Aplicações

MICEI/MSDPA 2006-2007

José Carlos Bacelar Almeida

(jba@di.uminho.pt)

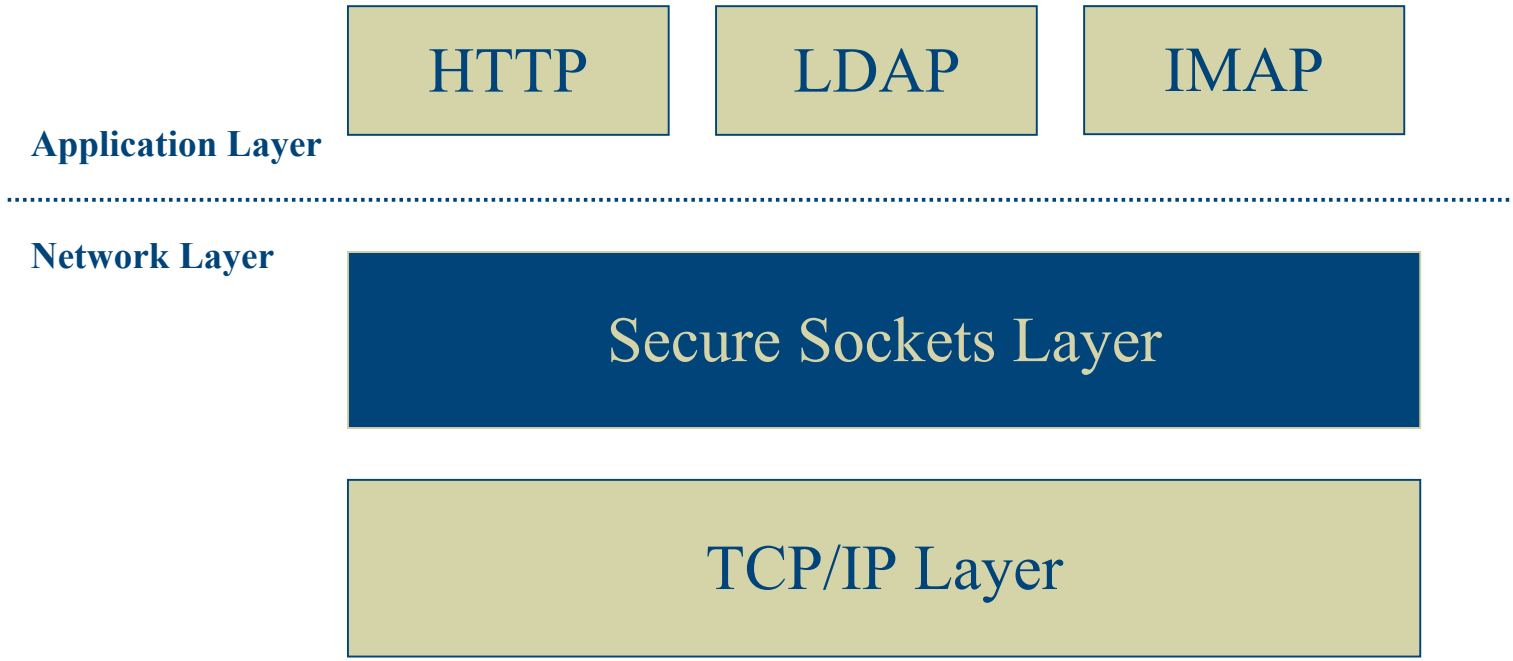
Aplicações da criptografia

Nível	Requer intervenção...	Exemplos
infra-estrutura de comunicações	hardware, sistema operativo	IPSec; DNS-Sec
Sessão	Sistema operativo, administrador do sistema	SSH; SSL
Mensagem	Utilizador	S/Mime; PGP

