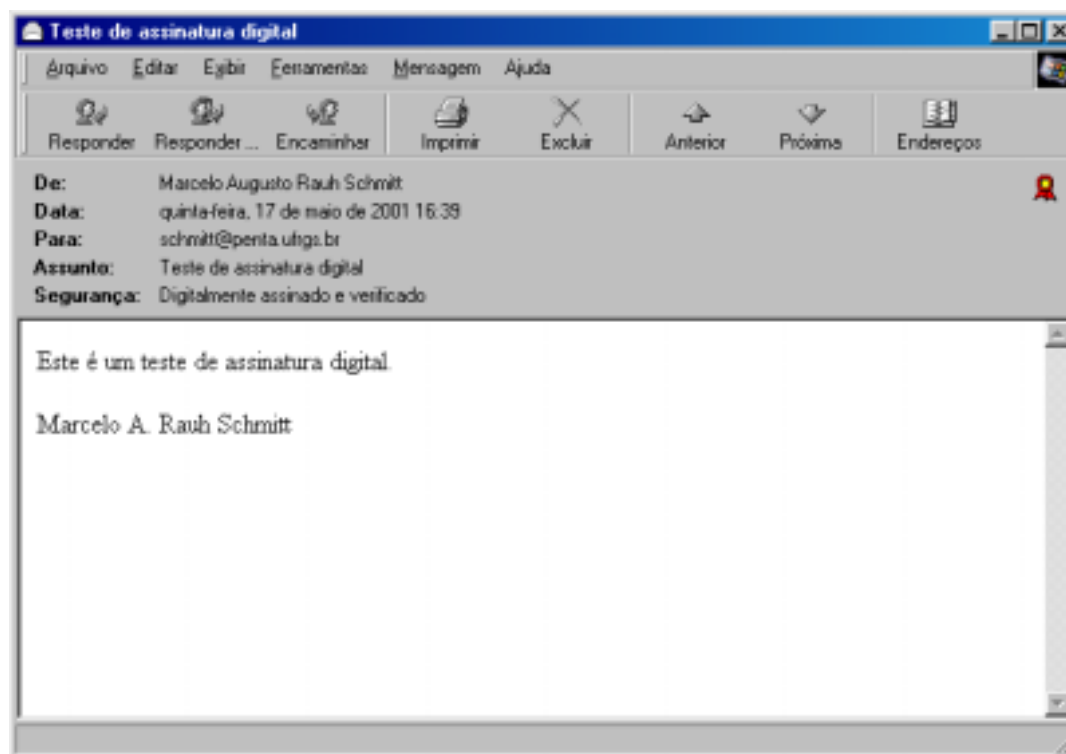


Autenticação / SMIME



Correio eletrônico

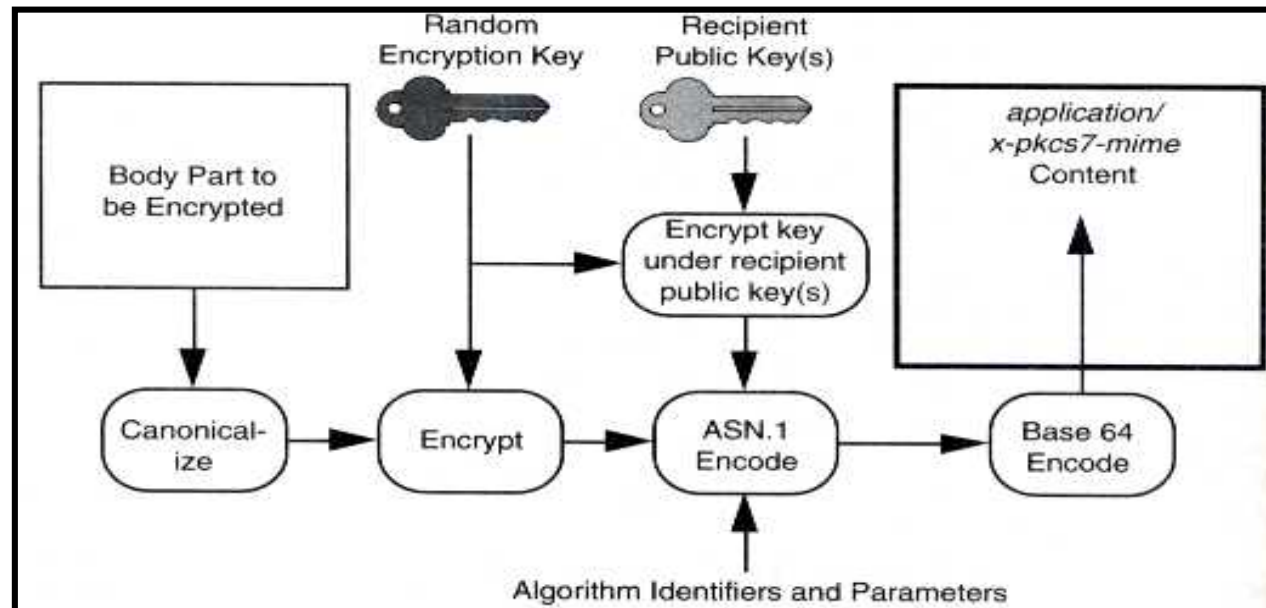
Autenticação / SMIME



Forma como a mensagem anterior aparece no Outlook Express.

