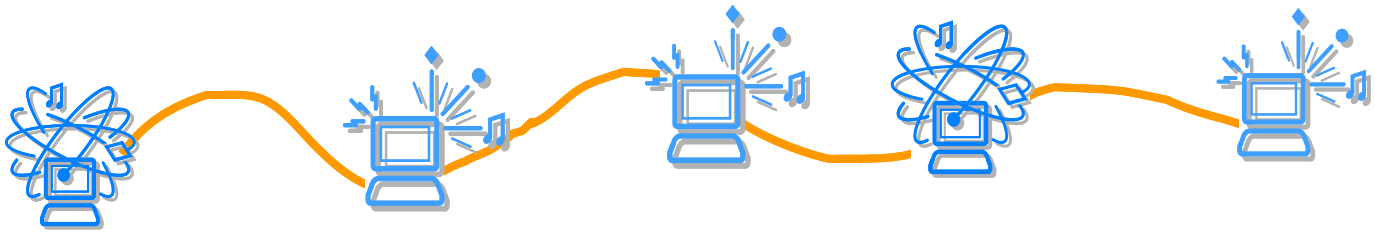
Segurança em Redes
S/MIME



Redes de Comunicação de Dados
Departamento de Engenharia da Electrónica e das Telecomunicações e de Computadores
Instituto Superior de Engenharia de Lisboa

- Baseados em:
  - Acetatos do Prof. Dr. Andreas Steffen da Zürcher Hochschule Winterthur

RFC 822

- Define um formato para mensagens de texto a serem enviadas por email
- Norma da Internet
- Estrutura das mensagens de acordo com o RFC 822, actualizado no RFC 2822
  - Linha do *header* (e.g., from: …, to: …, cc: …)
  - Linha em branco
  - Corpo (texto a ser enviado)

RFC 822

Exemplo

Date: Tue, 16 Jan 2005 01:27:05 (GMT)

From: “Vitor Almeida” <valmeida@deetc.isel.ipl.pt>

Subject: Teste

To: xpto@cobaia.deetc.isel.ipl.pt

Blablabla …

Problemas com o RFC 822 e o SMTP

- Os ficheiros executáveis devem ser convertidos em ASCII
  - Existem vários esquemas (e.g., Unix UUencode)
  - É necessária uma norma
- O texto com caracteres especiais tem também de ser convertido (e.g., texto em português)
- Alguns servidores:
  - Rejeitam mensagens acima de um determinado tamanho
  - Apagam, adicionam e reordenam os caracteres CR e LF
  - Cortam ou dividem linhas maiores do que 76 caracteres
  - Removem espaços em branco no fim da linha (*tabs* e espaços)
  - Preenchem as linhas de uma mensagem até à mesma dimensão
  - Convertem caracteres *tab* em múltiplos espaços

MIME

- Define novos *headers* para os campos das mensagens
- Define um número de formatos de conteúdos (normaliza a representação de conteúdos multimédia)
- Define "codificações de transferência" que protegem o conteúdo de alterações pelo sistema de *mail*

MIME: Novos *headers*

- **MIME-Version**
- **Content-Type**
  - Descreve os dados contidos no corpo da mensagem
  - O agente receptor pode escolher um método apropriado para representar o conteúdo
- **Content-Transfer-Encoding**
  - Indica o tipo de transformação que foi utilizado para representar o corpo da mensagem
- **Content-ID**
- **Content-Description**
  - Descrição do objecto no corpo da mensagem
  - Útil quando o conteúdo não é legível (e.g., dados áudio)

MIME: Tipos e subtipos de conteúdos

- *text/plain*, *text/enriched*
- *image/jpeg*, *image/gif*
- *video/mpeg*
- *audio/basic*
- *application/postscript*, *application/octet-stream*
- *multipart/mixed*, *multipart/parallel*, *multipart/alternative*, *multipart/digest* (cada parte da mensagem/rfc822)
- *message/rfc822*, *message/partial*, *message/external-body*

MIME: Codificações de transferência

- **7bit**
  - Linhas pequenas de caracteres ASCII
- **8bit**
  - Linhas pequenas de caracteres não ASCII
- **binary**
  - Caracteres não ASCII
  - Linhas não necessariamente curtas
- **quoted-printable**
  - Caracteres não ASCII são convertidos em números hexadecimais (e.g., =EF)
- **base64** (radix 64)
  - Blocos de 3 x 8-bits em blocos de 4 x 6 bits a transformar em caracteres ASCII
- **x-token**
  - Codificação não normalizada

MIME: Exemplo

MIME-Version: 1.0
From: Nathaniel Borenstein <nsb@nsb.fv.com>
To: Ned Freed <ned@innosoft.com>
Date: Fri, 07 Oct 1994 16:15:05 -0700 (PDT)
Subject: A multipart example
Content-Type: multipart/mixed; boundary=unique-boundary-1

This is the preamble area of a multipart message. Mail readers that understand multipart format should ignore this preamble. If you are reading this text, you might want to consider changing to a mail reader that understands how to properly display multipart messages.

--unique-boundary-1
Content-type: text/plain; charset=US-ASCII

… Some text …

--unique-boundary-1

MIME: Exemplo

Content-Type: multipart/parallel; boundary=unique-boundary-2

--unique-boundary-2
Content-Type: audio/basic
Content-Transfer-Encoding: base64

... base64-encoded 8000 Hz single-channel mu-law-format audio data goes here ...

--unique-boundary-2
Content-Type: image/jpeg
Content-Transfer-Encoding: base64

... base64-encoded image data goes here ...

--unique-boundary-2--

MIME: Exemplo (continuação)

--unique-boundary-1
Content-type: text/enriched

This is <bold><italic>enriched.</italic></bold><smaller>as defined in RFC 1896</smaller>Isn't it <bigger><bigger>cool?</bigger></bigger>

--unique-boundary-1
Content-Type: message/rfc822

From: (mailbox in US-ASCII)
To: (address in US-ASCII)
Subject: (subject in US-ASCII)
Content-Type: Text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: Quoted-printable

... Additional text in ISO-8859-1 goes here ...

