Tim Matthews,
Director, Product Marketing

Crypto 301: Practical Implementations of Cryptography

RSA SECURITY

Problem #1

Clear understanding of the need for security…

...But no security architecture

RSA SECURITY

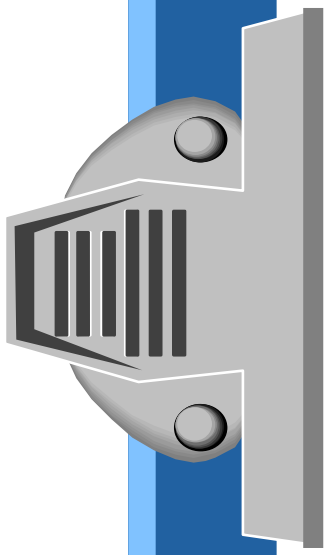
Problem #2

Rough security architecture design...

…No detailed implementation path

RSA SECURITY

Task List



0) Get a grip on security

1) Home Banking Application

2) Secure Messaging Client

RSA SECURITY

ÂrÒÞú/{N`vÝ

#K]r·G¥ì•ûÈÉ©¡d5þfÌë0‡:„®GBi8ïû(¤DG¹Ü±–

î…, Zwø„Ûá¥×>³¬&—Ú«AÂÄuÍª“
ÖüTOµƒ‘A[tiBçw±ðÇõkfxCUF½qx2t¸¬_•(4s/
4 >„Èêô¥ÈGP¾šn¿yk¹tq /õx¡Ô»Öüf_p¥ê'A®
9>ªÄa&}”xGó¹âÄÐf©ß\›á„½]0ôÂ9mb×u4'Œ
WA¿«7•²~Æ¯;yMöÉmR,’I?ª*IùëFðÔ1å…ý=&

lâ,½+N Çþ«]¬’£s=f‡4ÜÂrÒÞú/{N`vÝ

#K]r·G¥ì•ûÈÉ©¡d5þfÌë0‡:„®GBi8ïû(¤DG¹Ü±–

î…, Zwø„Ûá¥×>³¬&—Ú«AÂÄuÍª“
ÖüTOµƒ‘A[tiBçw±ðÇõkfxCUF½qx2t¸¬_•(4s/

RSA SECURITY

Competitive Strategy/ Cryptography

What is Cryptography?

Cryptographer's View

- Privacy
- Data Integrity
- Authentication
- Non-Repudiation

Business View

- Trust/Comfort
- Fraud Protection
- Assent/Authentication
- Guarantee/Recourse

RSA SECURITY

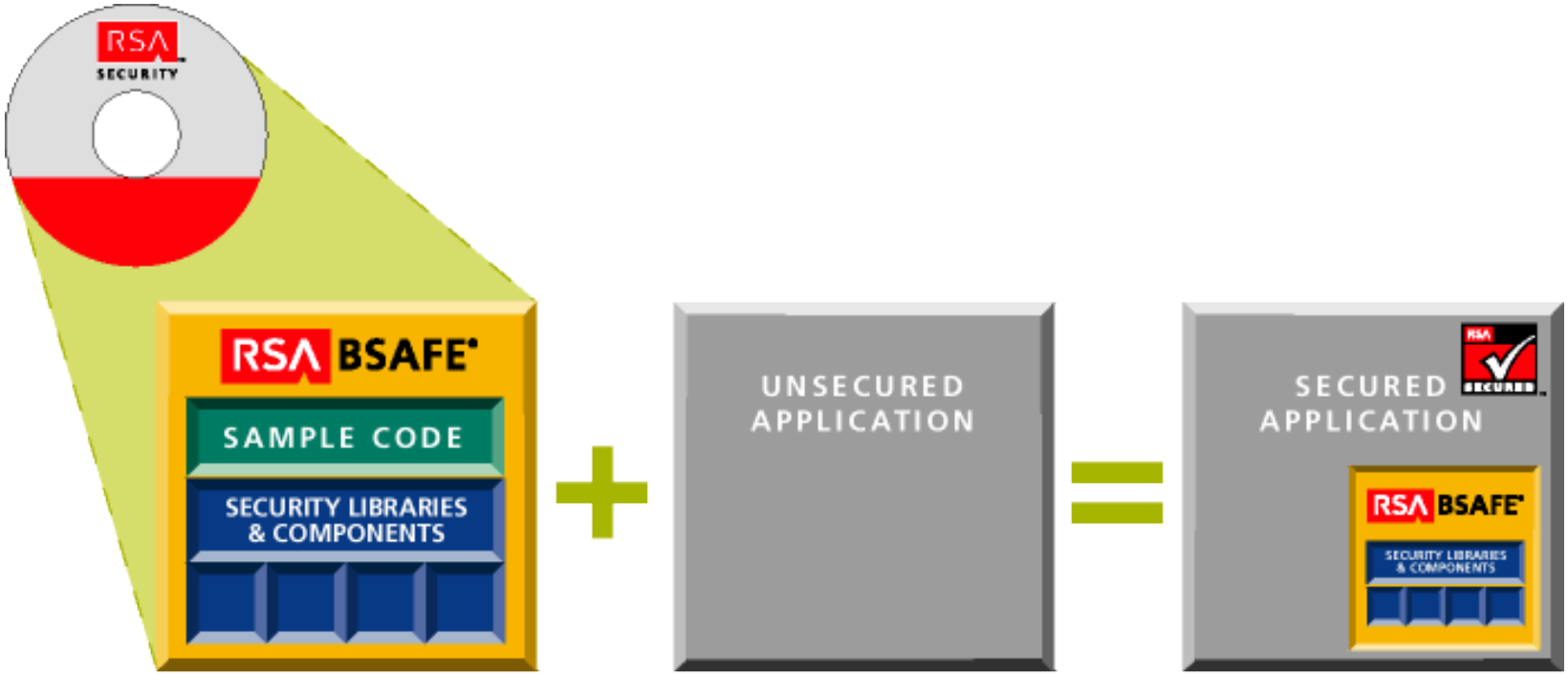
Competitive Strategy/ Cryptography

Mapping Concepts to Practices - Cryptographic Analogs

Cryptographic Construct		Result
◆ Digital Envelope	⇒	◆ Privacy, Protection
◆ Digital Signature	⇒	◆ Assent, Authorization, Integrity
◆ Digital Certificate	⇒	◆ Identity