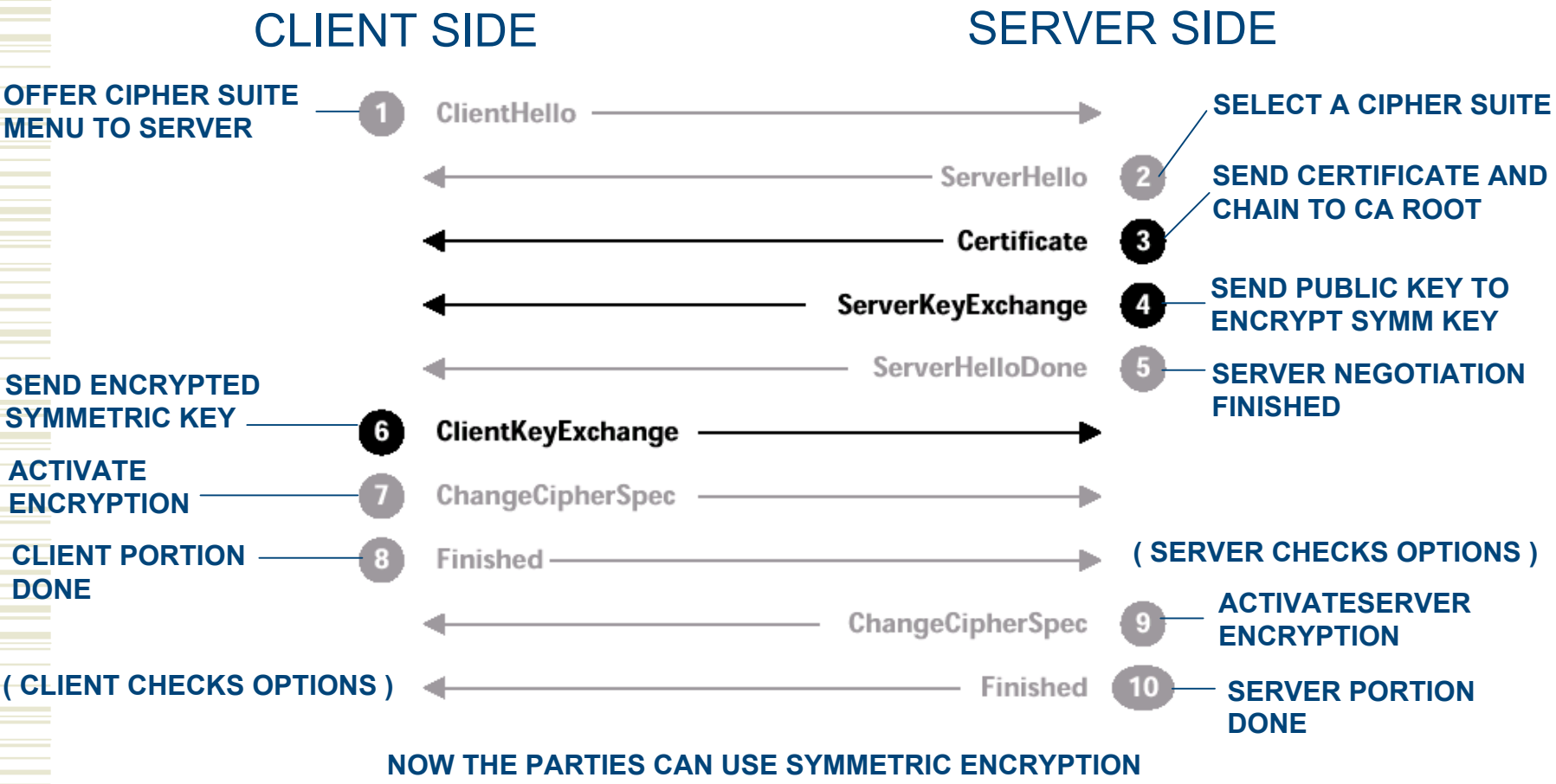
Secure Sockets Layer (SSL)