--unique-boundary-1--

S/MIME: Serviços

- **enveloped data** (application/pkcs7-mime; smime-type = enveloped-data)
  - Envelope digital normalizado
- **signed data** (application/pkcs7-mime; smime-type = signed-data)
  - Assinatura digital normalizada (“hash and sign”)
  - conteúdo + assinatura são codificados usando codificação base64
- **clear-signed data** (multipart/signed)
  - Assinatura digital normalizada
  - Apenas a assinatura é codificada usando base64
  - Receptor sem capacidade S/MIME pode ler a mensagem mas não pode verificar a assinatura
- **signed and enveloped data**
  - Entidades assinadas e cifradas podem ser em qualquer ordem

Algoritmos de criptografia

- ***Message digest***
  - deve: SHA-1
  - pode (receptor): MD5 (compatibilidade para trás)
- **Assinatura digital**
  - deve: DSS
  - pode: RSA
- **Cifra assimétrica**
  - deve: ElGamal
  - pode: RSA
- **Cifra simétrica**
  - emissor:
    - pode: 3DES, RC2/40
  - receptor:
    - deve: 3DES
    - pode: RC2/40

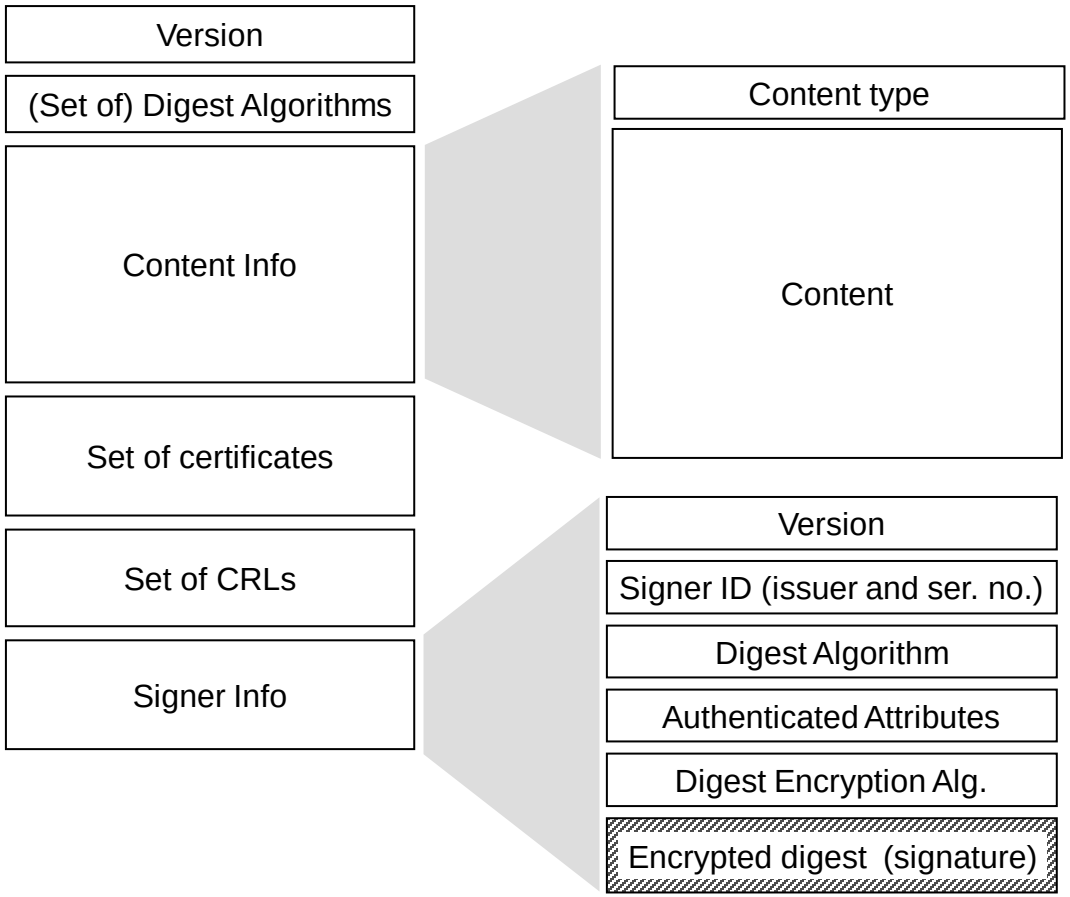
Segurança de uma entidade MIME

- Uma entidade MIME é preparada de acordo com as regras normais para a preparação de uma mensagem MIME

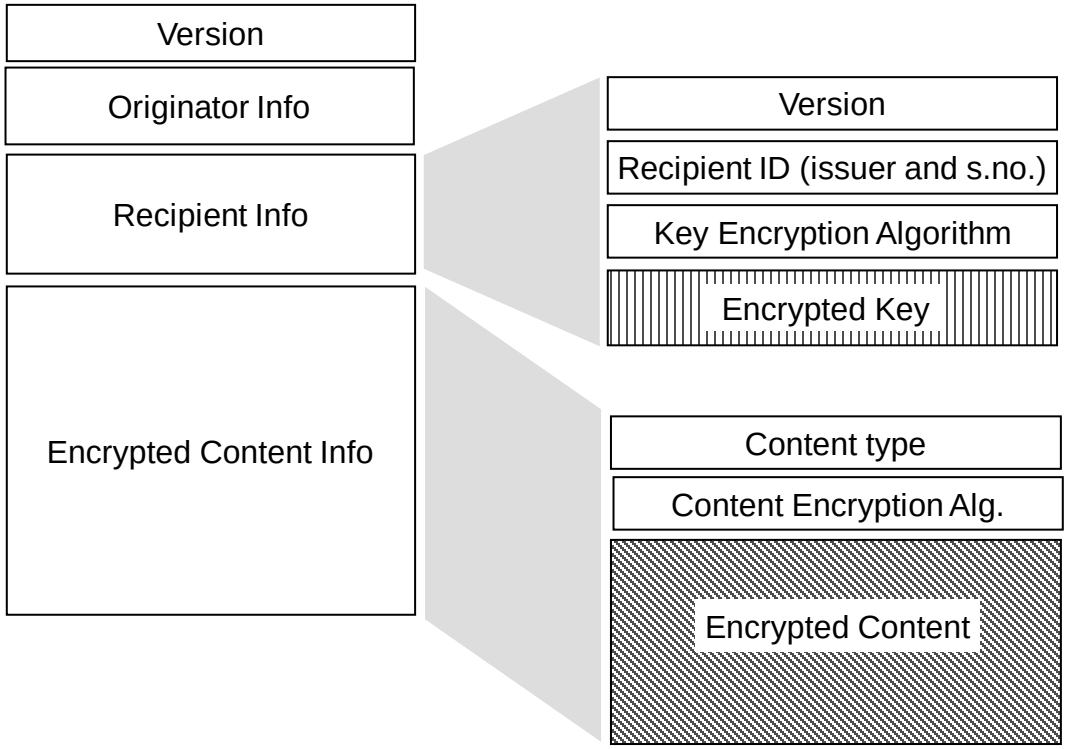
- A entidade MIME preparada é processada pelo S/MIME para produzir um objecto PKCS

- O objecto PKCS é tratado como o conteúdo de uma mensagem e passada ao MIME

PKCS7: “Dados assinados”



PKCS7: “Dados cifrados”



Exemplo: Dados cifrados

Content-Type: application/pkcs7-mime; smime-type=enveloped-data; name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m

rfvbnj756tbBghyHhHUujhJhjH77n8HHGT9HG4VQpfyF467GhIGfHfYT6
7n8HHGghyHhHUujhJh4VQpfyF467GhIGfHfYGTrfvbnjT6jH7756tbB9H
f8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
0GhIGfHfQbnj756YT64V

Exemplo: Dados assinados

Content-Type: multipart/signed; protocol="application/pkcs7-signature";
micalg=sha1; boundary=boundary42

--boundary42
Content-Type: text/plain

This is a clear-signed message.

--boundary42
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s

ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT6
4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbB9HGTrfvbnj
n8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
7GhIGfHfYT64VQbnj756

--boundary42--

O que é o S/MIME?