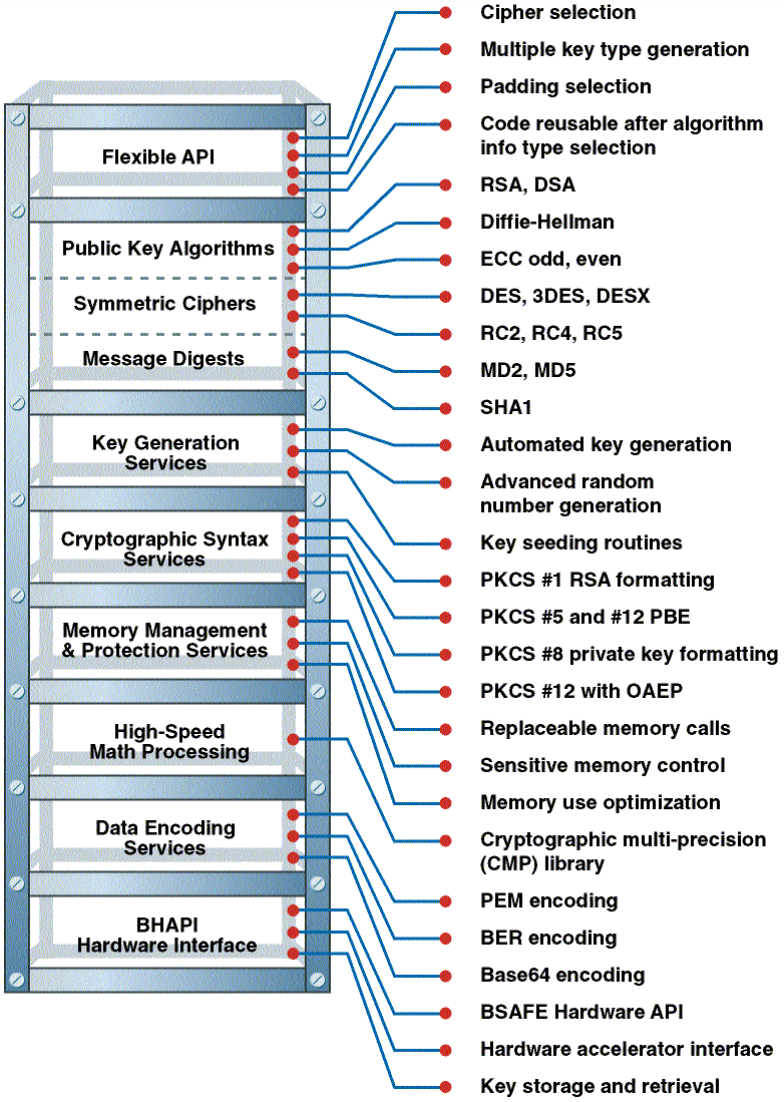
RSA SECURITY

Building in Security



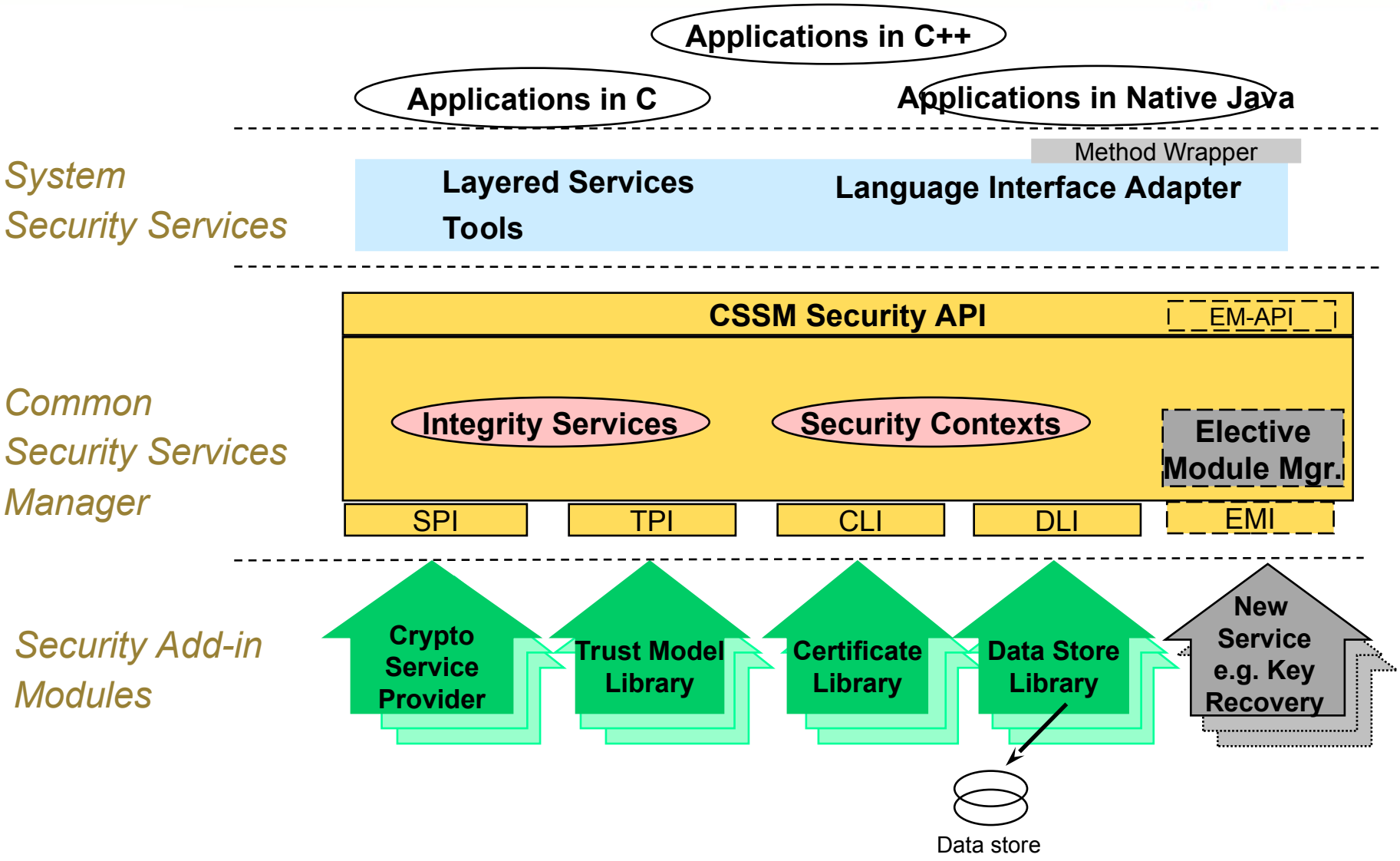
RSA SECURITY

Inside a Crypto Stack

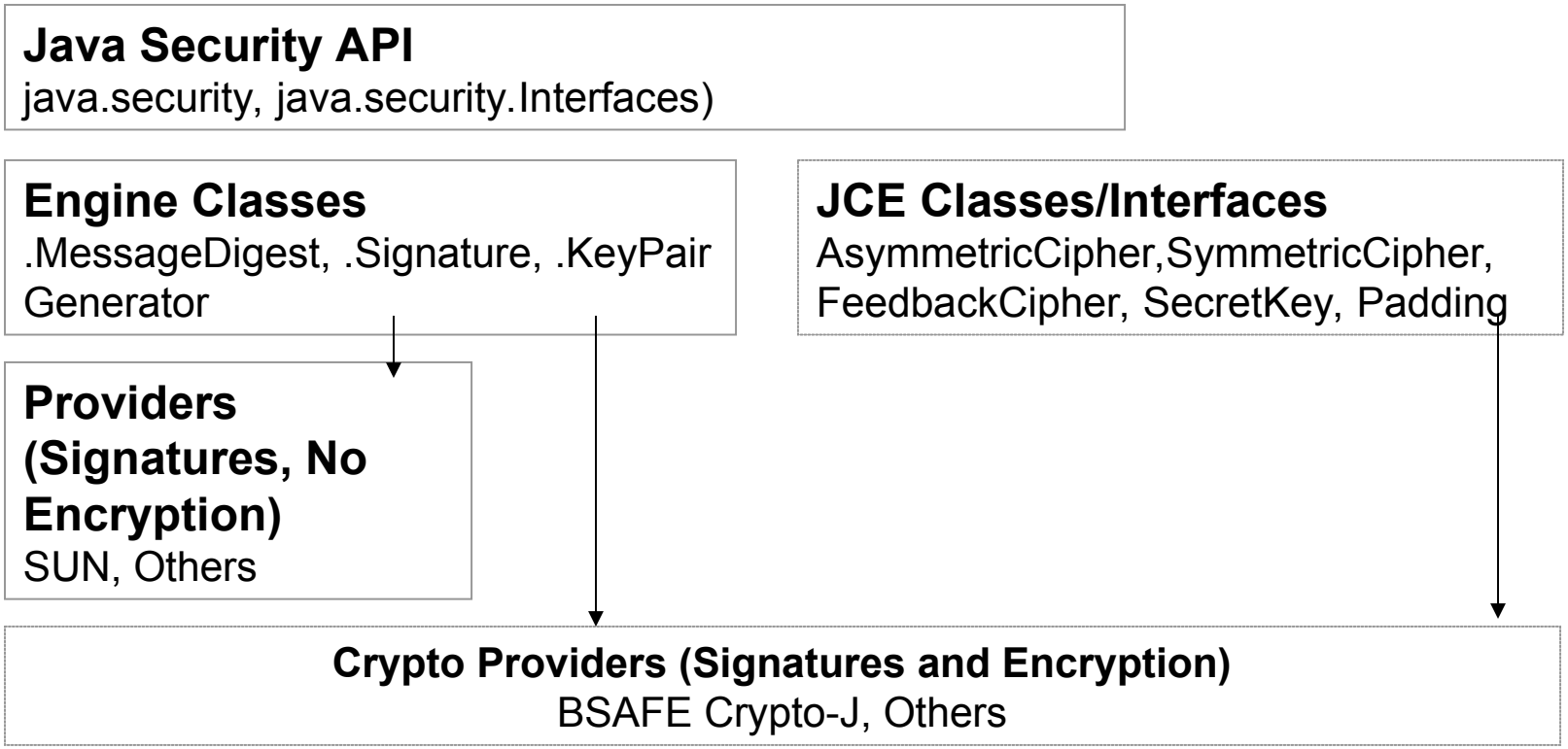


RSA SECURITY

CDSA