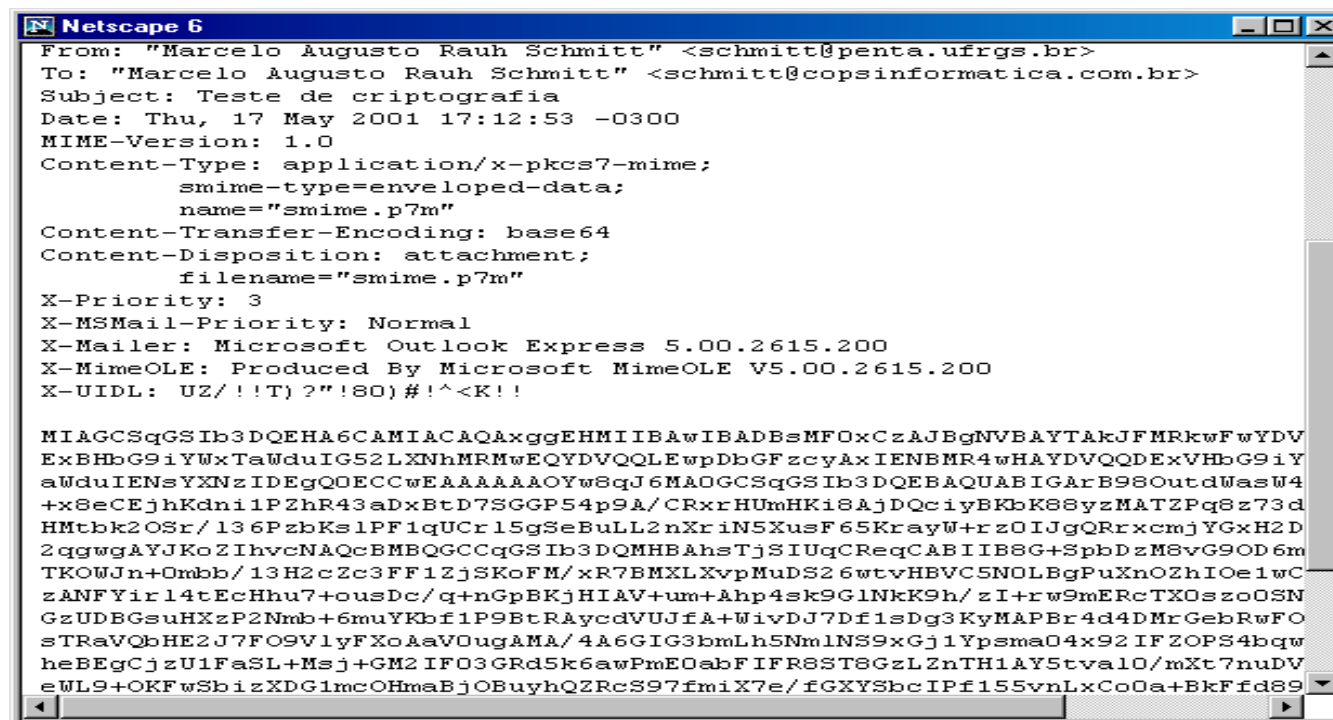
Correio eletrônico

Criptografia / SMIME



Correio eletrônico

Criptografia / SMIME



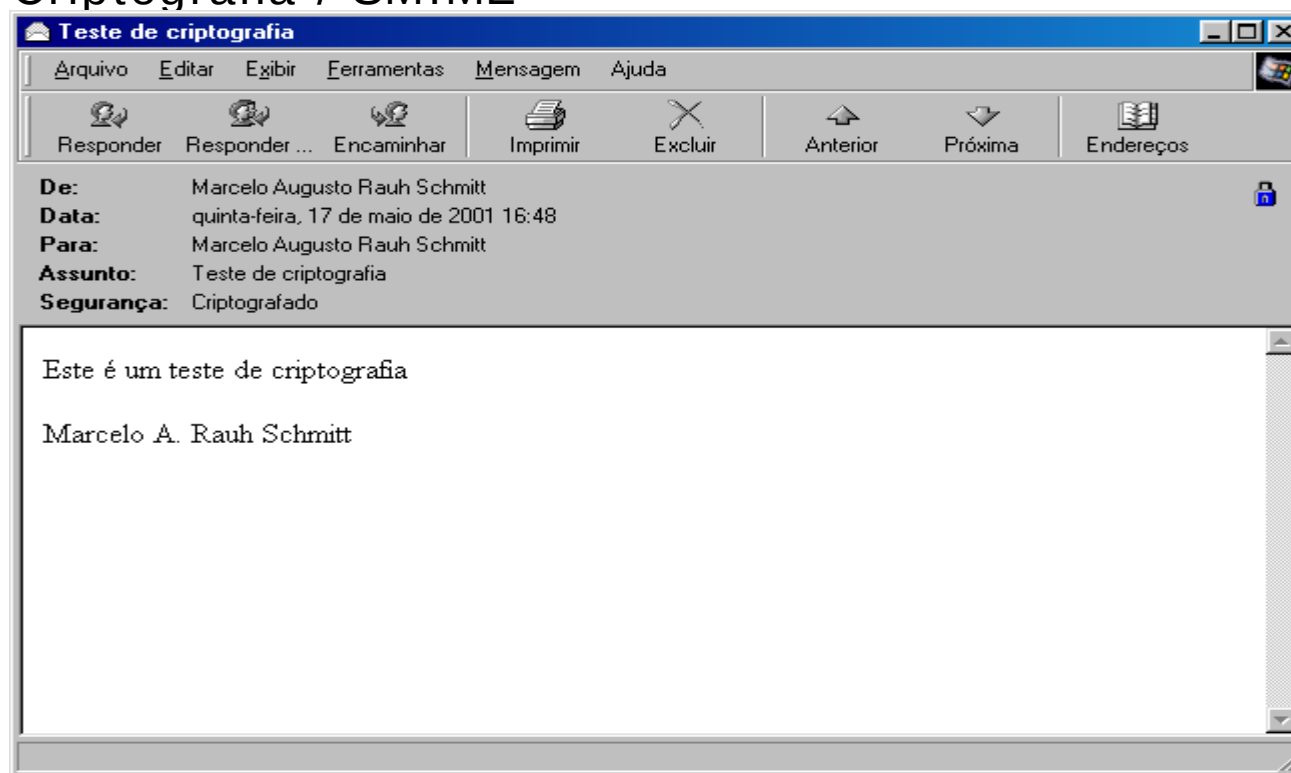
```
From: "Marcelo Augusto Rauh Schmitt" <schmitt@penta.ufrgs.br>
To: "Marcelo Augusto Rauh Schmitt" <schmitt@copsinformatica.com.br>
Subject: Teste de criptografia
Date: Thu, 17 May 2001 17:12:53 -0300
MIME-Version: 1.0
Content-Type: application/x-pkcs7-mime;
    smime-type=enveloped-data;
    name="smime.p7m"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
    filename="smime.p7m"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.00.2615.200
X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2615.200
X-UIDL: UZ/!!T) ?"!80)#!^<K!!

MIAGCSqGSib3DQEHA6CAMIACAQAQxggEHMIIBAwIBADBsmFOxCzAJBgNVBAYTAkFMRkwFwYDV
ExBHBG9iYWxTaWduIG52LXNhMRMwEQYDVQLEwPDbGFzcyAxIENBMR4wHAYDVQQDExVHbG9iY
aWduIENsYXNzIDBgQOECCwEAAAAAAOYw8qJ6MAOGCSqGSib3DQEBAQUABIGArB98OutdWasW4
+x8eCEjhKdni1PZhR43aDxBtD7SGGP54p9A/CRxrHUmHKi8AjDQciyBKbK88yzMATZPq8z73d
HMtbk2OSr/136PzbKs1PF1qUCr15gSeBuLL2nXriNSXusF65KrayW+rzoIJgQRrxcmjYGxH2D
2qgwgAYJKoZIhvcNAQcBMBQGCCqGSib3DQMHBAAhsTjSIUqCReqCABIIB8G+SpbDzM8vG9OD6m
TKOWJn+Ombb/13H2cZc3FF1ZjSKoFM/xR7BMXLXvpMuDS26wtvHBVC5NOLBgPuXnoZhIOe1wC
zANFYir14tEcHhu7+ousDc/q+nGpBKjHIAV+um+Ahp4sk9G1NkK9h/zI+rw9mERcTXOszoOSN
GzUDBGsuHXzP2Nmb+6muYKbf1P9BtR&ycdVUJfA+WivDJ7Df1sDg3KyMAPBr4d4DMrGebRwFO
sTRaVQbHE2J7FO9VlyFXoAaVOugAMA/4A6GIG3bmLh5Nm1NS9xGj1Ypsma04x92IFZOPS4bqw
heBEgCjzU1FaSL+Msj+GM2IF03GRd5k6awPmEOabFIFR8ST8GzLZnTH1AY5tvalO/mXt7nuDV
eWL9+OKFwSbizXDG1mcOHmaBjOBuyhQZRCs97fmiX7e/fGXYSbcIPf155vnLxCo0a+BkFfd89
```

Fonte de uma mensagem criptografada enviada pelo Outlook Express e recebida pelo Netscape.

