

Building Applications Using BSAFE, BCERT & TIPEM

Tim Matthews
Senior Cryptographic Engineer
tim@rsa.com
January 30, 1997

Problem #1

*Clear understanding of the need
for security...*

...But no security architecture

Problem #2

*Rough security architecture
design...*

*...No detailed implementation
path*

The Layered Open Cryptography Toolkit (LOCT) Architecture

Application-Specific Tools

TIPEM Toolkit

S/PAY Toolkit

Certificate Engine

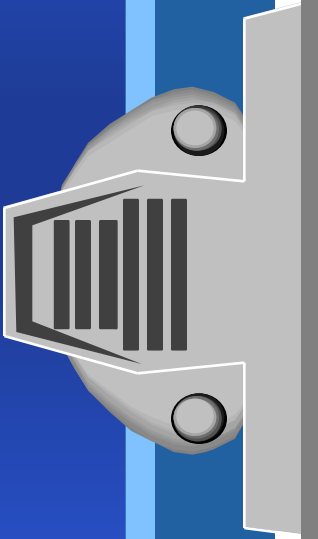
BCERT 1.0

Crypto Engine

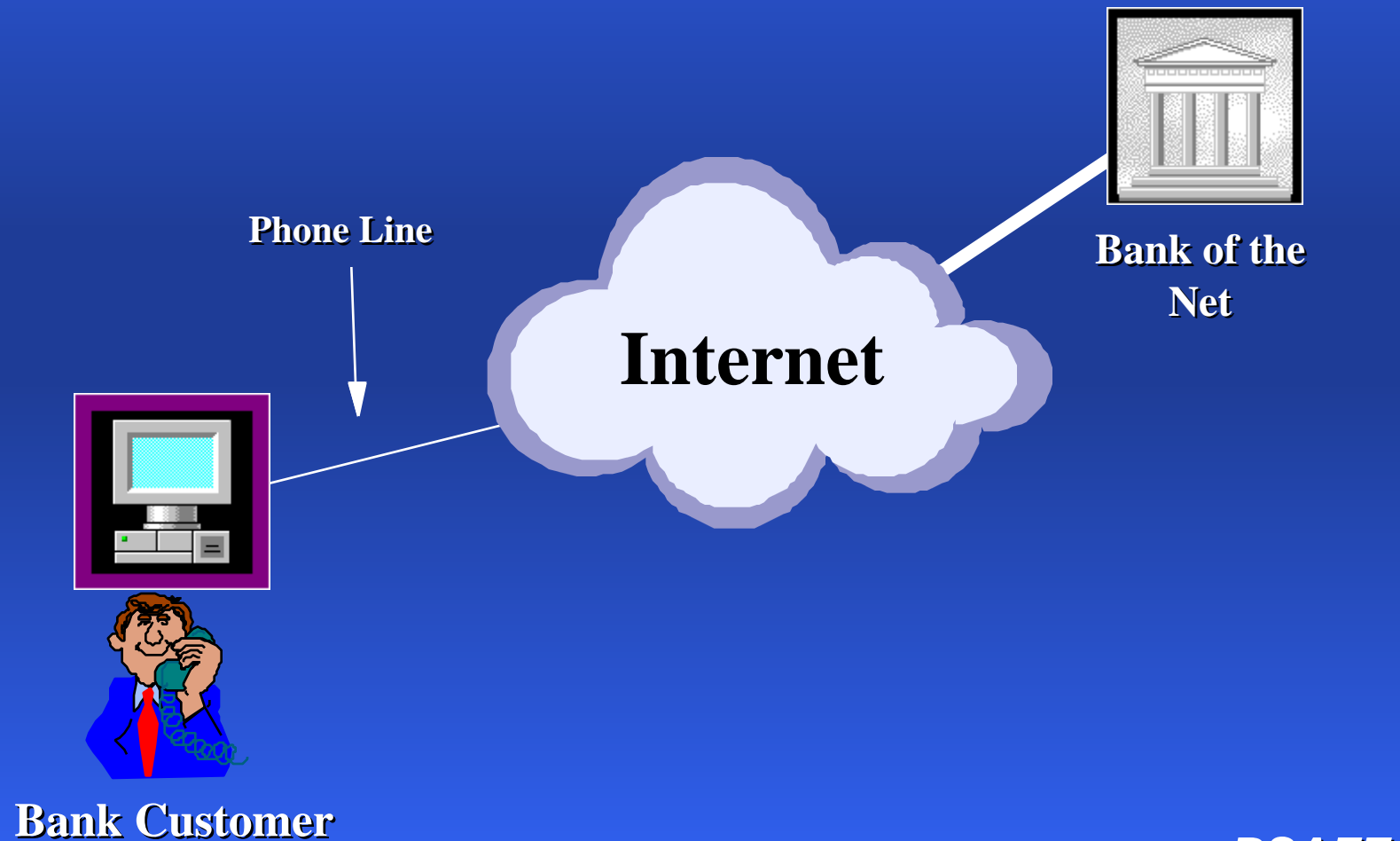
BSAFE 3.0

Hardware
Token
Interface

Task List

- 
- 1) Home Banking
Application
 - 2) Certificate Issuing
System
 - 3) S/MIME E-mail Client

Home Banking Client/Server



BSAFE

Electronic Banking Application: Needs

- ◆ **Link Security**
- ◆ **Authentication Based on Account #'s**
- ◆ **Message Integrity**
- ◆ **Moderate Amount of Traffic**
- ◆ **No Export**

BSAFE

Electronic Banking Application: Constructs

- ◆ Key Exchange _____
- ◆ Symmetric Encryption _____
- ◆ Message Digest _____

BSAFE

BSAFE API Specifics

- B_CreateAlgorithmObject
- B_SetAlgorithmInfo
- B_EncryptInit
- B_EncryptUpdate
- B_EncryptFinal
- B_DestroyKeyObject,
B_DestroyAlgorithmObject

BSAFE

Other Applications

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

BSAFE

Certificate Issuing System

IntraCert

Management GUI

Hooks to Applications

Cert Policy Rules

Basic Cert Processing

Hooks to Database

BCERT

Certificate Issuing System: Needs

- ◆ Create and Revoke Certificates
- ◆ Allow Corporate Certification
- ◆ Allow Departments to Add Custom Extensions
- ◆ Use Standard Certificates
- ◆ Interface with HR Application

BCERT

Certificate Issuing System: Constructs

- ◆ Trust Model _____
- ◆ Certificate Attributes _____
- ◆ Certificate Extensions _____
- ◆ Certificate Request Format _____
- ◆ CRLs _____

BCERT

BCERT API Specifics

- `C_CreateCertRequestObject...`
 - `Name_Object`
 - `Attributes_Object`
- `C_CreateCertObject...`
- `C_CreateCRLObject...`