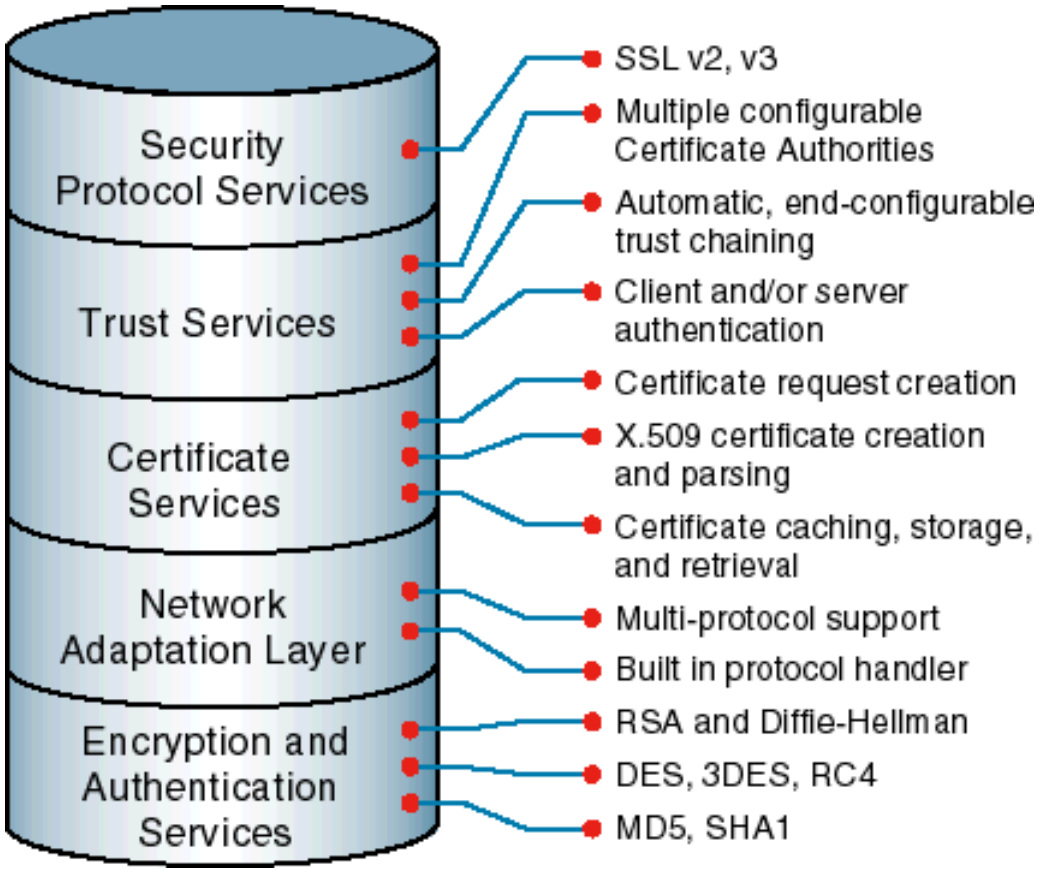

Applications in C++
Applications in C
Applications in Native Java
System Security Services
Method Wrapper
Layered Services
Tools
Language Interface Adapter
Common Security Services Manager
CSSM Security API
EM-API
Integrity Services
Security Contexts
Elective Module Mgr.
SPI
TPI
CLI
DLI
EMI
Security Add-in Modules
Crypto Service Provider
Trust Model Library
Certificate Library
Data Store Library
New Service e.g. Key Recovery
Data store