- ***Secure / Multipurpose Internet Mail Extension***
- Melhoria de segurança do MIME
- Fornece serviços semelhantes ao PGP
- Baseado na tecnologia da RSA Security
- Norma da indústria
  - RFC 2630 ("*Cryptographic Message Syntax*")
  - RFC 2632 ("*S/MIME Version 3 Certificate Handling* ")
  - RFC 2633 ("*S/MIME Version 3 Message Specification* ")

S/MIME

- Teve origem na RSA Data Security Inc. em 1995.
- Foi depois mais desenvolvido pelo *working group* IETF S/MIME em:

  www.ietf.org/html.charters/smime-charter.html
- A versão 3 é especificada nos **RFC 2630-2634**.
- Algumas alterações levaram à versão 3.1
- Permite segurança flexível cliente-cliente através de cifra e assinaturas
- Grande suporte, e.g. no Microsoft Outlook, Netscape Messenger, Lotus Notes…

S/MIME: Formato das mensagens

- Como o nome sugere, o S/MIME adiciona facilidades de segurança através da extensão do MIME

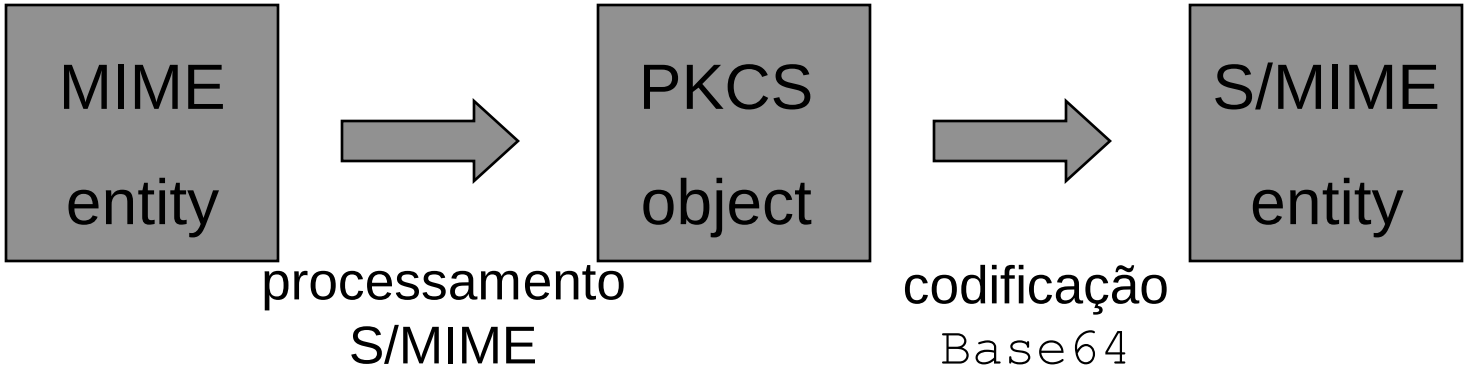
- O S/MIME adiciona 5 novas combinações de conteúdos “type/subtype” incluindo:
  - `application/pkcs7-mime; smime-type=enveloped-data`
  - `application/pkcs7-mime; smime-type=signed-data`
  - `multipart/signed`

- Os restantes tipos são para as mensagens de gestão de chaves

S/MIME: Processamento

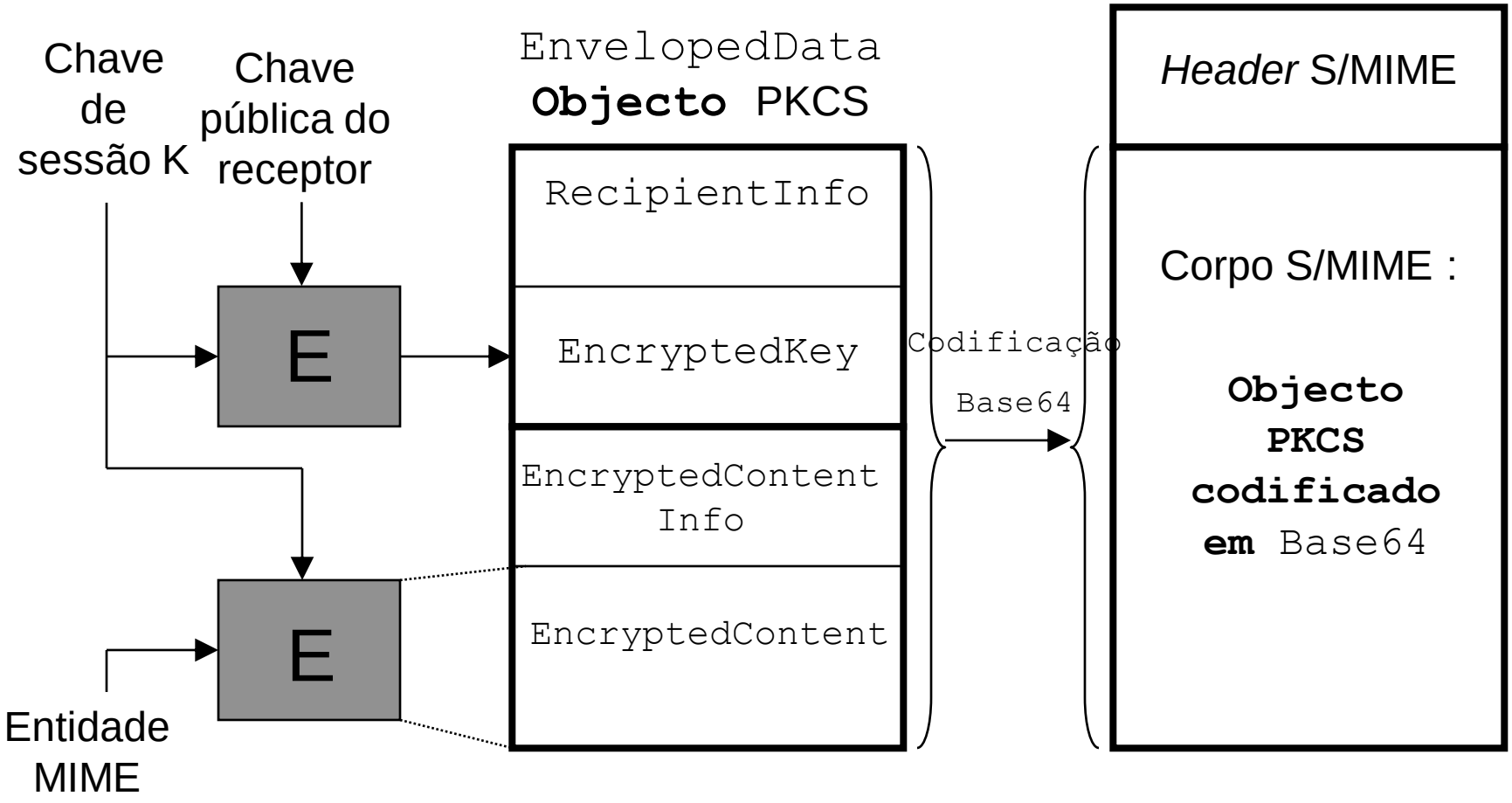
- O processamento S/MIME pode ser aplicado a qualquer entidade MIME:
  - Uma parte de uma mensagem *multipart* MIME, talvez uma que seja ela própria do tipo S/MIME `Content-Type`.
  - O resultado final é sempre outra entidade MIME, do tipo S/MIME `Content-Type`.
  - Então a cifra e a assinatura podem ser aplicadas uma depois da outra, em qualquer ordem