Correio eletrônico

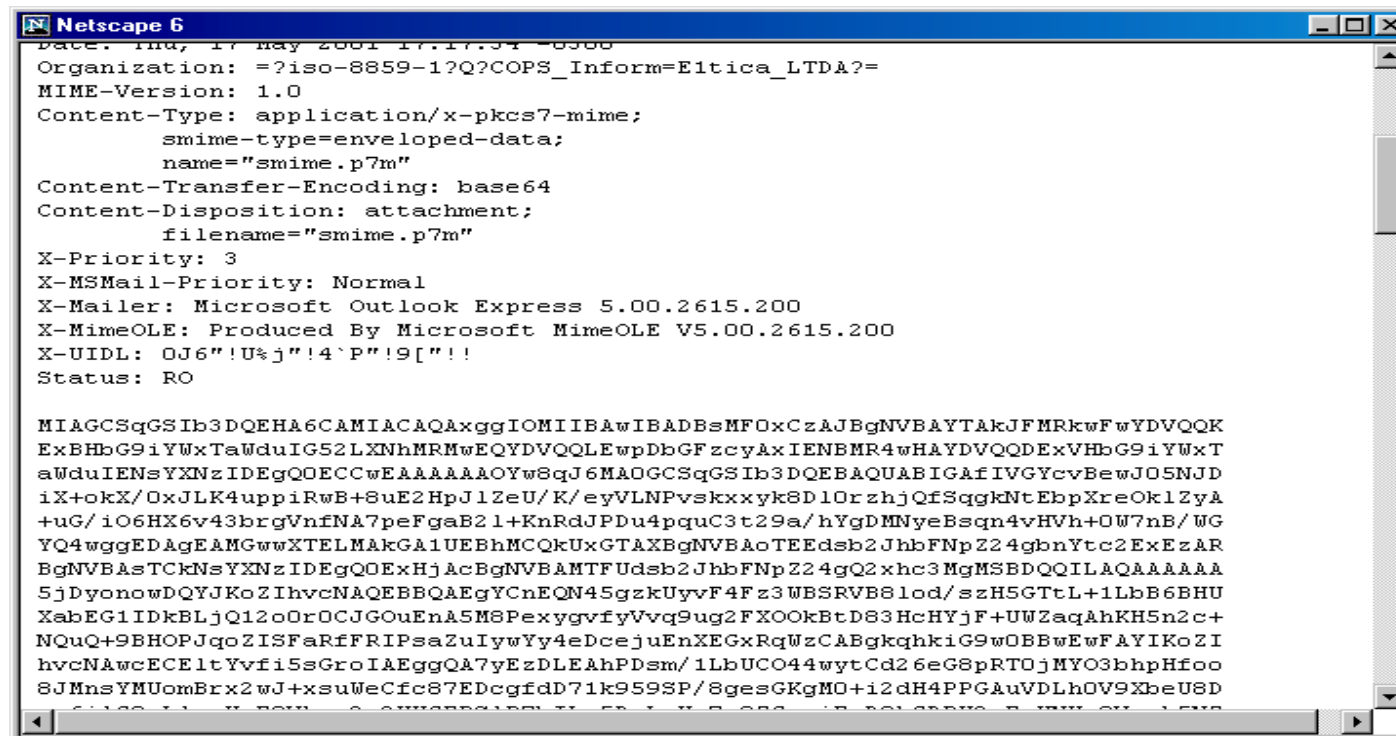
Criptografia / SMIME



Forma como a mensagem anterior aparece no Outlook Express.

Correio eletrônico

Autenticação e Criptografia / SMIME



```

Date: Thu, 17 May 2001 17:17:34 -0300
Organization: =?iso-8859-1?Q?COPS_Inform=Eitica_LTDA?=
MIME-Version: 1.0
Content-Type: application/x-pkcs7-mime;
    smime-type=enveloped-data;
    name="smime.p7m"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
    filename="smime.p7m"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.00.2615.200
X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2615.200
X-UIDL: OJ6"!U%j"!4`P"!9["!!
Status: RO

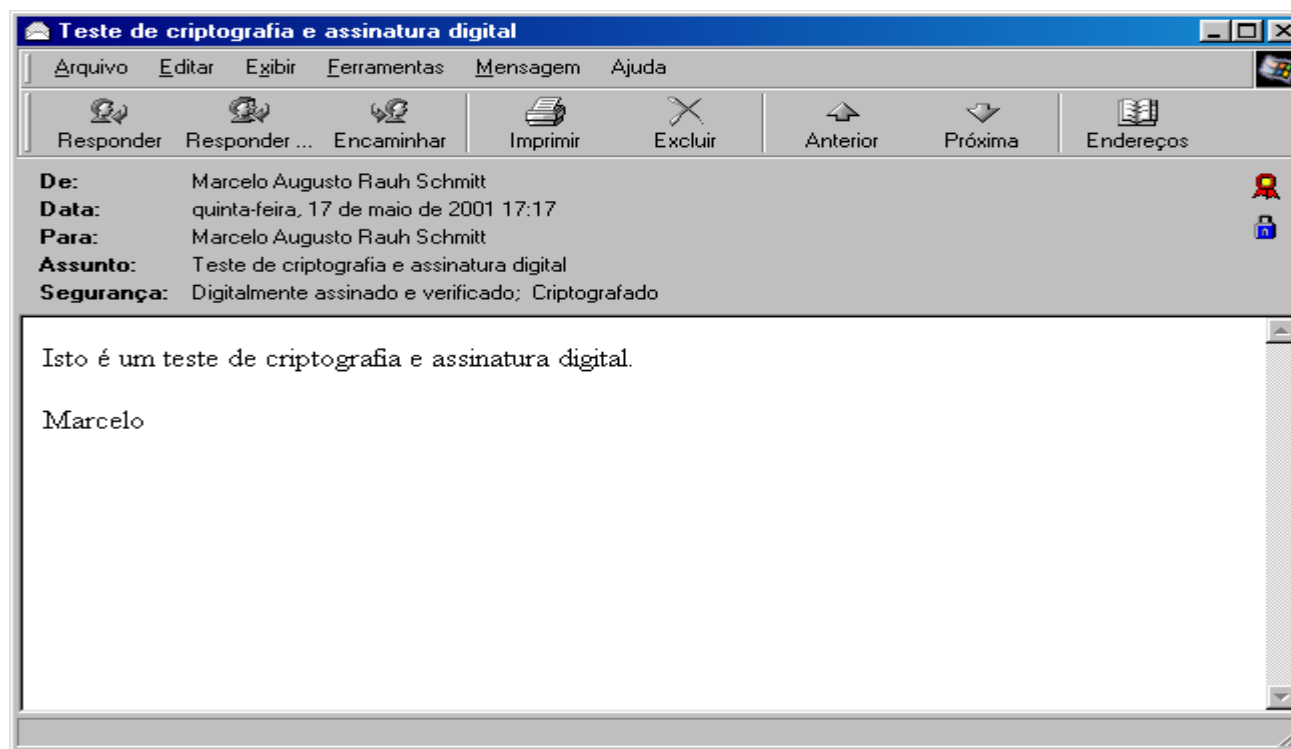
MIAGCSqGSIB3DQEHA6CAMIACAQAQxggIOMIIBAwIBADBAMF0xCzAJBgNVBAYTAkJKFMRkwFwYDVQQK
ExBHBG9iYWxTaWduIG52LXNhMRMwEQYDVQLEWpDbGFzcyAxIENBMR4wHAYDVQQDEExVHbG9iYWxT
aWduIENSYXNzIDEGQOECCwEAAAAAAOYw8qJ6MAOGCSqGSIB3DQEBAQUABIGAfIVGYcvBewJ05NJD
iX+okX/OxJLK4uppiRwB+8uE2HpJ1ZeU/K/eyVLNPvskxxk8D1OrzhjQfSgqkNtEbpXreOk1ZyA
+uG/iO6HX6v43brgVnfNA7peFgaB21+KnRdJPdu4pquC3t29a/hYgDMNyeBsqn4vHVh+OW7nB/WG
YQ4wggEDAgEAMGwwXTELMakGA1UEBhMCQkUxGTAXBgNVBAoTEEdsb2JhbFNpZ24gbnYtc2ExEzAR
BgNVBAsTCkNsYXNzIDEGQOEExHjAcBgNVBAMTFUdsb2JhbFNpZ24gQ2xhc3MgMSBDQQILAQAAAAAA
5jDyonowDQYJKoZIhvcNAQEBBQAEgYCnEQN45gzKuyvF4Fz3WBSRVB8lod/szH5GTtL+1LbB6BHU
XabEG1IDkBLjQ12o0rOCJGOuEnA5M8PexygvfyVvq9ug2FXOOkBtD83HcHYjF+UW2aqAhKH5n2c+
NQwQ+9BHOPJqoZISFaRfFRIPsaZuIywYy4eDcejuEnXEGxRqWzCABgkqhkiG9w0BBwEwFAYIKoZI
hvcNAweCE1tYvfi5sGroIAEggQA7yEzDLEAhPdsm/1LbUCO44wytCd26eG8pRTOjMYO3bhpHfoo
8JMnsYMUomBrx2wJ+xsuWeCfc87EDcgfdD71k959SP/8gesGKgMO+i2dH4PPGAuVDLhOV9XbeU8D

```

Fonte de uma mensagem criptografada e autenticada enviada pelo Outlook Express e recebida pelo Netscape.

Correio eletrônico

Autenticação e Criptografia / SMIME



Forma como a mensagem anterior aparece no Outlook Express.

WEB

Resumo

- Requisitos
 - Autenticação do servidor
 - Autenticação do cliente
 - Integridade de conteúdo
 - Confidencialidade
- Protocolos
 - SSL (Secure Socket Layer)
 - Secure HTTP

Outras aplicações

- SSH
- IPSec
- VPNs
- EDI

- Proteção da chave privada
 - Guardar em um hardware removível, como smartcard ou cartão PCMCIA.
 - Guardar criptografada.

Justificativa

• Usuário de chaves públicas

- Originador de uma mensagem criptografada
 - Precisa conhecer a chave pública do destinatário.
- Destinatário de uma mensagem autenticada
 - Precisa conhecer a chave pública do originador.