The Java Security Model



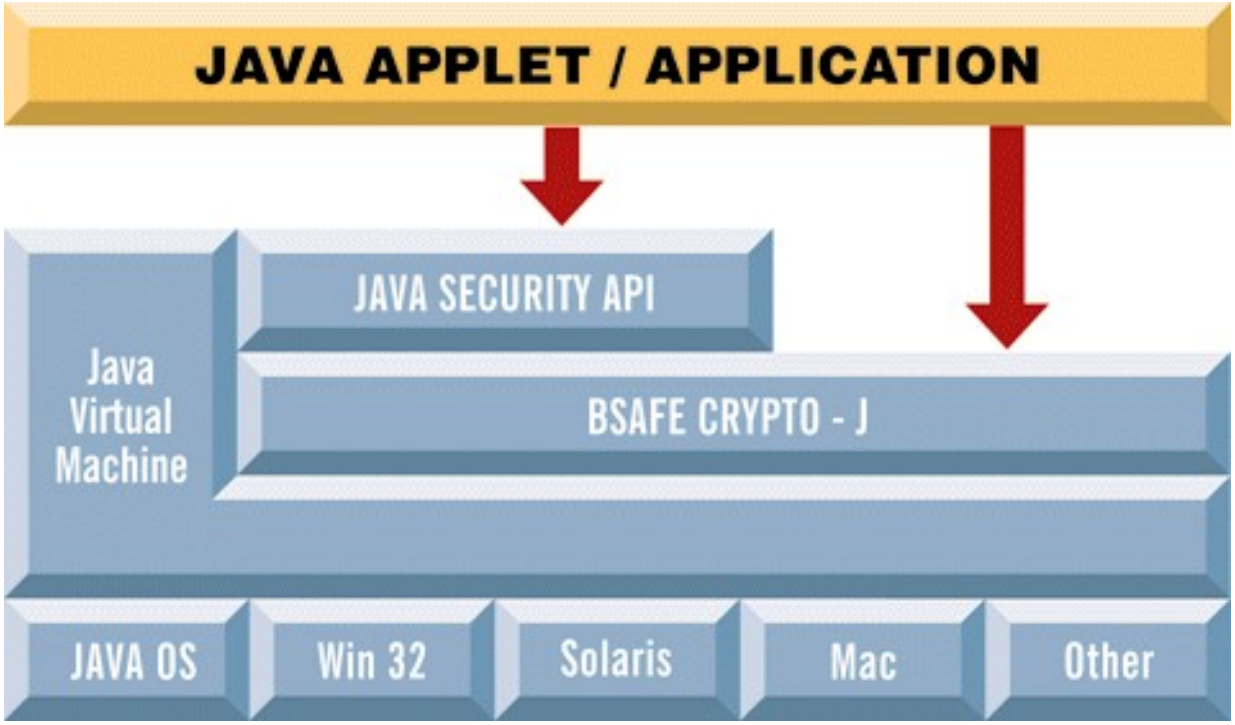
RSA SECURITY

Functional Layers for SSL



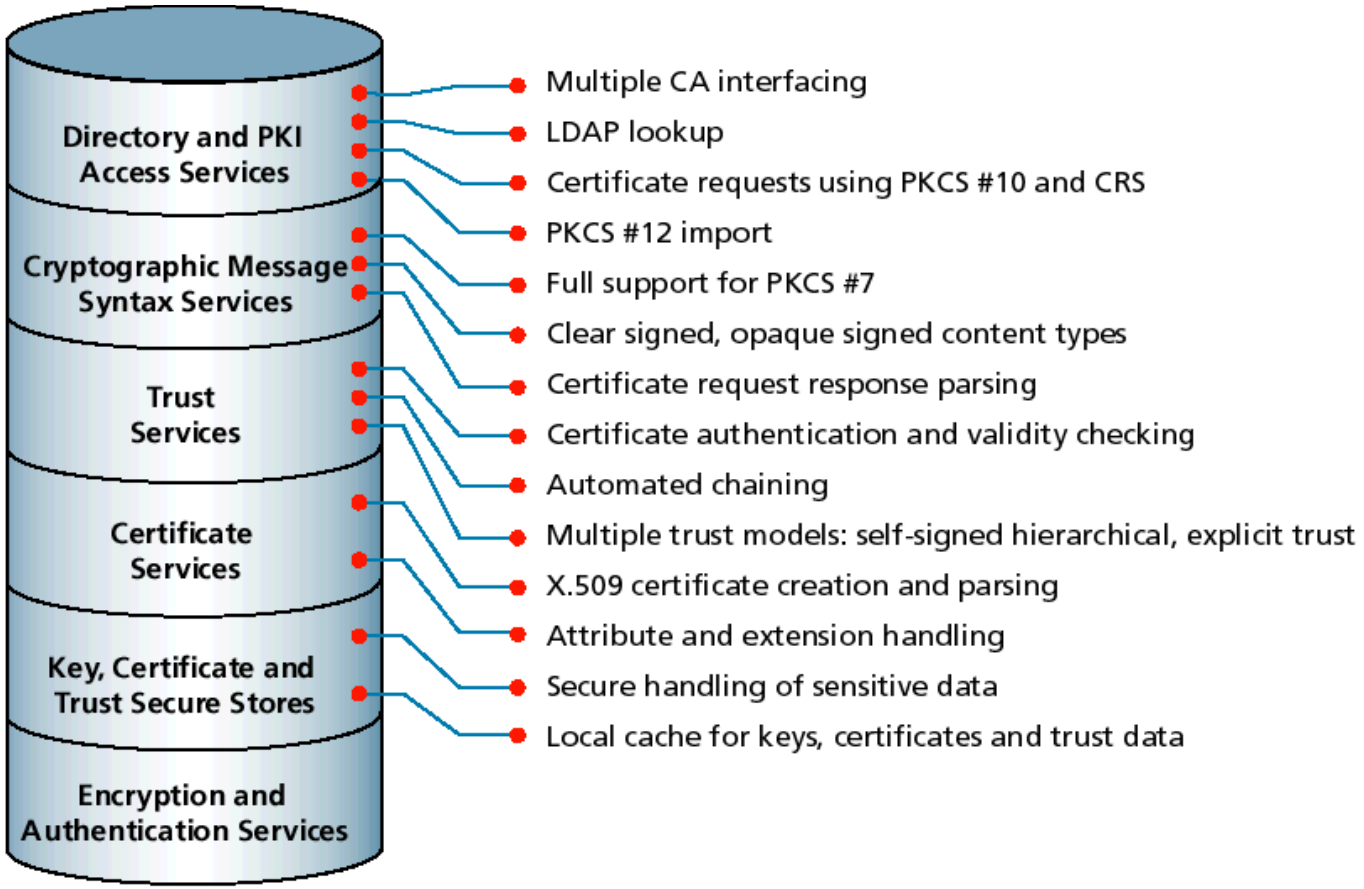
RSA SECURITY

A Crypto Provider Example



RSA SECURITY

Functional Layers for PKI-Enabling



RSA SECURITY

ÂrÒÞú/{N`vÝ

#K]r·G¥ì•ûÈÉ©¡d5þfÌë0‡:„®GBi8ïû(¤DG¹Ü±–

î…, Zwø„Ûá¥×>³¬&—Ú«AÂÄuÍª“
ÖüTOµƒ‘A[tiBçw±ðÇõkfxCUF½qx2t¸¬_•(4s/
4 >„Èêô¥ÈGP¾šn¿yk¹tq /õx¡Ô»Öüf_p¥ê'A®
9>ªÄa&}”xGó¹âÄÐf©ß\›á„½]0ôÂ9mb×u4'Œ
WA¿«7•²~Æ¯;yMöÉmR,’I?ª*IùëFðÔ1å…ý=&