S/MIME: Processing – Sender



- O processamento inicial do S/MIME produz um objecto PKCS.
  - **PKCS = *Public Key Cryptography Standard***, conjunto de especificações desenvolvidas pela RSA
- Os objectos PKCS incluem a informação necessária ao processamento pelo receptor assim como o conteúdo original. O objecto PKCS é em formato binário, tendo de ser codificado em base64 para produzir um objecto MIME do tipo S/MIME `content-type`
- O receptor efectua as operações em ordem inversa

S/MIME: enveloped-data



S/MIME: `enveloped-data`

Exemplo de mensagem (de RFC 2633):

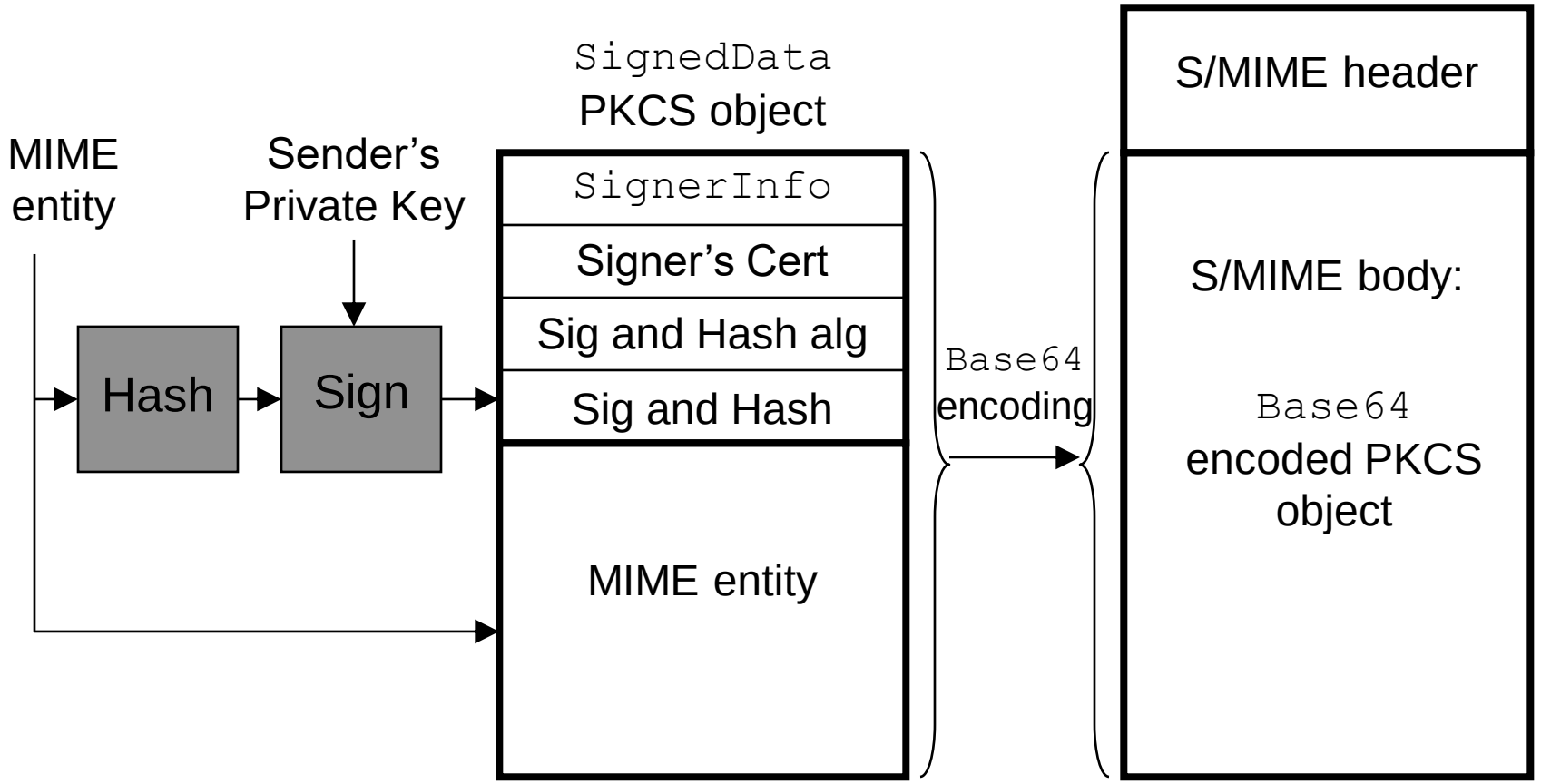
```
Content-Type: application/pkcs7-mime;
   smime-type=enveloped-data; name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition:attachment;filename=smime.p7m

rfvbnj756tbBghyHhHUujhJhjH77n8HHGT9HG4VQpfyF467GI
7n8HHGghyHhHUujhJh4VQpfyF467GhIGfHfYGTrfvbnjT6jHd
f8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHh6
```

S/MIME: `enveloped-data`

- O tipo S/MIME `enveloped-data` fornece um serviço de confidencialidade de dados através de cifra.
- O *header* S/MIME contém os campos originais `To:`, `From:` e `Subject:`, pelo que a protecção não é completa.
- Algoritmos simétricos com chaves de sessão para cifra eficiente de grandes quantidades e cifra assimétrica para protecção das chaves de sessão.
- O receptor realiza os seguintes passos: obtém a chave de sessão K usando a chave privada, usa K para decifrar `EncryptedContent`.
  - Os algoritmos usados são especificados nos blocos `RecipientInfo` e `EncryptedContentInfo`.

S/MIME: `signed-data`



S/MIME: `signed-data`

Exemplo de mensagem (do RFC 2633):

```
Content-Type: application/pkcs7-mime;
   smime-type=signed-data; name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition:attachment;filename=smime.p7m

567GhIGfHfYT6ghyHhHUujpfyF4f8HHGTrfvhJhjH776tbB97
7n8HHGT9HG4VQpfyF467GhIGfHfYT6rfvbnj756tbBghyHhHU
HUujhJh4VQpfyF467GhIGfHfYGTrfvbnjT6jH7756tbB9H7n8
```

S/MIME: `signed-data`

- O tipo S/MIME signed-data fornece serviços de integridade de dados, autenticação da origem dos dados e não-repudiação utilizando as assinaturas dos emissores.
- São suportados múltiplos assinantes – prepara um bloco SignerInfo para cada um.
- O receptor testa a assinatura usando a entidade S/MIME embebida no objecto PKCS e a chave pública do emissor.
- O receptor sem capacidade S/MIME não consegue ler a mensagem original (mesmo que não queira saber das assinaturas).