- Desenvolvido pela *Netscape inc.* para disponibilizar uma abstracção segura sobre os *sockets*.
- Disponibiliza três modos de autenticação
  - Autenticação nula (...desaconselhada...)
  - Autenticação de servidor
  - Autenticação mutua
- Faz uso de certificados X509 para autenticações.
- Parametrizado pelas técnicas criptográficas utilizadas (*cipher suites*).
- SSLv3 deu origem ao standard IETF *TLS* v1 *(Transport Layer Security)*

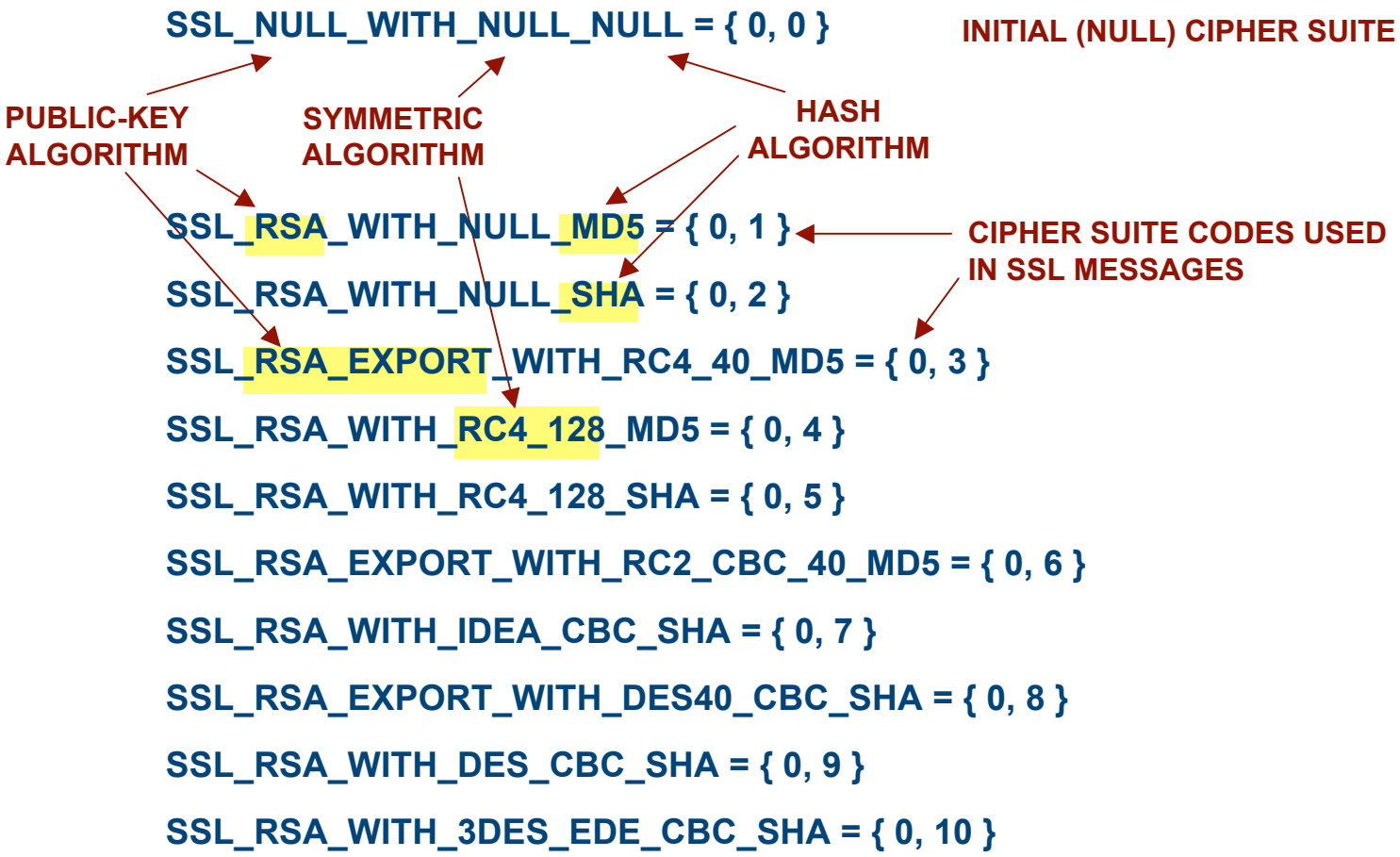
SSL (cont.)