É necessário que o usuário tenha certeza de que a chave pública que está utilizando é autêntica.

- Pequeno grupo - poderia trocar as chaves públicas e guardá-las de forma segura.
- Grande grupo - troca manual de chaves impraticável.
- Solução: Certificados de Chave Pública.

Funcionamento

• Autoridade Certificadora

Entidade que emite certificados para possuidores de chaves públicas e privadas (pessoa, dispositivo, servidor).

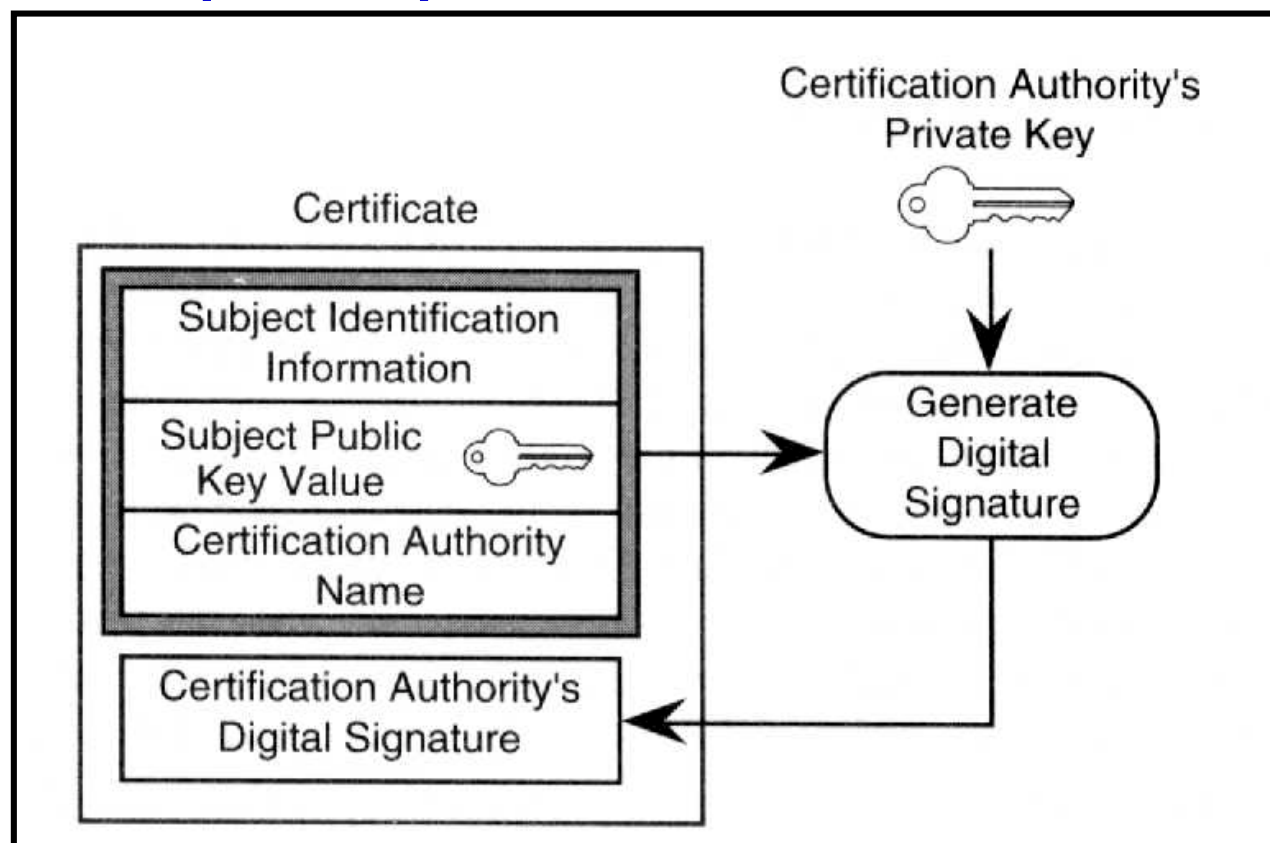
• Conteúdo do certificado

- chave pública;
- informação que identifica univocamente o sujeito do certificado;
- assinatura da autoridade certificadora.

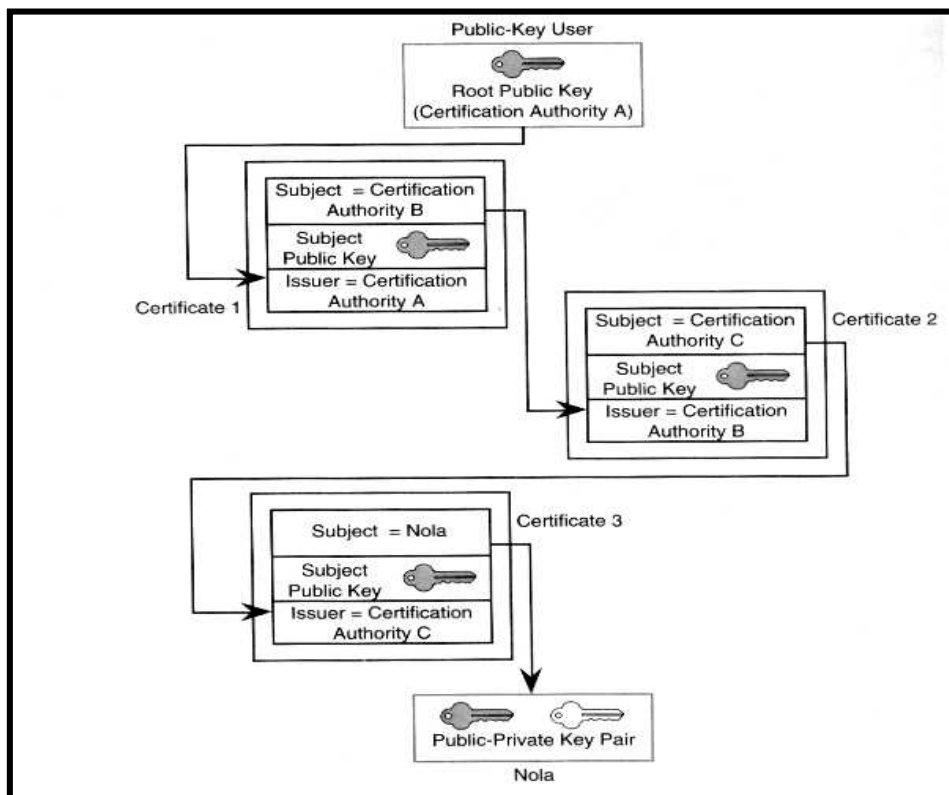
• Apenas a chave pública da Autoridade Certificadora precisa ser obtida de forma segura!

- O usuário confia na Autoridade Certificadora.
- A Autoridade Certificadora deve determinar a identidade do sujeito.

Exemplo simplificado



Cadeia de certificados (caminho)



A chave pública do usuário é autenticada pela Autoridade Certificadora C, cuja chave pública é autenticada pela Autoridade Certificadora B, cuja chave pública é autenticada pela Autoridade Certificadora A.