S/MIME: Assinatura em claro

- Usa o conteúdo do MIME tipo `multipart/signed`.
- A primeira parte contem a entidade MIME a ser assinada
- A segunda contém a entidade S/MIME `application/pkcs7-signature`, criada como para o tipo `signed-data`.
- Os receptores que têm capacidade MIME mas não S/MIME podem ainda ler a mensagem
- Os receptores que têm capacidade S/MIME usam a primeira parte como objecto MIME na verificação da assinatura S/MIME

S/MIME: Assinatura em claro

```
Content-Type: multipart/signed;
   protocol="application/pkcs7-signature";
   micalg=sha1; boundary=boundary42
--boundary42
Content-Type: text/plain

This is a clear-signed message.
--boundary42
Content-Type: application/pkcs7-signature;
   name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition:attachment;filename=smime.p7s
   ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF4674VQ
   pfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tb6
--boundary42--
```

Algoritmos S/MIME

- Cifra simétrica:
  - DES, 3DES, RC2 com chaves de 40 e 64 bits.
- Cifra assimétrica:
  - RSA, ElGamal.
- *Hashing*:
  - SHA-1, MD5.
- Assinaturas:
  - RSA, *Digital Signature Standard* (DSS).

MIME: *Multipurpose Internet Mail Extension*

RFC 1521 / RFC 1522

```
From: trinity@matrix.org
To: neo@matrix.org
MIME-Version: 1.0
Content-Type: multipart/mixed;
  boundary=boundary1

--boundary1
Content-Type: text/plain; charset=us-ascii

Dear Neo, please study the attached Word document.

--boundary1
Content-Type: application/msword; name="Matrix.doc"
Content-Transfer-Encoding: base64

ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfH
4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbTrfv=

--boundary1--
```

S/MIME: Formato das mensagens assinadas I

RFC 1847 / RFC 2311 / PKCS #7

```
Content-Type: multipart/signed;
  protocol="application/pkcs7-signature";
  micalg=sha1; boundary=boundary1

--boundary1
Content-Type: text/plain

This is a clear-signed message.

--boundary1
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s

ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfH
4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbTrfv=

--boundary1--
```

Entidade MIME a ser assinada

S/MIME: Mensagens assinadas

Multiplos anexos

```
Content-Type: multipart/signed;
  protocol="application/pkcs7-signature";
  micalg=sha1; boundary=boundary1

--boundary1
Content-Type: multipart/mixed; boundary=boundary2

  ... multipart message with various MIME-types ...

--boundary1
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s

ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfH
4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbTrfv=

--boundary1--
```

PKCS #7 – *Public Key Cryptography Standard*
Norma de sintaxe de mensagens criptográficas

- Estrutura ASN.1 para conteúdos do tipo SignedData

```
version
digestAlgorithms
contentInfo
certificates (OPTIONAL)
crls (OPTIONAL)
signerInfos (SET OF)
```

Campo vazio
(conteúdo transportado em entidade MIME separada

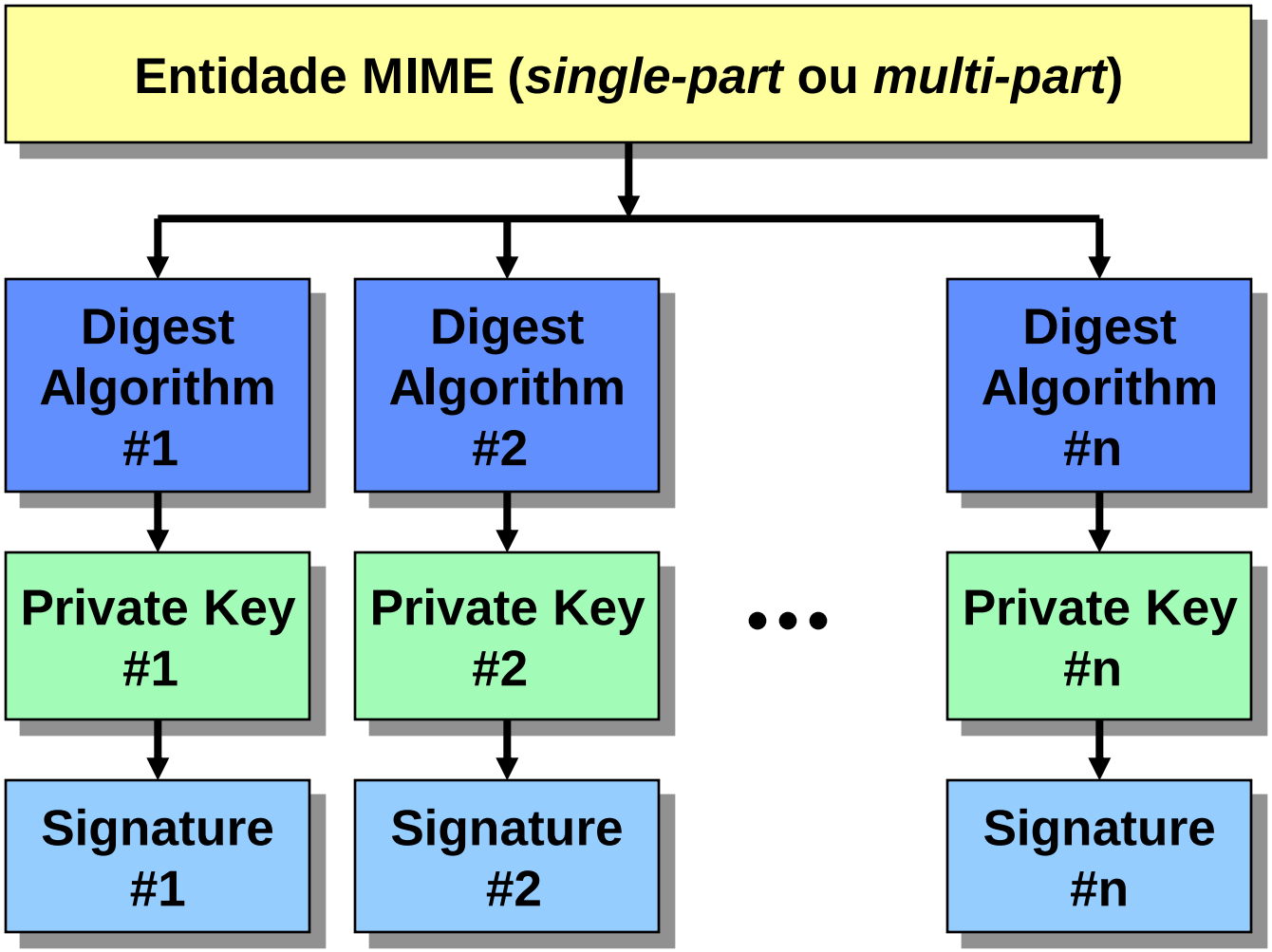
vários assinantes possível

- Estrutura ASN.1 para o tipo SignerInfo

```
version
issuerAndSerialNumber
digestAlgorithm
authenticatedAttributes
digestEncryptionAlgorithm
encryptedDigest
unauthenticatedAttributes
```

assinatura

Mensagem assinada com múltiplas assinaturas



S/MIME: Formato de mensagem assinada II

RFC 2311 / PKCS #7

```
Content-Type: application/pkcs7-mime;
  smime-type=signed-data;
  name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m

ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfH
4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbTrfv=
```

- Conteúdo MIME transportado num "*Signed Data Object*" PKCS#7
  - Esta alternativa de formato de assinatura é usado, por exemplo, no Outlook 2000
  - Pro: O conteúdo MIME não é sujeito a alterações da codificação de transferência forçada por agentes intermédios de mail.
  - Contra: De maneira a ler a mensagem MIME embebida, o cliente de email do receptor tem de suportar S/MIME.