HTTP
LDAP
IMAP
Application Layer
Network Layer
Secure Sockets Layer
TCP/IP Layer

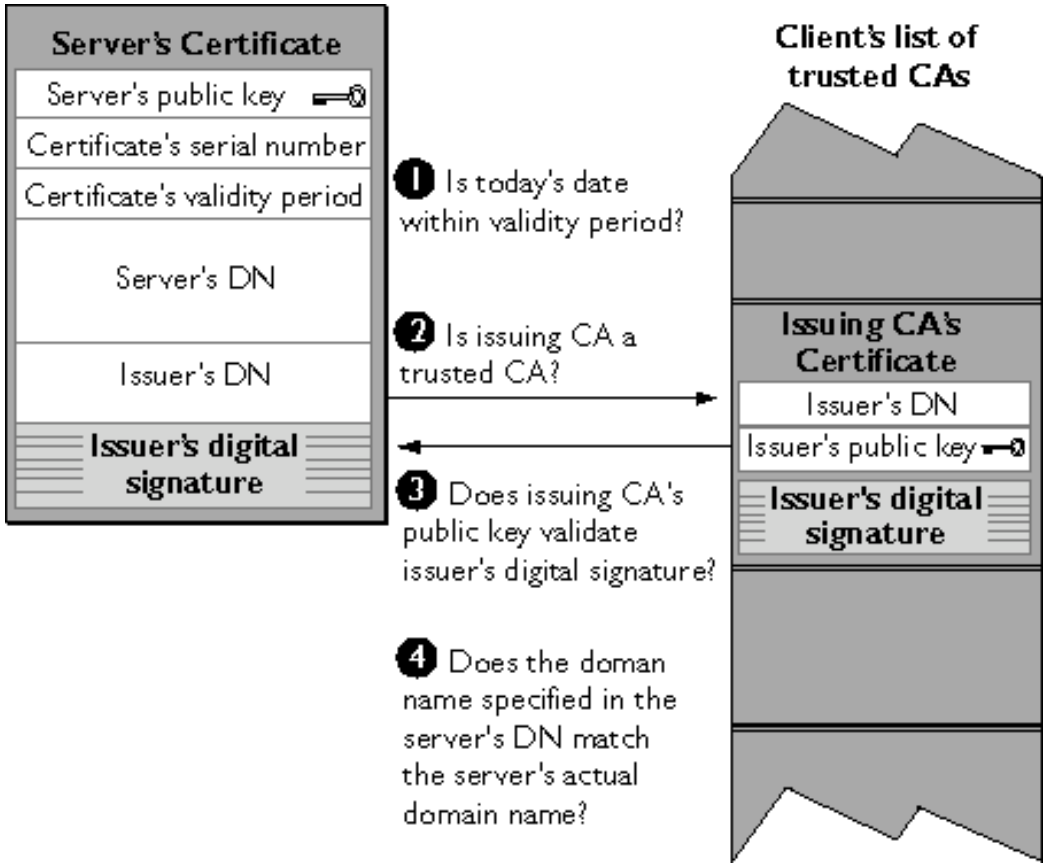
SSL - handshake



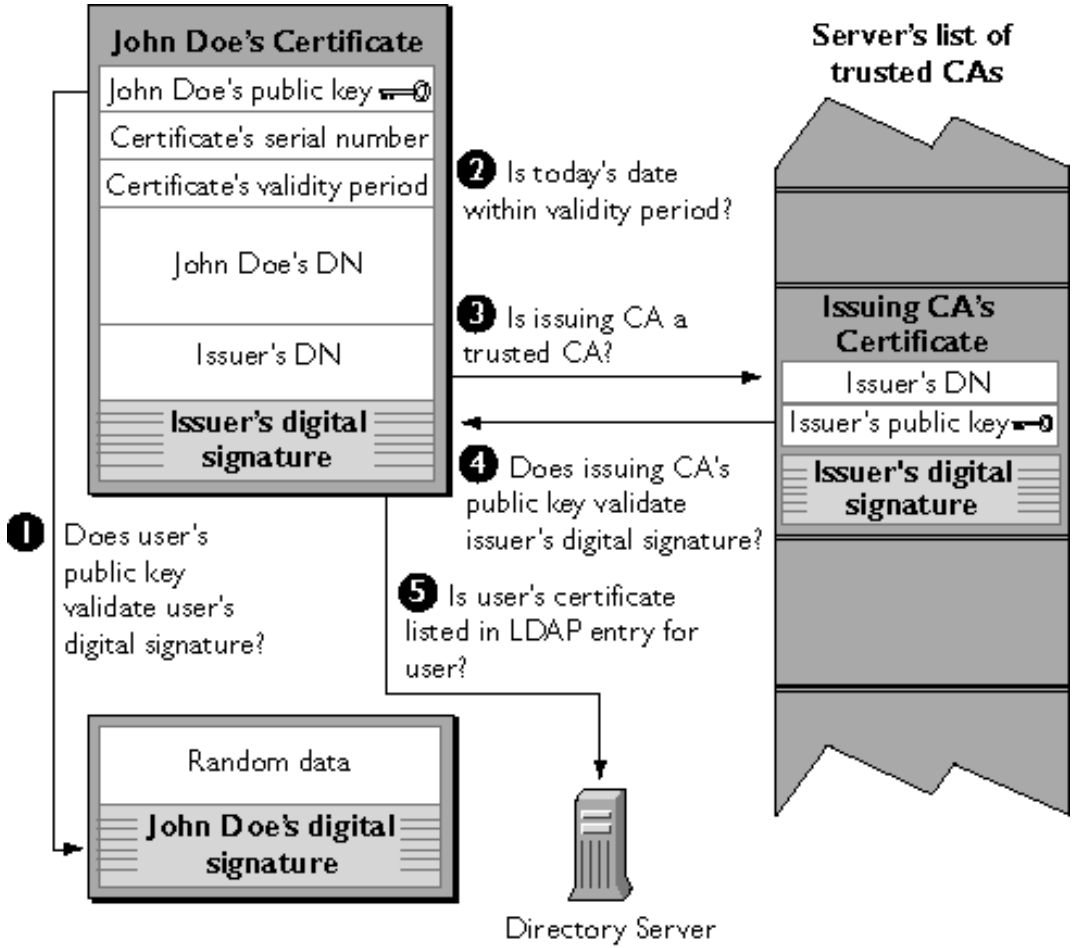
SSL - *cipher suites*



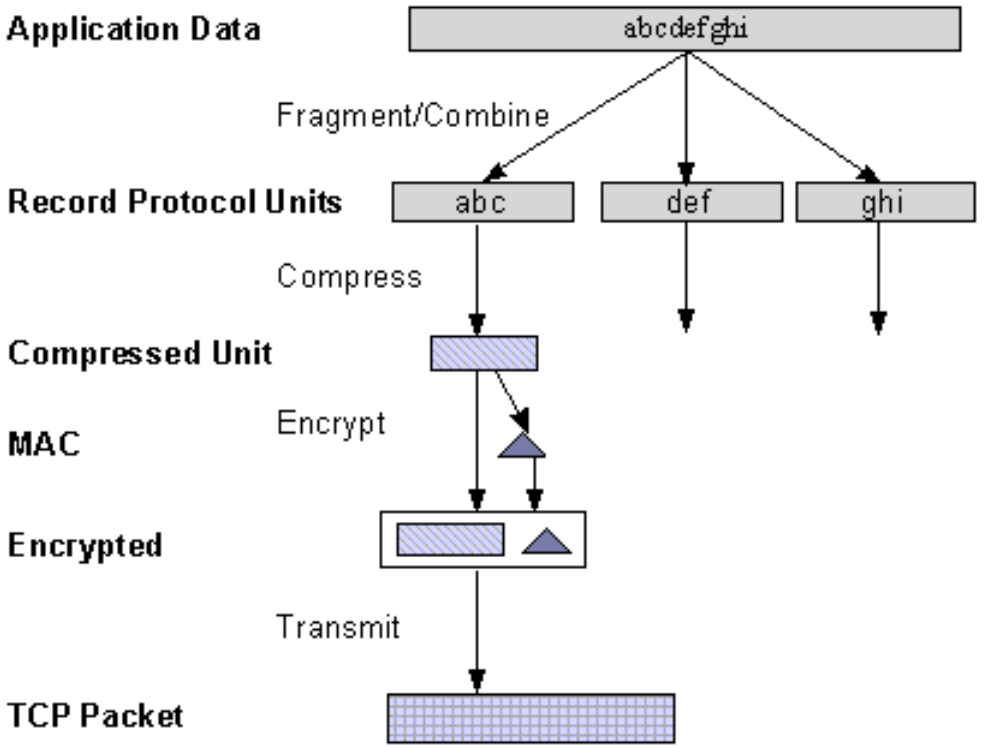
SSL - autenticação de servidor