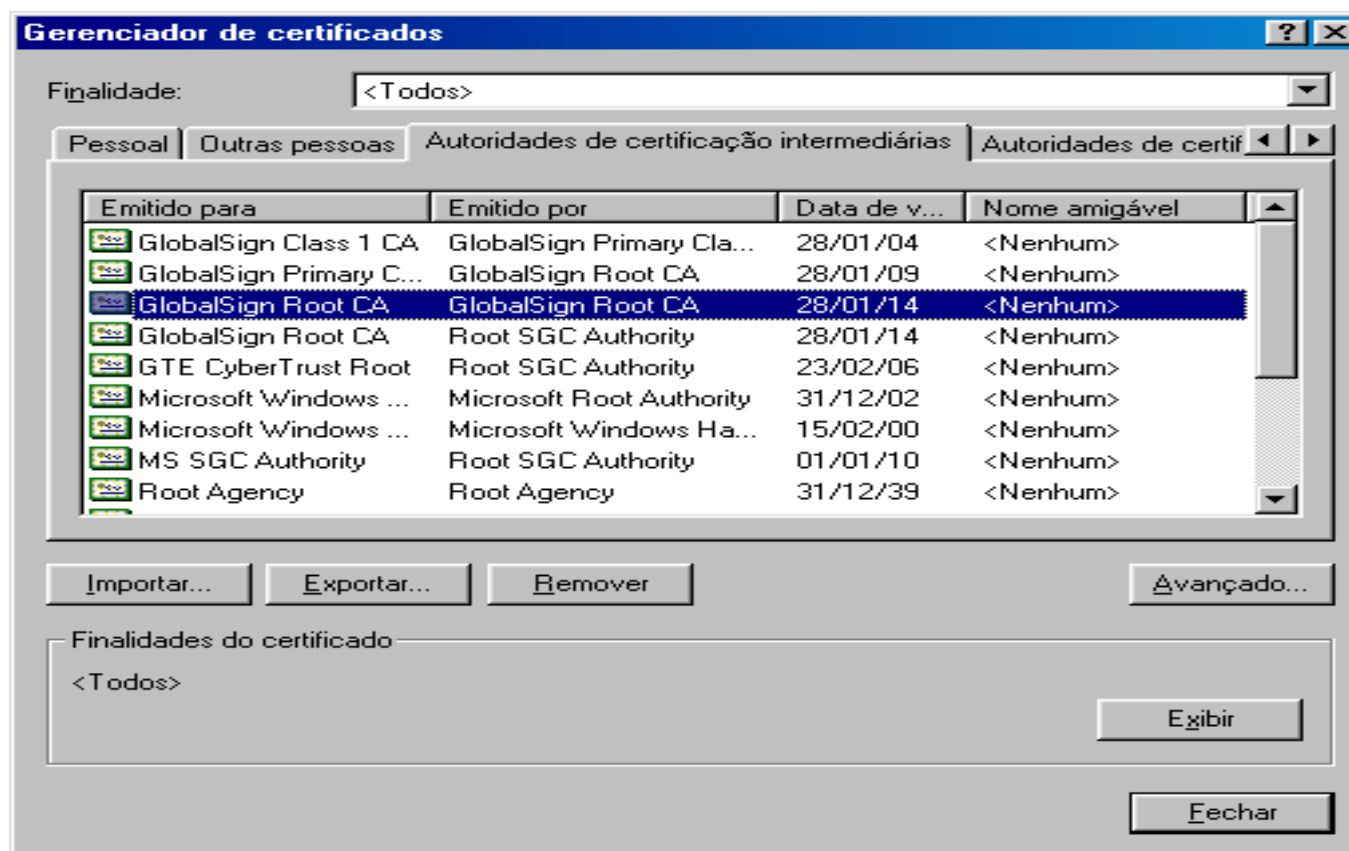
Período de validade e revogação

Chaves públicas não são válidas indefinidamente

- Os certificados definem períodos de validade para as chaves públicas.
- Certificados podem ser revogados antes de sua expiração:
 - Suspeita de corrupção da chave privada.
 - Término de contrato.
 - Mudança de nome.

Exemplo

Certificado de um CA

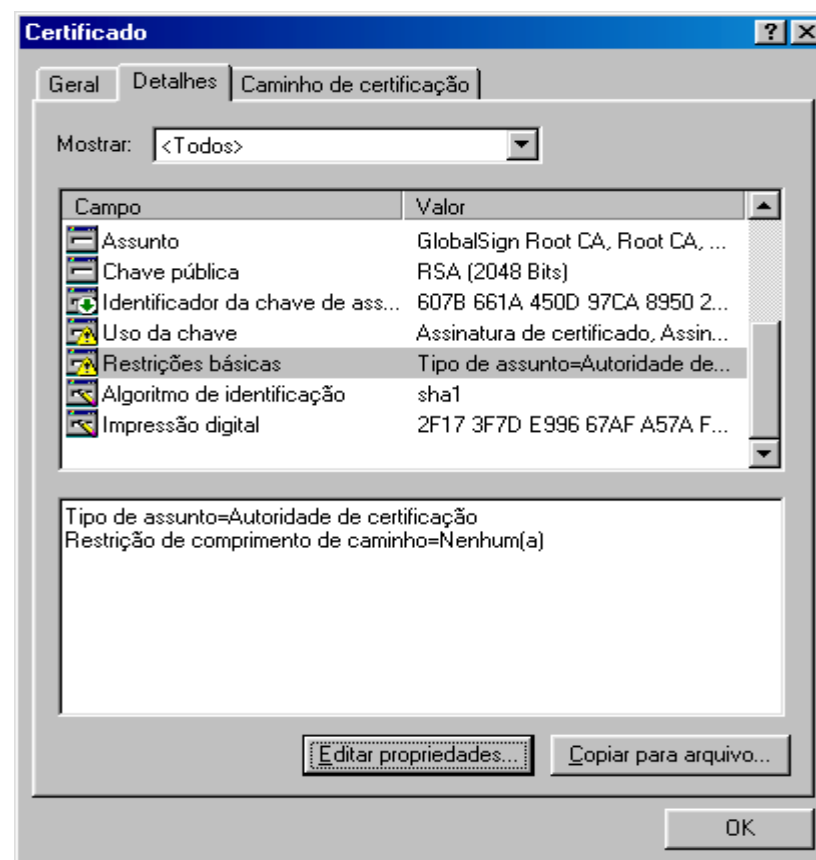
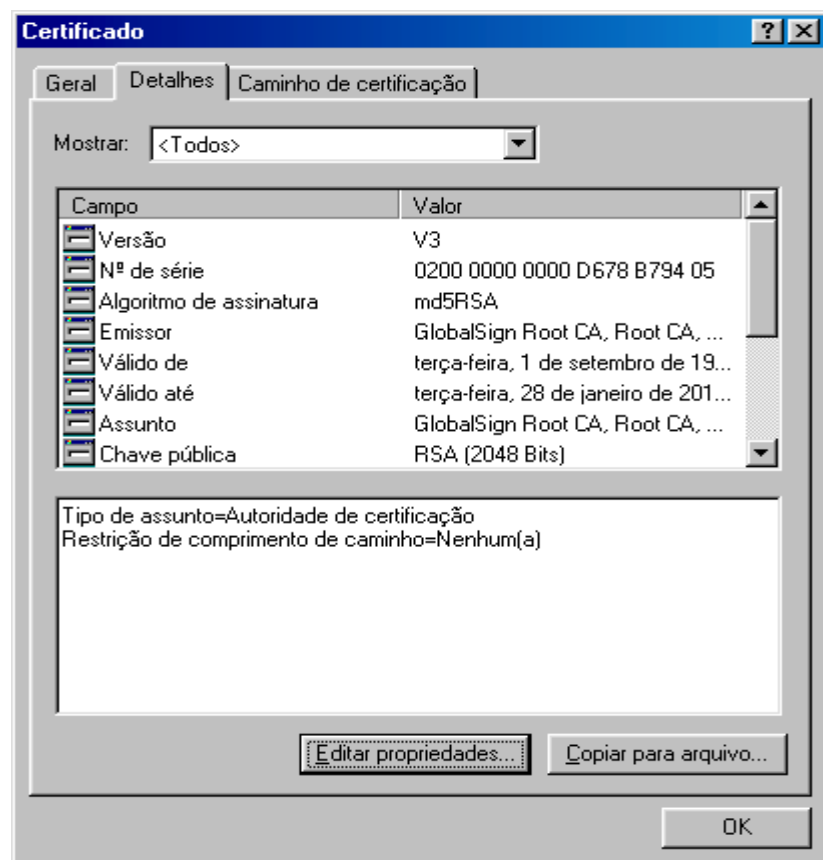