S/MIME: Formato da mensagem cifrada

RFC 2311 / PKCS #7

```
Content-Type: application/pkcs7-mime;
  smime-type=enveloped-data;
  name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m

ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfH
4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbTrfv=
```

- Estrutura ASN.1 para conteúdos do tipo EnvelopedData

```
version
recipientInfos
encryptedContentInfo
```

Possibilidade de vários receptores

(cifrado com chave simétrica)

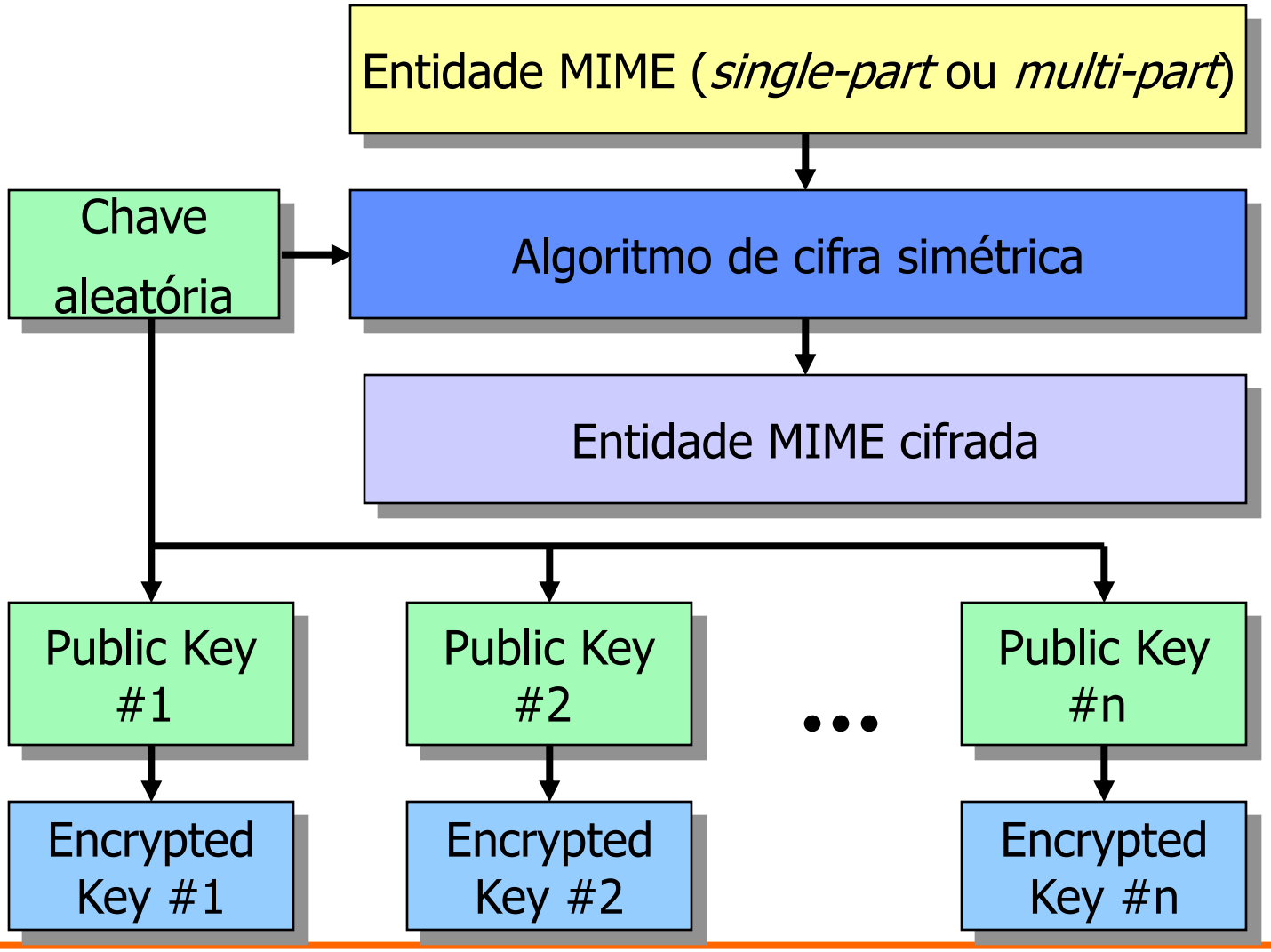
```
contentType
contentEncryptionAlgorithm
encryptedContent
```

Entidade MIME cifrada

(*single-part* ou *multi-part*)