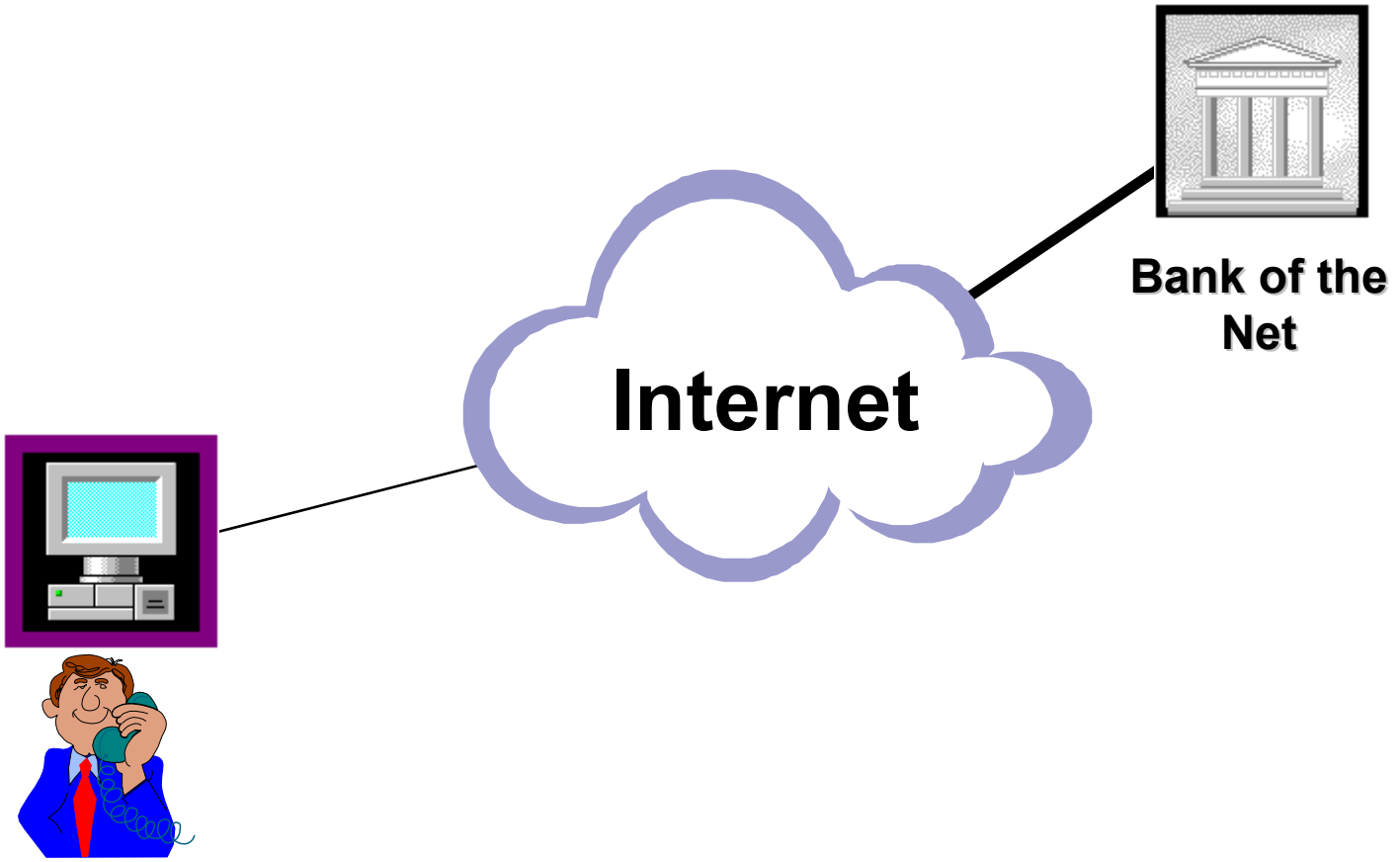
lâ,½+N Çþ«]¬’£s=f‡4ÜÂrÒÞú/{N`vÝ

#K]r·G¥ì•ûÈÉ©¡d5þfÌë0‡:„®GBi8ïû(¤DG¹Ü±–

î…, Zwø„Ûá¥×>³¬&—Ú«AÂÄuÍª“
ÖüTOµƒ‘A[tiBçw±ðÇõkfxCUF½qx2t¸¬_•(4s/

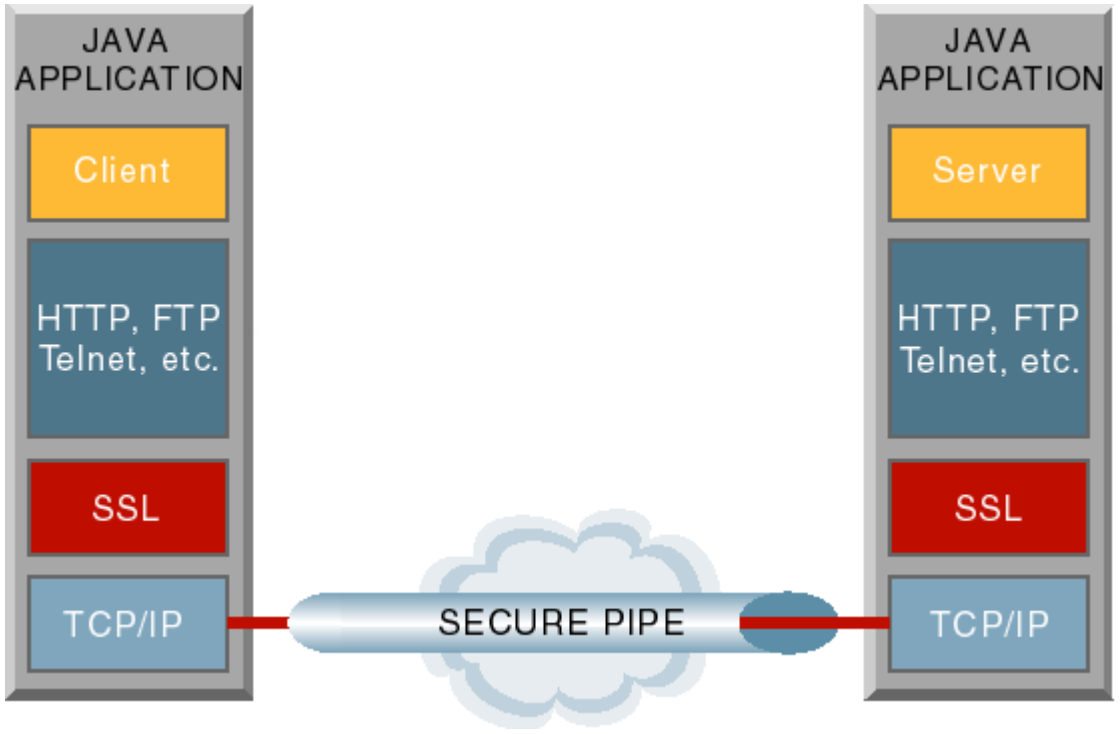
RSA SECURITY

Task #1:
Home Banking Client/Server



RSA SECURITY

SSL in Java



RSA SECURITY

Electronic Banking Application: Needs

- Link Security
- Authentication Based on Account #'s
- Message Integrity
- Moderate Amount of Traffic

RSA SECURITY

Electronic Banking Application: Constructs

- Key Exchange **Diffie-Hellman**
- Symmetric Encryption **Triple-DES**
- Message Digest **SHA-1**

RSA SECURITY

BSAFE SSL-J API Calls

- `SSLParams.setCipherSuites (new DH_With_3DES_EDE_CBC_SHA());`
- `SSLSocket.getCipherSuite();`
- `SSLParams.setCertificateAndKey();`
- `SSLSocket.getPeerCertificateChain();`

- To initiate an SSL session, use
- `getInputStream()`
- To encrypt and decrypt, use `write()` and `read()`