SSL - autenticação de cliente



SSL (Record protocol)



Secure SHell (SSH)

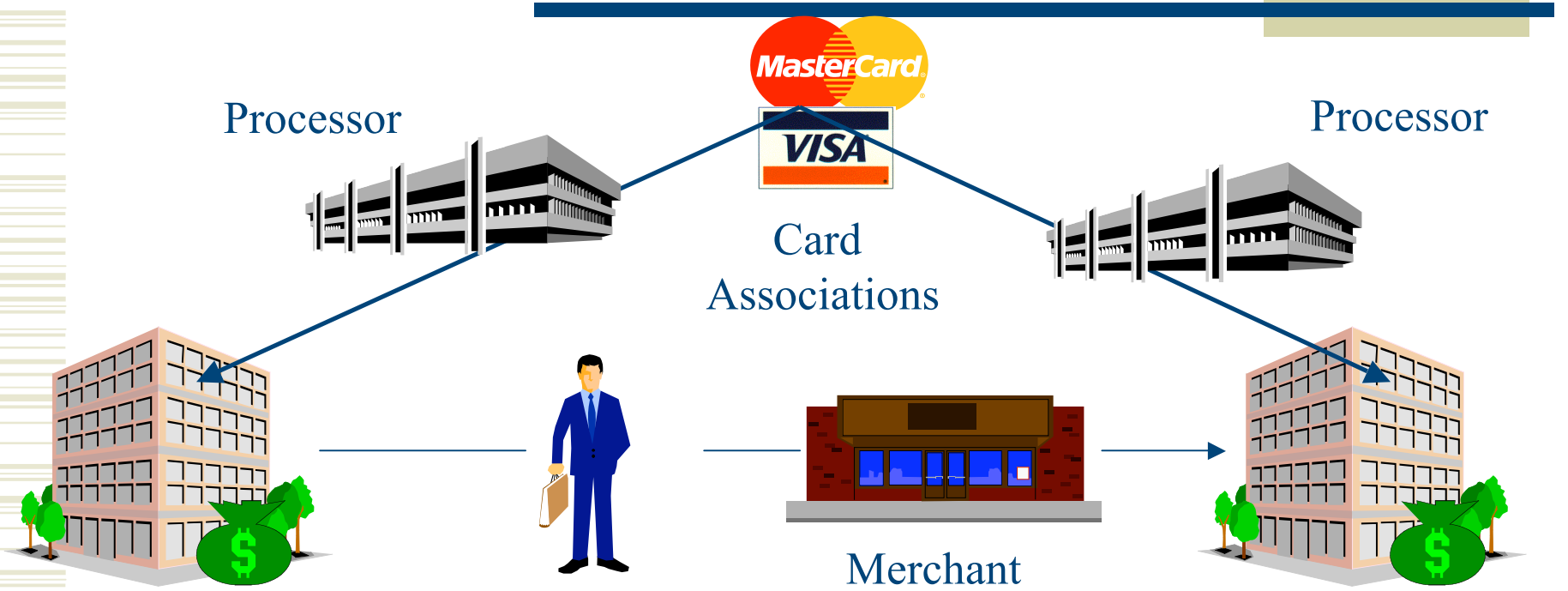
- Substituto seguro para *rsh* (...e *rlogin, telnet, ftp*)
- Utiliza técnicas criptográficas fortes para autenticação da máquina e, opcionalmente, do utilizador.
- Permite encapsular *sockets* (*port forwarding)* disponibilizando uma forma expedita para tornar seguro serviços existentes (e.g. *X11 tunneling*)
- Em V1, chave de sessão é gerada pelo cliente. EmV2, é utilizado o acordo de chaves *Diffie-Hellman* e é permitida a utilização de certificados próprios, X509v3 ou OpenPGP.