Certificados



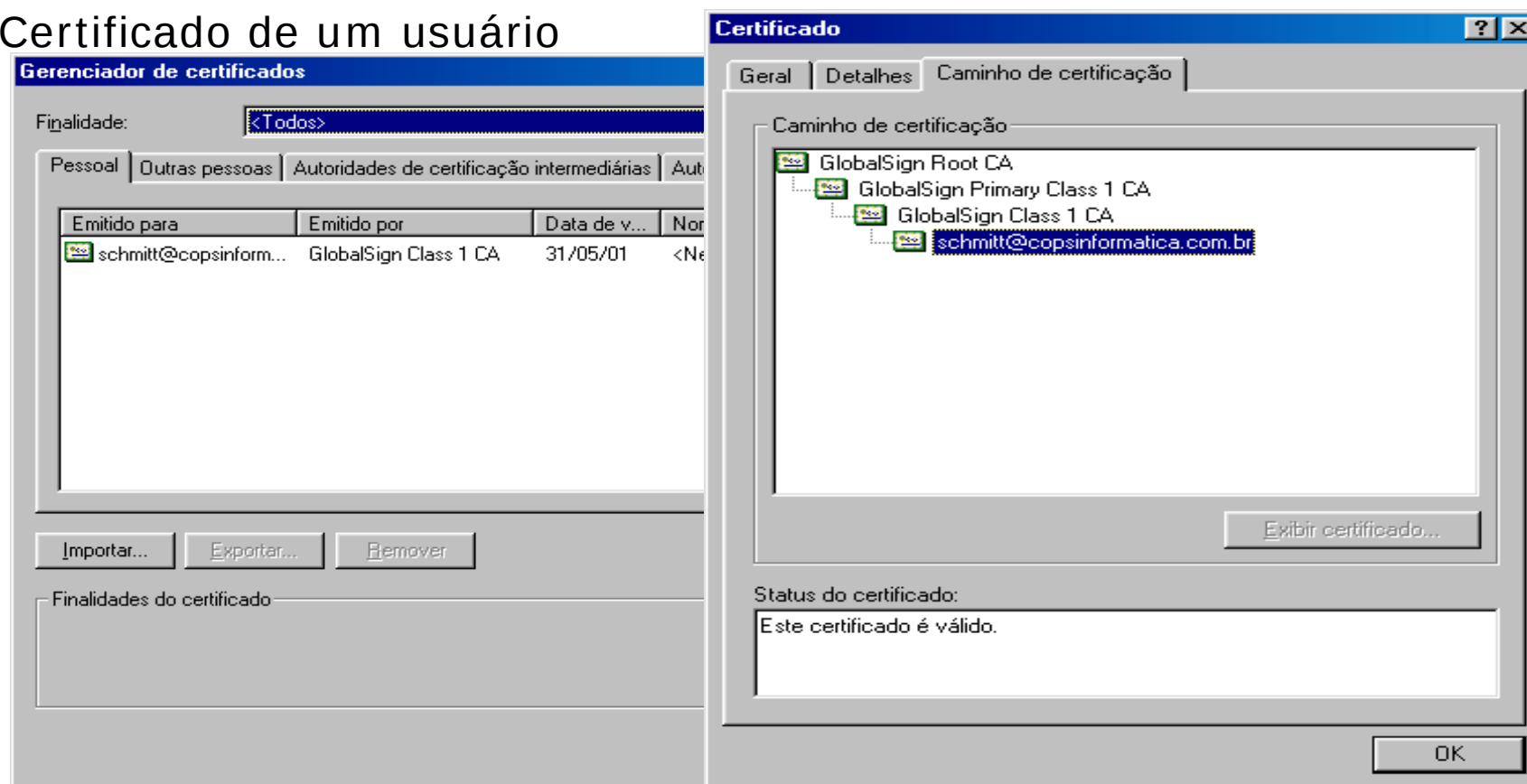
Exemplo

Certificado de um CA



Exemplo

Certificado de um usuário

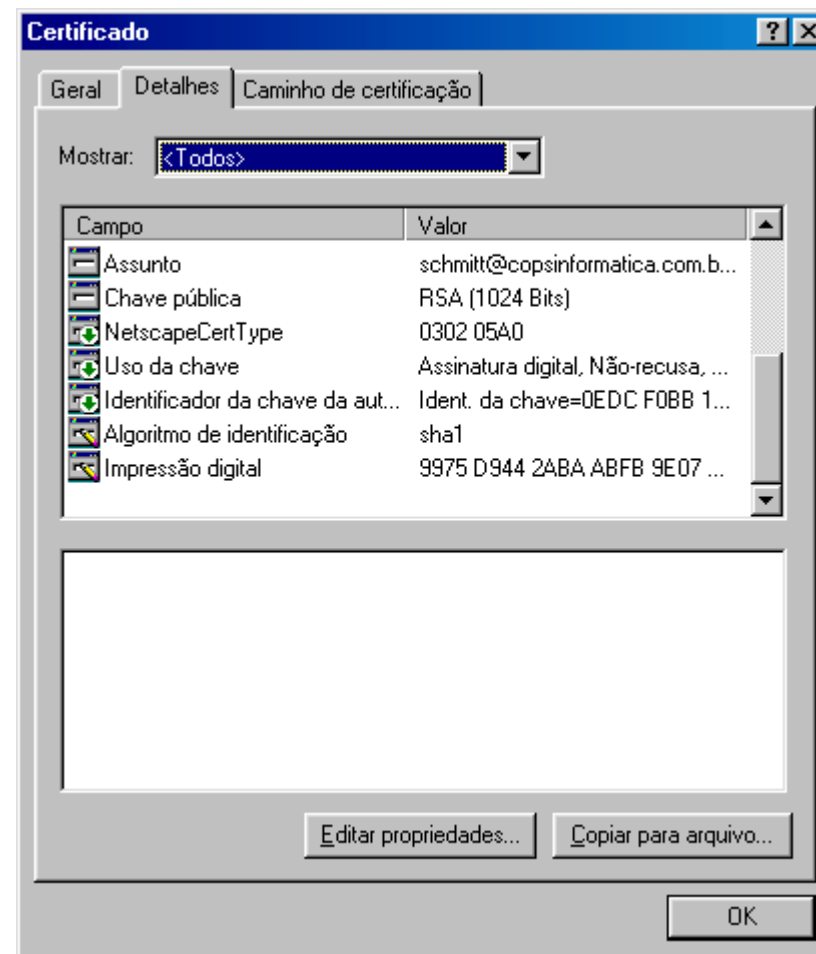
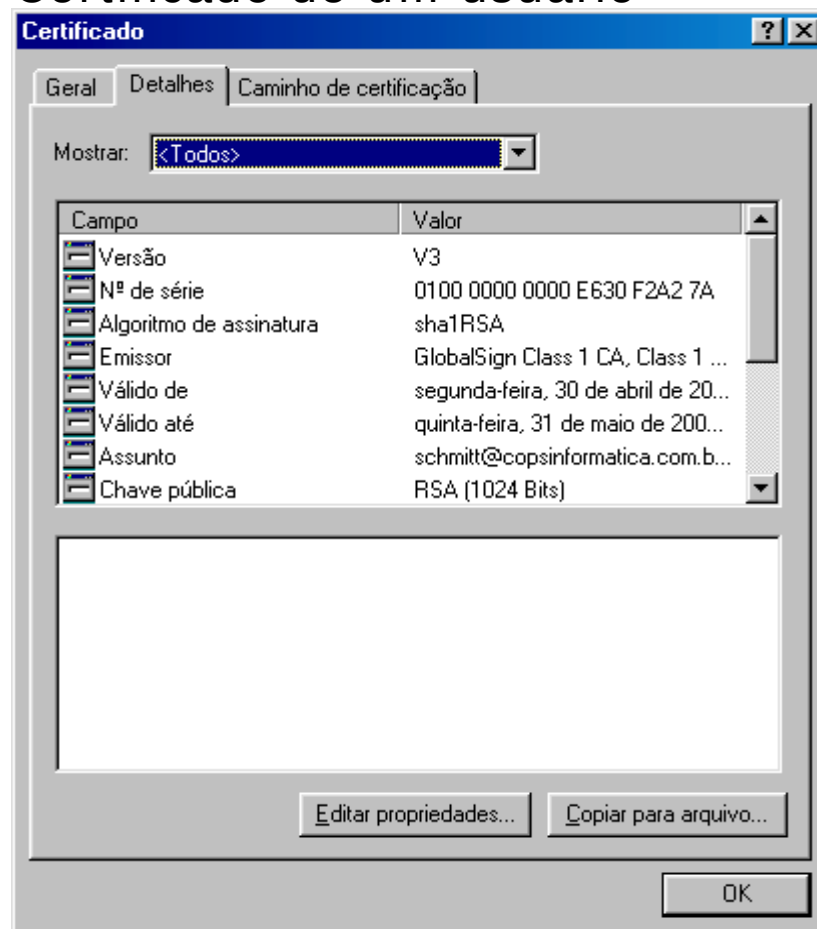