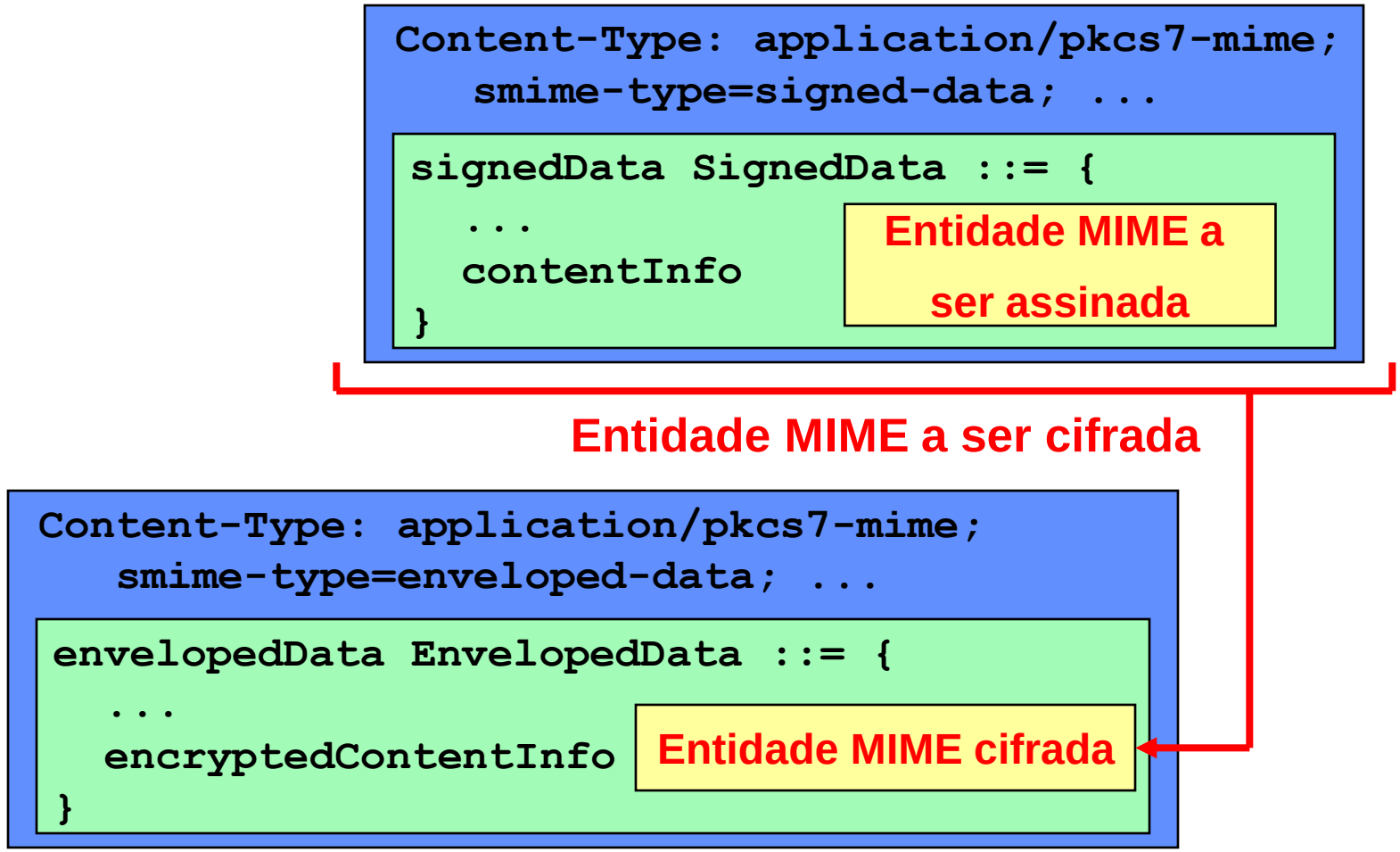
Mensagem cifradas com receptores múltiplos

Envelope utilizando cifra simétrica



S/MIME: Mensagem assinada e cifrada I

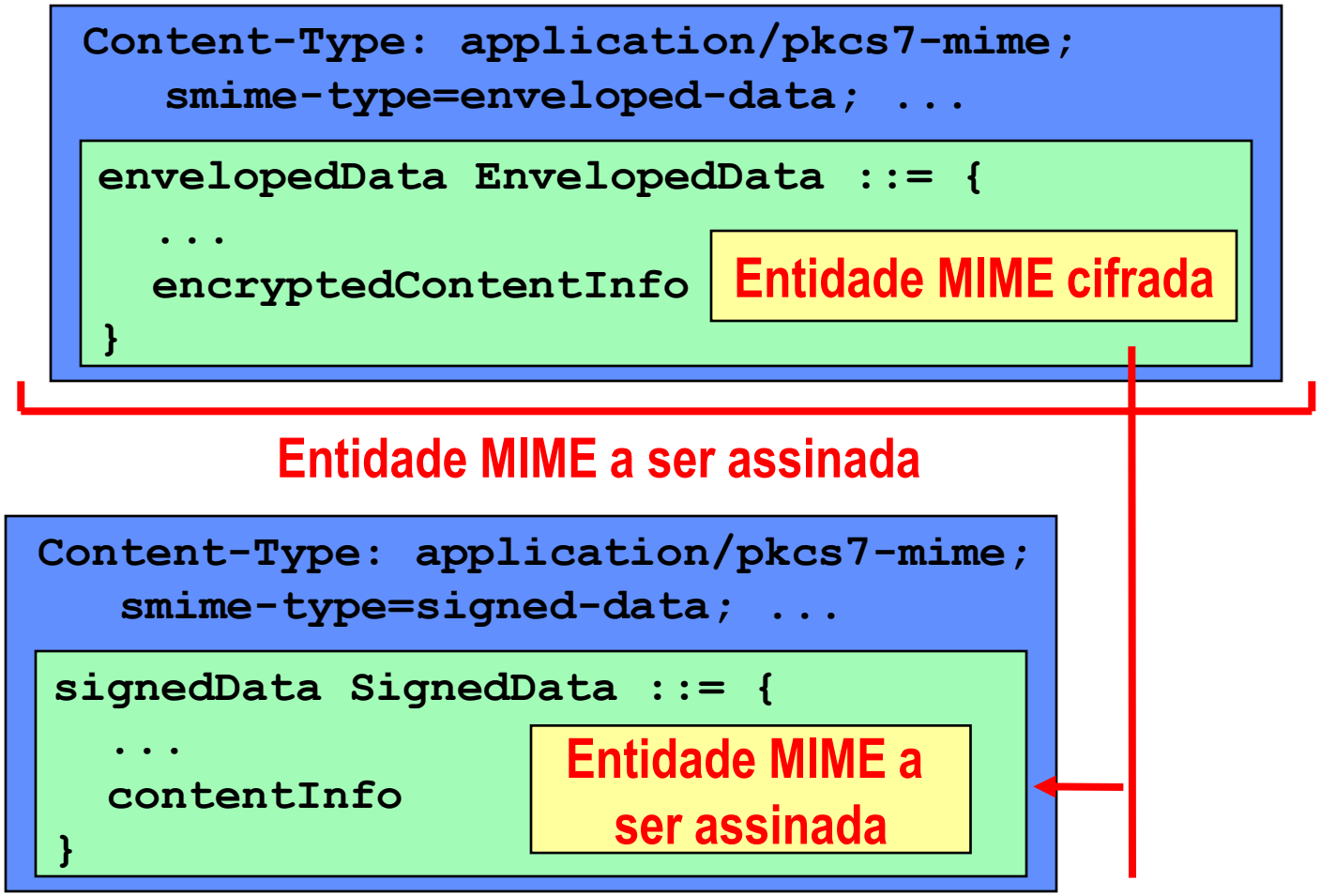
Assinar antes de cifrar



- A(s) assinatura(s) não são visiveis antes da decifração (Anonimato)

S/MIME: Mensagem assinada e cifrada II

Cifra antes da assinatura



- A(s) assinaturas podem ser verificadas antes de decifrar (Confiança)

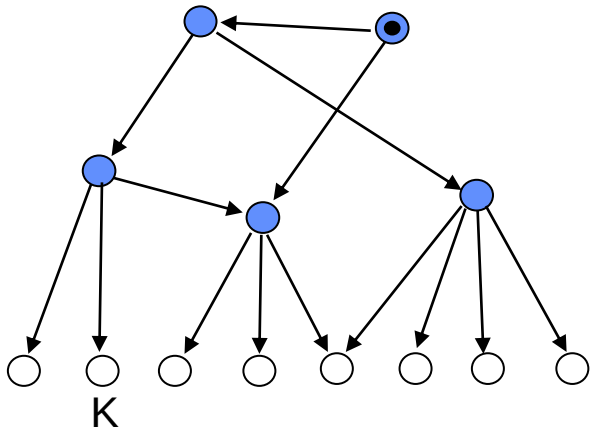
Gestão de chaves no PGP e S/MIME

- O PGP e o S/MIME usam:
  - Chaves públicas para cifra de chaves de sessão/verificação de assinaturas.
  - Chaves privadas para decifrar chaves de sessão / criar assinaturas.