Secure Electronic Transactions (SET)

- Standard para transacções comerciais electrónicas desenvolvido pela VISA e MasterCard (evolução e standard proprietários desses grupos).
- Faz uso de certificados X509, utilizando uma hierarquia e certificação própria.

- ... penetração no mercado bastante lenta ... (...comércio electrónico parece contentar-se com transmissão dos números de cartão de crédito cifrados numa sessão SSL...)

SET (cont.)



- Issuing Bank
- Issues card
- Extends credit
- Assumes risk of card
- Cardholder reporting

- Merchant Bank (Acquirer)
- Sets up merchant
- Extends credit
- Assumes risk of merchant
- Funds merchant

SET (cont.)

Browsing

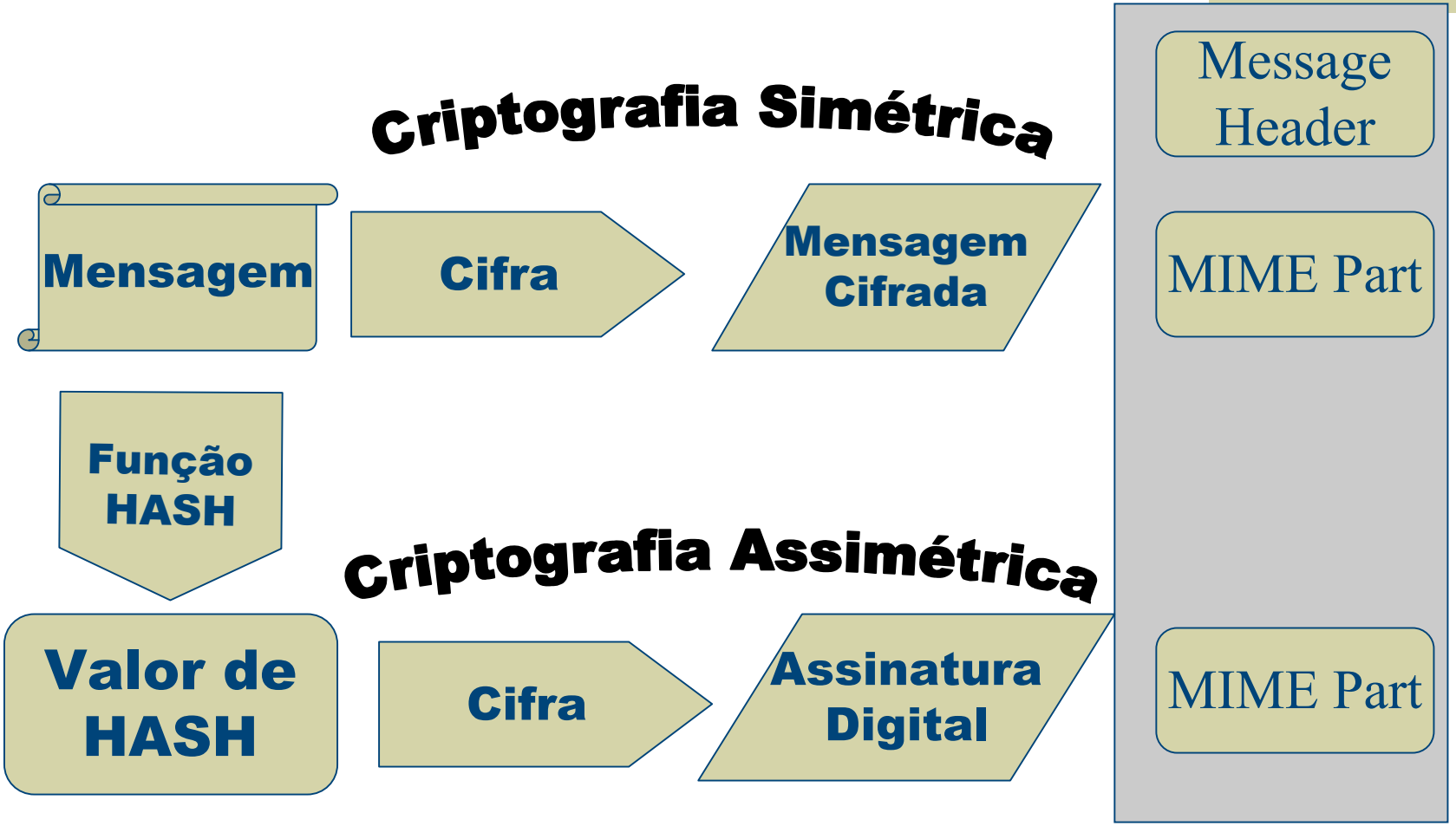
2. Product selection
3. Customer order entry
4. Selection of payment mechanism
5. **Customer sends order and payment instructions**
6. **Merchant requests payment authorization**
7. **Merchant sends order confirmation**
8. Merchant ships goods
9. **Merchant requests payment from bank**

SET PROTOCOL FUNCTIONS:

S/MIME

- Extensão ao MIME (*Multi-propose Internet Mail Extensions*) que possibilita o envio de mensagens assinadas e/ou cifradas por correio electrónico.
- Originalmente desenvolvido por RSA Labs, mas posteriormente adoptado como standard.