Certificados



Exemplo

Certificado de um usuário

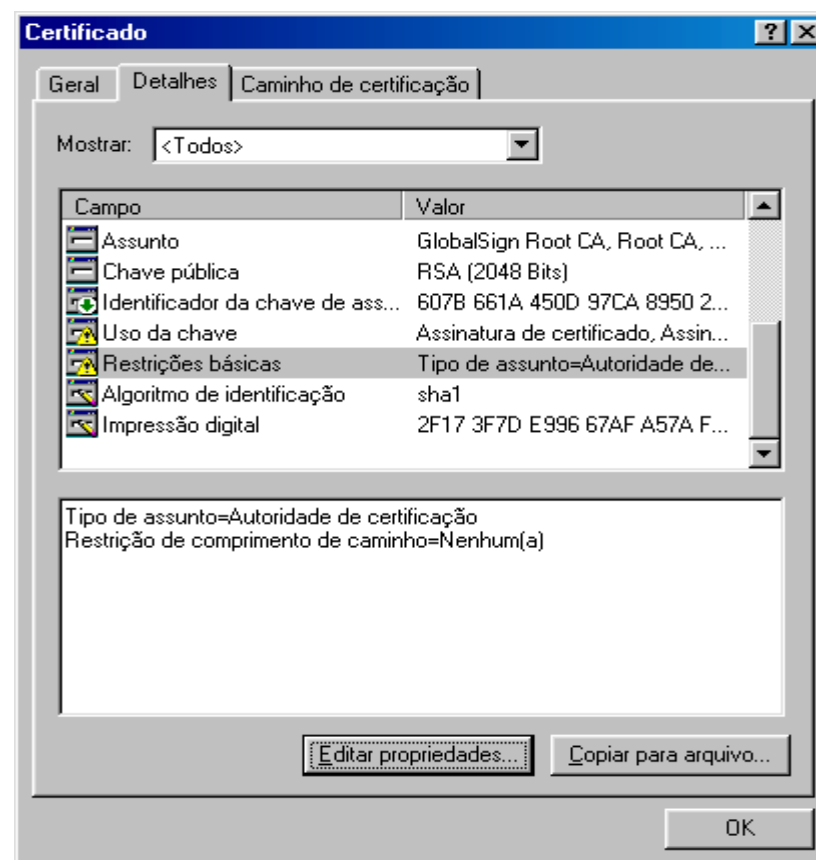
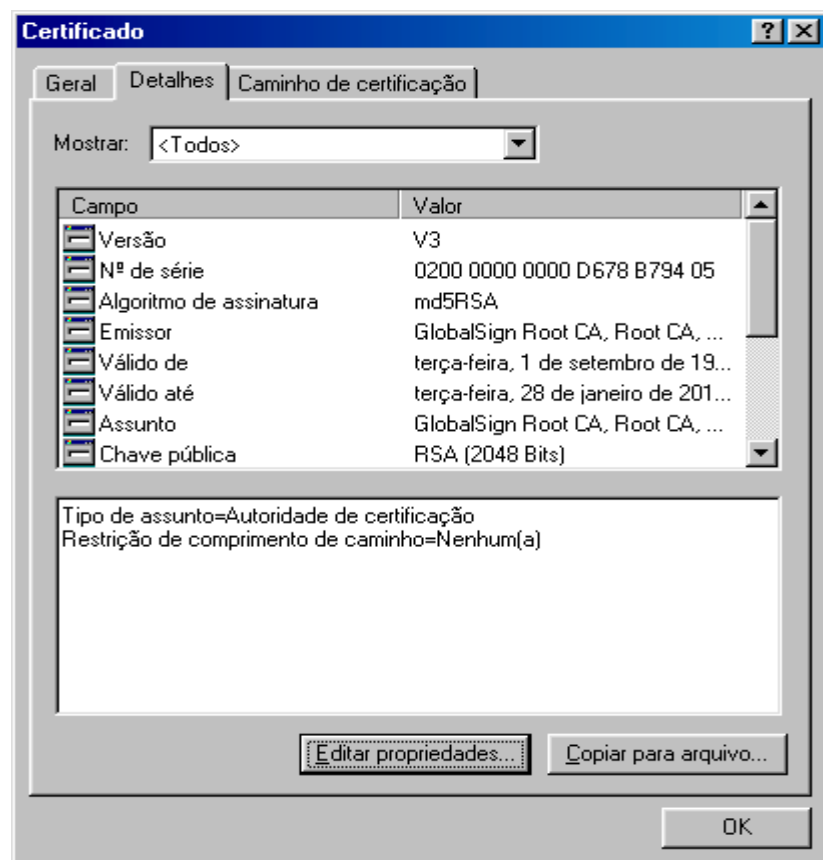


Certificados



Exemplo

Certificado de um CA



Geração de certificados

• Modalidades

- O par é gerado no mesmo sistema em que a chave privada será guardada e utilizada.
- O par é gerado em um sistema central, associado à Autoridade Certificadora.

• Responsabilidades da Autoridade Certificadora

- Autenticar o usuário (pessoa, página, sistema)
- Assinar a chave pública para gerar o certificado
- Distribuir a chave pública
- Atualizar o par de chaves
- Revogar certificados
- Distribuir listas de revogação
- *Gerar, entregar e armazenar a chave privada de forma segura*

Distribuição de certificados

✎ Assinatura digital

- O certificado pode acompanhar o dado assinado.

✎ Criptografia

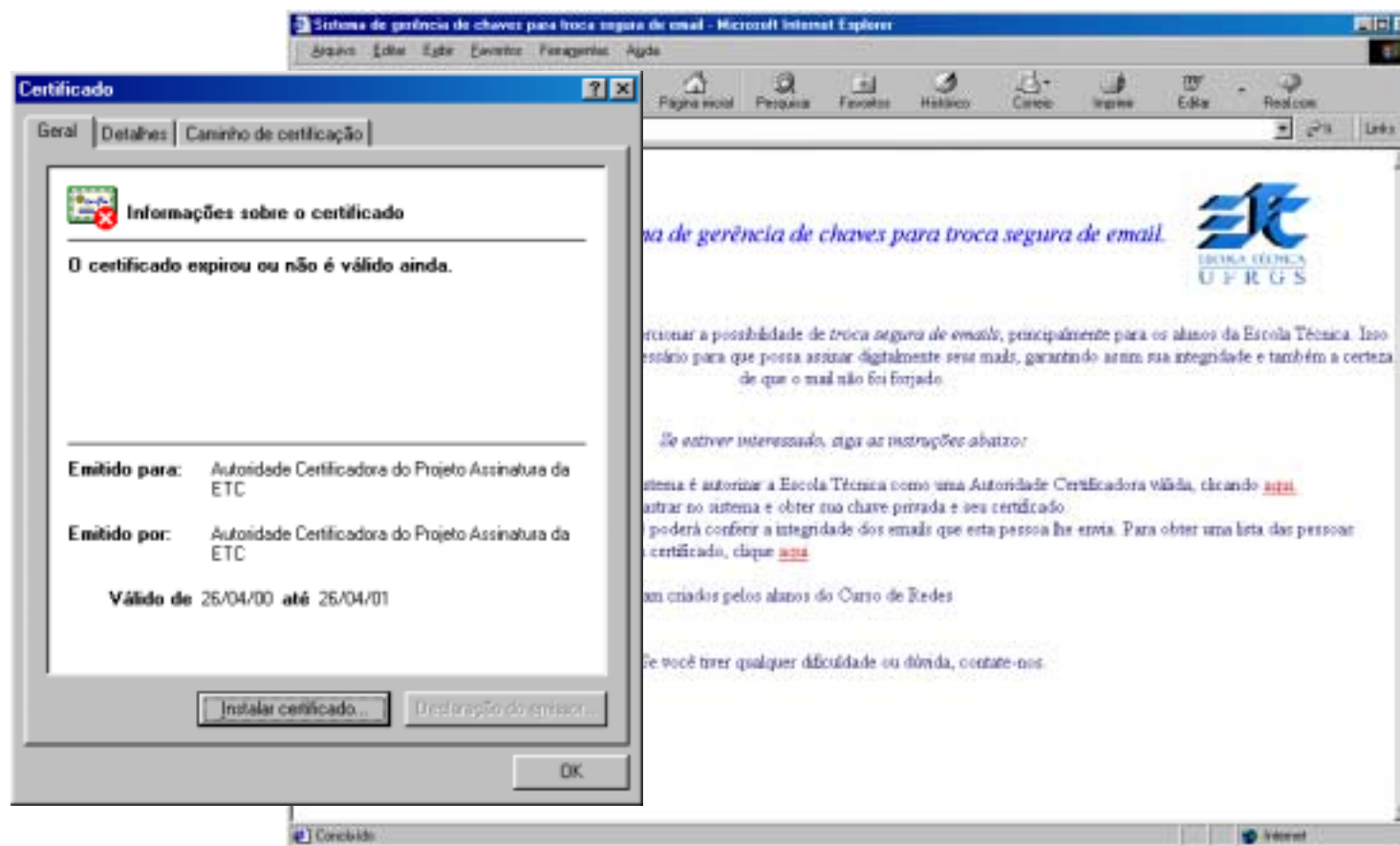
- Remetente precisa obter a chave pública certificada do destinatário.
- Serviço de diretório
 - X.500
 - NDS
 - Lotus Notes
 - Microsoft
 - LDAP
- WEB
- S/MIME