- De onde vêm estas chaves e até onde é que se pode confiar nelas?

Gestão de chaves

- Os certificados S/MIME estão de acordo com o ISO/ITU-T X.509v3. A mesma norma que é usada para definir certificados no SSL/TLS e IPSec.
- O esquema de gestão de chaves está entre a hierárquia rigida de certificação e a "*web of trust*" do PGP
  - Os certificados são assinados pelas autoridades de certificação (CA)
  - A autenticação das chaves é baseada em cadeias de certificados.
  - Utilizadores/gestores são responsáveis por configurar os seus clientes com uma lista de chaves de raíz de confiança.



S/MIME: Gestão de chaves

Alguns pormenores:

- **Interpretação**: Ao utilizador final é perguntado: "Confia neste certificado?" Como é que um utilizador não consciente dos certificados deve interpretar isto?
- **Escala**: Como gerir um grande número de utilizadores?
- **Revogação**: Como comunicar a todos os utilizadores de que um certificado já não é válido?
- **Responsabilidade**: Quanta responsabilidade (se alguma) aceita o emissor? Talvez tudo bem se o emissor for o empregador.
- **Armazenamento da chave privada**: No computador do utilizador final, talvez protegida por uma *password*.
- **Procedimento de emissão de certificados** (registo): É mesmo o Xavier? Sim? Qual Xavier?

Segurança no E-mail: Para lá do PGP e do S/MIME

- O PGP e o S/MIME contrariam as ameaças básicas à confidencialidade, integridade e autenticidade do email razoavelmente bem (assumindo uma boa gestão das chaves).
- Eles não protegem contra outras ameaças (vírus, DoS, divulgação, uso não-autorizado,…)
- Não fornecem nenhuma protecção contra análise de tráfego.
- Medidas de segurança adicional serão necessárias para construir um sistema de email seguro.

Anti-virus e filtagem de conteúdos

- Complementar o servidor de email (ou máquinas clientes) com software de filtragem de conteúdos/SPAM
  - Bloquear *emails* com conteúdos ativos ou tipos específicos de anexos.
  - Rejeitar ou marcar *emails* suspeitos de serem SPAM
  - Analisar emails de entrada e de saída à procura de vírus e de conteúdos não apropriados.
  - Adicionar avisos.
  - O servidor não pode aplicar filtragem de conteúdos a emails cifrados (só se tivesse as chaves necessárias)
- Carga significativa para o servidor de *email*, pode aborrecer os utilizadores (mas a quem pertencem afinal os emails?).

Protecção *anti-spamming*

- Configurar o servidor de *email* para não permitir a realização das funções de *mail relay*.
- Prevenir que o servidor seja utilizado como um agente no envio de *emails* por *spammers*.
- Jogar fora todos os *emails* de servidores na *Open Relay Blacklist* (ORB) [http://www.ordb.org/].
- Controlar quem pode correr um servidor de *email* na sua organização através da política apropriada e vigilância apropriadas.

Firewalls e servidores de *email*

- Colocar o servidor de *email* por detrás do *firewall*.
- Configurar o *firewall* para bloquear todo o tráfego externo de/para o MTA excepto do porto 25 (SMTP).
- Limitar as possibilidades de ataques ao servidor de *email*, mas um ataque com sucesso pode dar acesso a sistemas internos.
  - Necessita de medidas de segurança.
- Melhor utilização de uma rede de perímetro.
  - Isolar totalmente o servidor das redes interiores e exteriores através de *firewalls*
  - Configurar o *firewall* para bloquear todo o tráfego interno de/para o MTA excepto nos portos 25, 110 (POP3),143 (IMAP) e 53 (DNS).
- Utilização de *DomainKeys* para certificar os servidores de *email* dos respectivos domínios.

Fortalecer os servidores de *email*

Tomar medidas adicionais no servidor de *email*:

- Fortalecer o sistema operativo (OS):
  - Remover contas não necessárias, aplicações e serviços de rede.
  - Aplicar os "*patches*" mais recentes do OS.
- **Fortalecer a aplicação do servidor de *email* (eg Sendmail, Microsoft Outlooh Exchange):**
  - Usar as últimas versões do software.
  - Escolher configurações apropriadas (eg limitar as dimensões dos anexos, as facilidades de *mail relay* e permissões de ficheiros).
  - Manter actualizados com os "*patches*" dos vendedores.

Administração do servidor de *email*

- Fazer *log* dos dados dos servidor de *email* e rever os ficheiros de *logs* regularmente (considerar a análise automática).
- Ter em atenção os alertas de vulnerabilidades e manter o servidor de *email* com os *patches* actualizados.
- Considerar permitir apenas administração a partir da consola ou utilizar SSH para a administração remota.
- Efectuar os *backups* apropriados do servidor de *email*.

Segurança do *email* do lado do cliente

De novo, uma boa configuração e os *patches* apropriados são essenciais:

- Desactivar o "*preview*" automático de mensagens.
- Desactivar o processamentode conteúdoa activos (macros, ActiveX, Java, Javascript,…).
- Desactivar as caixas de diálogo "*remember this password*?" POP/IMAP se possível.
- Considerar protocolos POP e IMAP fortalecidos.
- Estar atento aos riscos extra dos acessos através da Web:
  - Armazenamento das teclas introduzidas e captura das credenciais dos utilizadores.
  - Os conteúdos sobre HTTP podem não passar pelos filtros de conteúdos.
  - Os *emails* dos clientes podem ser deixados no histórico do *browser* ou em ficheiros temporários.

Política de *emails* e treino

- Desenvolver e publicitar uma politica de *email* para os utilizadores.
  - Regras de utilização, definições de abuso de serviço, clarificação de a quem pertencem os *emails*.
- Assegurar que os utilizadores percebem a política de *email* antes de utilizarem o sistema.
- Aumentar a consciência de segurança na organização através de treino.
- Forçar a política de segurança!

Súmario

- O *email* passa através de redes internas e da rede pública da Internet.
- O *email* é sujeito a muitas ameaças.
- O PGP e o S/MIME podem servir para resolver o problema da segurança extremo-a-extremo através de mecanismos de cifra e de assinatura digital.
- Endereçar os restantes assuntos requer uma ponderação cuidadosa de segurança do computador, segurança da rede e contra-medidas na gestão de segurança.

Alguns recursos

- NIST Special Publication 800-45:

  Guidelines on Electronic Mail Security por S. Bisker, M. Tracy e W. Jansen. Available de:

  http://csrc.nist.gov/publications/nistpubs/index.html
- W. Stallings, “Network Security Essentials”, Capítulo 5: Mais sobre PGP e S/MIME.
- http://www.spamlaws.com/: detalhes sobre a legislação anti-spam.
- Open PGP: www.openpgp.org
- S/MIME: www.ietf.org/html.charters/smime-charter.html
- Todos os RFCs estão em www.ietf.org.