- Utiliza certificados X509 (logo, dependente de uma infra-estrutura de chave pública).
- Suportado pelas principais ferramentas de mail.

S/MIME


Criptografia Simétrica
Mensagem
Cifra
Mensagem Cifrada
Função HASH
Criptografia Assimétrica
Valor de HASH
Cifra
Assinatura Digital
Message Header
MIME Part
MIME Part

Pretty Good Privacy (PGP)

- Programa desenvolvido por *P. Zimmerman* com o intuito de disponibilizar uma ferramenta de correio electrónico efectivamente segura (...com "ciprografia forte")
- Utiliza cifras de domínio público (e.g. IDEA) como forma de evitar licenças sobre algoritmos patenteados.
- Exportado dos EU na forma de livro...
- Faz uso de um esquema de certificação "original" - *web-of-trust.*

S/MIME Vs PGP

Mandatory features	S/MIME v3	OpenPGP
Message format	Binary, based on CMS	Binary, based on previous PGP
Certificate format	Binary, based on X.509v3	Binary, based on previous PGP
Symmetric encryption algorithm	TripleDES (DES EDE3 CBC)	TripleDES (DES EDE3 CFB)
Signature algorithm	Diffie-Hellman (X9.42) with DSS	ElGamal (Diffie Hellman) with DSS
Hash algorithm	SHA-1	SHA-1
MIME encapsulation of signed data	Choice of multipart/signed or CMS format	multipart/signed with ASCII armor
MIME encapsulation of encrypted data	application/pkcs7-mime	multipart/encrypted