Certificados

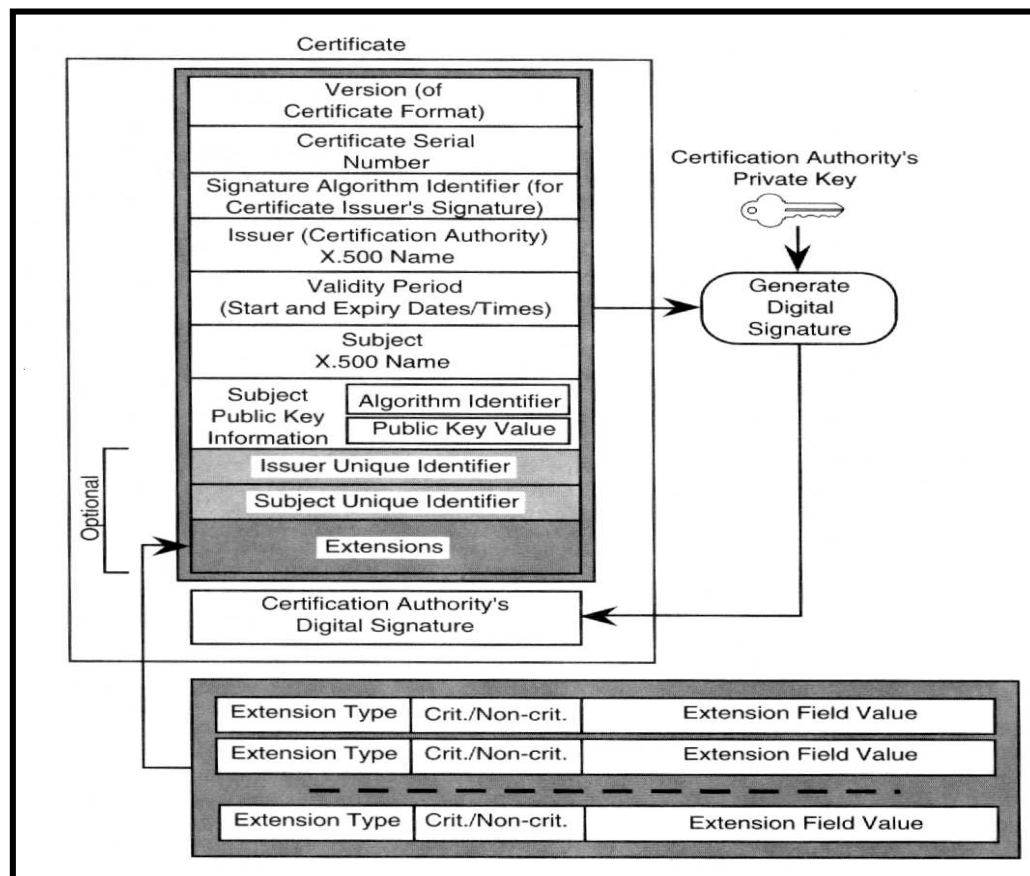


Distribuição de certificados

Distribuição via WEB



Formato de Certificado X.509



Formato da Versão 3

Formato de Certificado X.509

☞ Algumas extensões utilizadas

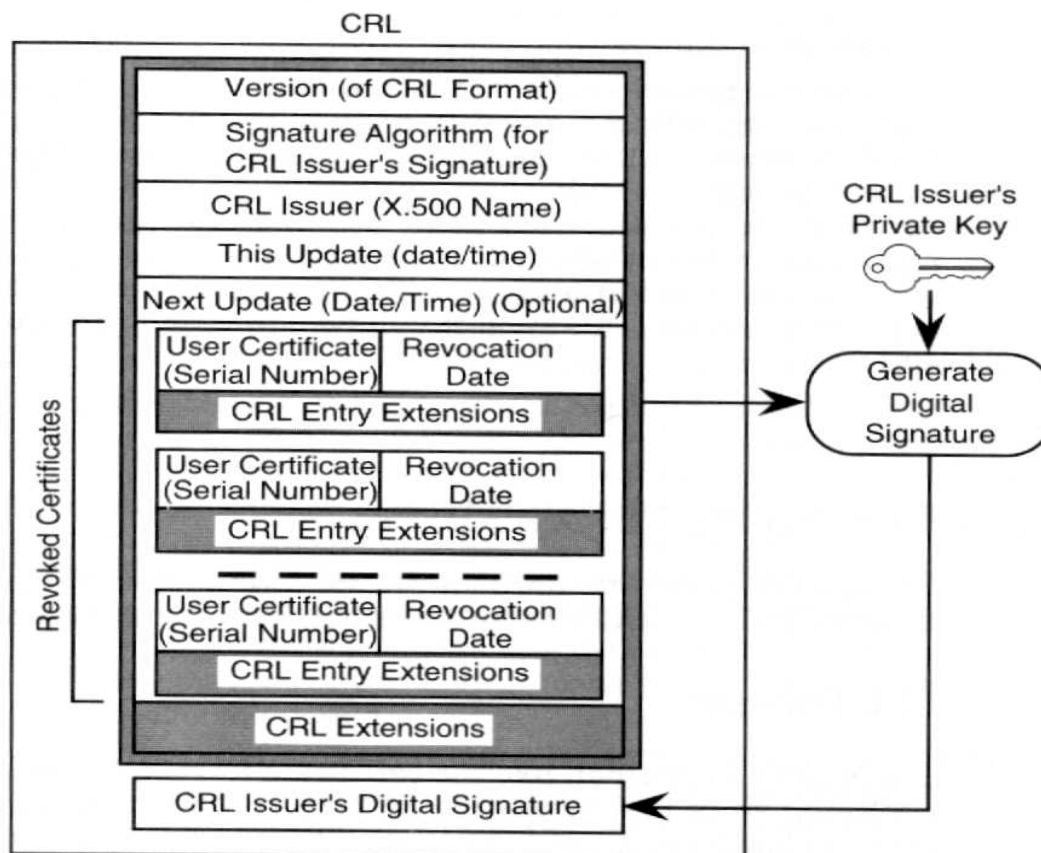
- Informações de chaves e políticas
 - ex: *Key Usage* - propósito da chave
- Atributos do sujeito e do emissor
 - ex: *Subject Alternative Name*
- Limitações de caminho de certificação
 - ex: *Basic Constraints*
- Extensões relacionadas a listas de revogação de certificados (CRL).

CRL - Lista de Revogação de Certificados

Conceitos

- Publicação
 - *Pull*
 - Diretório
 - WEB
 - *Push*
- A verificação de um certificado exige também a verificação de uma lista atualizada de certificados revogados.
 - Pontos de distribuição de CRL
 - Delta de CRL
 - CRL indireta
 - Suspensão de certificado (*held*)

Formato de CRL X.509



Formato da CRL

Requisitos para uma Infraestrutura de Chave Pública

Requisitos básicos

- escalabilidade
- suporte a várias aplicações
- interoperabilidade
- suporte a múltiplas políticas
- limitação de responsabilidade
- padronização