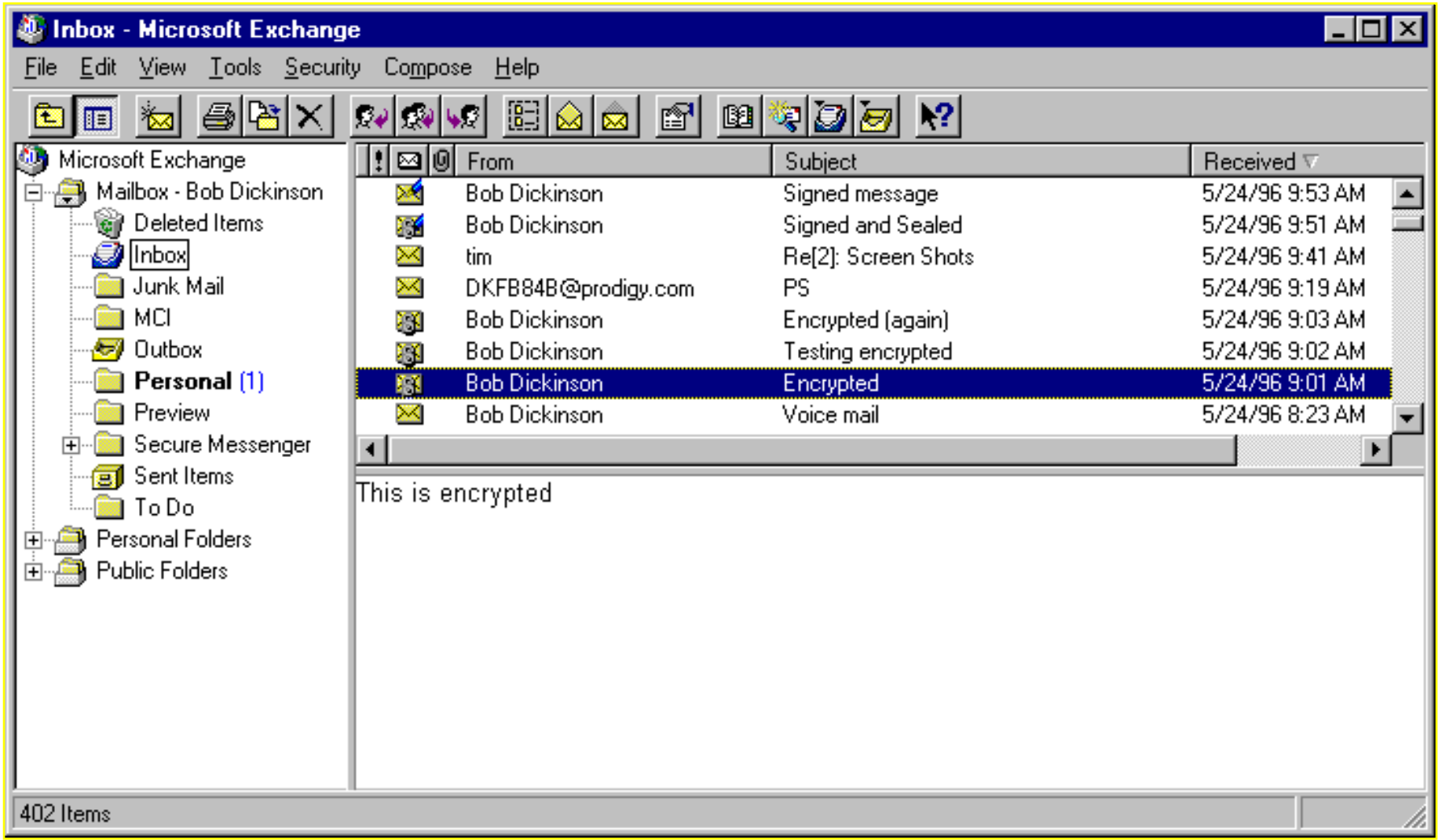
RSA SECURITY

Other Applications

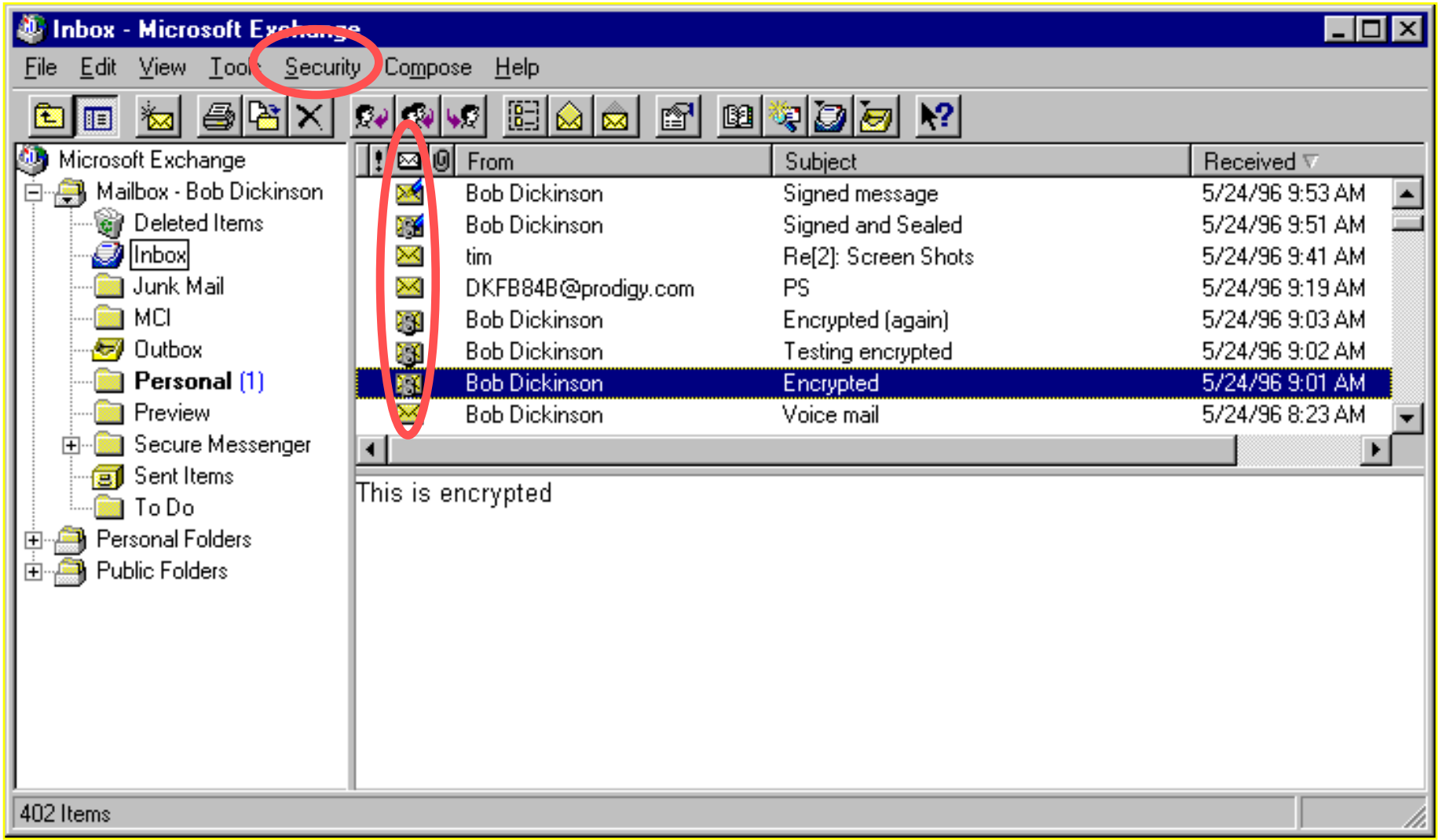
- Groupware
- Web Browser
- Internet Firewall
- Medical Record Security
- _____
- _____

RSA SECURITY

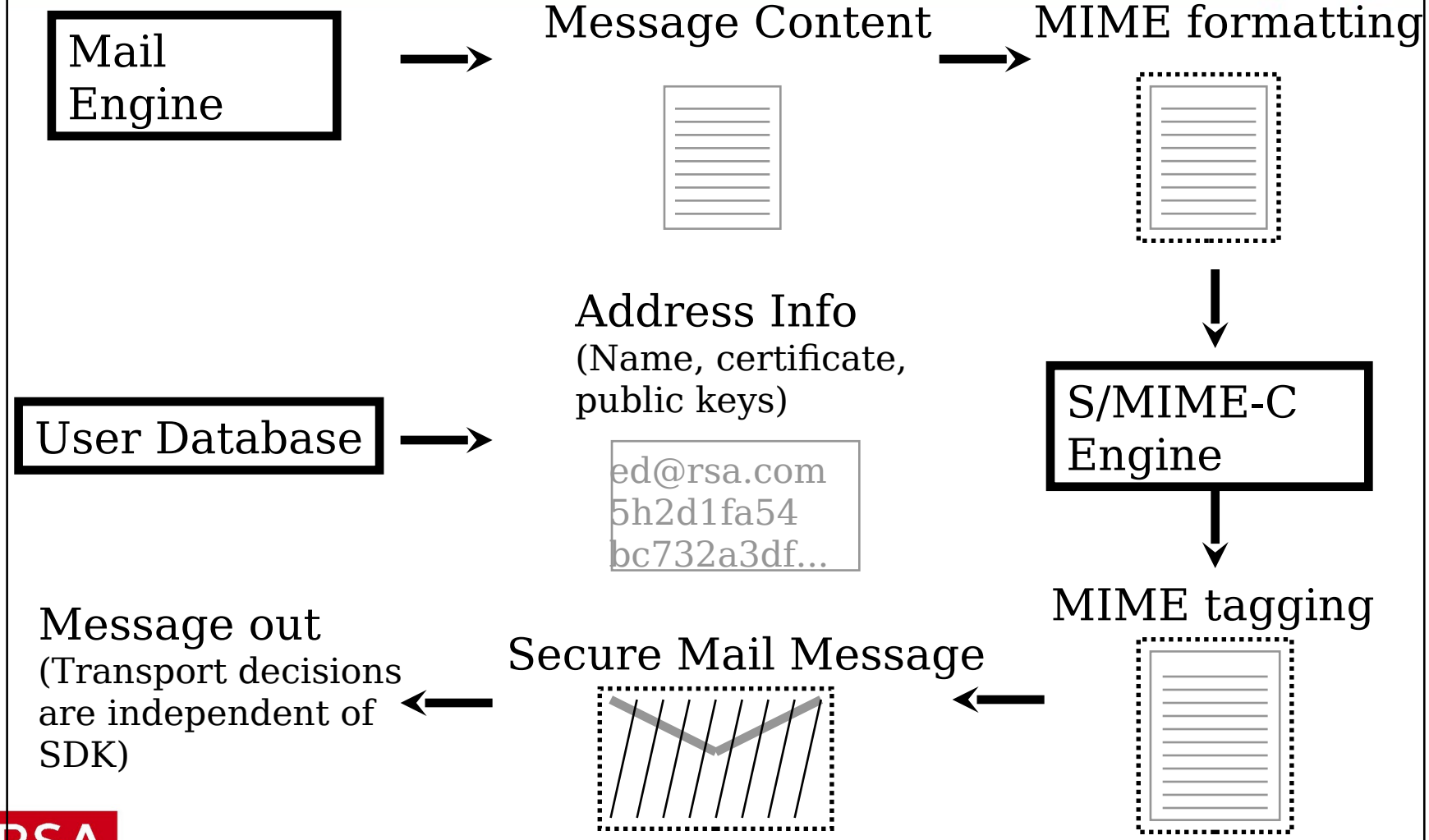
Task #2: Secure E-Mail Client



S/MIME E-Mail Client



S/MIME E-Mail Environment



RSA SECURITY

S/MIME E-mail Client: Needs

- Digital Envelopes
- Digital Signatures
- Certificate Chaining
- Certificate Requests
- Export

RSA SECURITY

S/MIME E-mail Client: Constructs

- Message Format PKCS #7
- Certificates X.509 v3
- Algorithms RSA, SHA-1, RC2, Triple-DES

RSA SECURITY

BSAFE S/MIME-C API Calls

- `SmtMsg_EncryptAndSign`
- `SmtMsg_DecryptAndVerify`
- `Also`
  - `SmtCert_EnumCerts`
  - `SmtAddress_AttachCertificate`

RSA SECURITY

Other Applications

- EDI Over Internet
- Downloading Secure Objects
- Executable Signing
- _____
- _____

RSA SECURITY

Links

- **This Presentation**
  - www.rsaconference.com/presentations/RSA00-Crypto301.ppt
- **Developing Secure Applications**
  - http://www.rsasecurity.com/developers/
- **Tim Matthews**
  - tim@rsasecurity.com

RSA SECURITY