BCERT

Other Applications

- ◆ Adding Certs to Applications

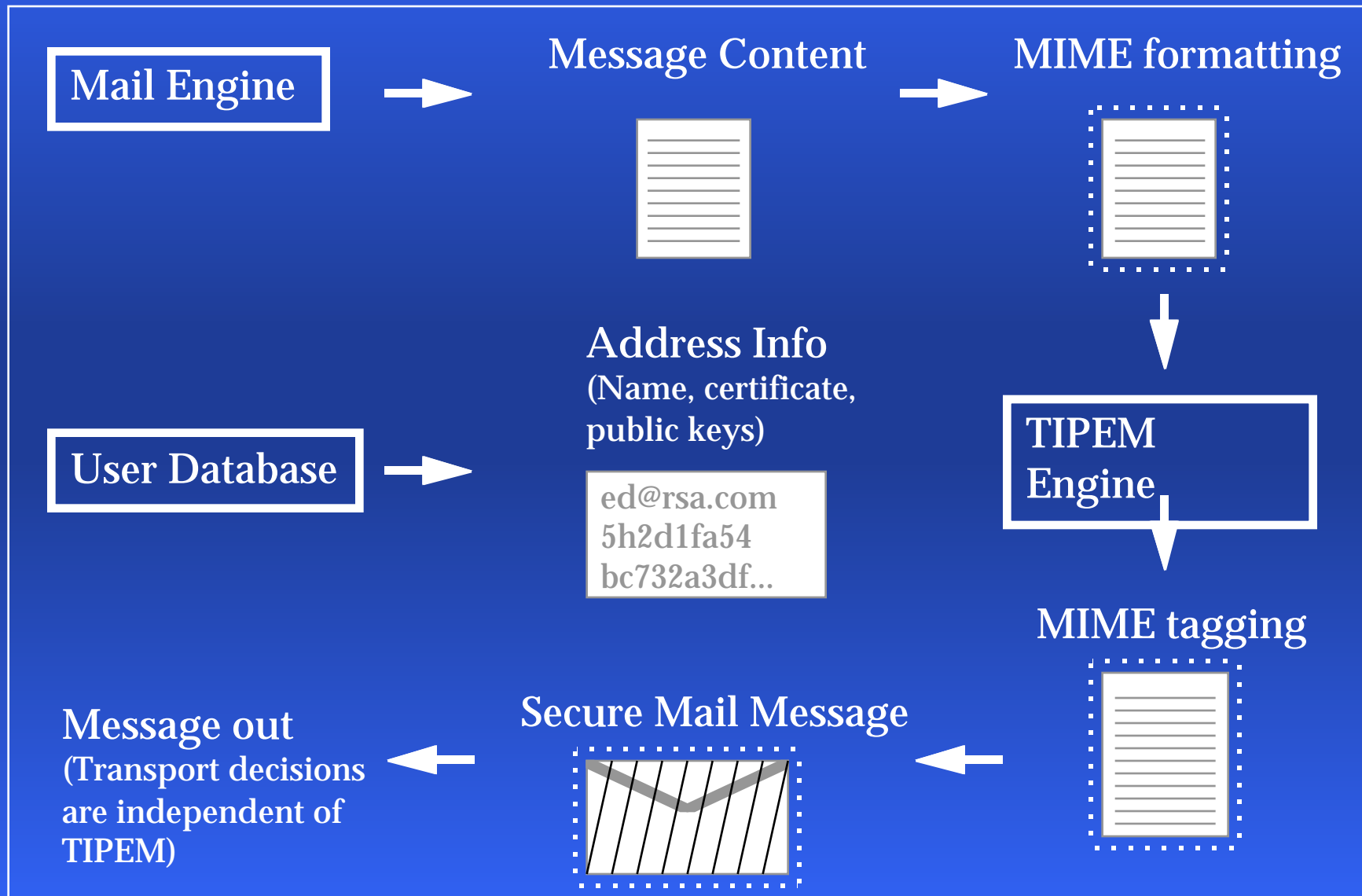
- ◆ _____

BCERT

S/MIME E-Mail Client



S/MIME E-Mail Environment



S/MIME E-mail Client: Needs

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

TIPEM

S/MIME E-mail Client: Constructs

- ◆ Message Format _____
- ◆ Certificates _____
- ◆ Algorithms _____

TIPEM

TIPEM API Specifics

- **GeneratePKCS_RSARquest**
- **PreparePKCSMessage**
- **ReceivePKCSMessage**

TIPEM

Other Applications

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

TIPEM

The Layered Open Cryptography Toolkit (LOCT) Architecture

Application-Specific Tools

TIPEM Toolkit

S/PAY Toolkit

Certificate Engine

BCERT 1.0

Crypto Engine

BSAFE 3.0

Hardware
Token
Interface



Copyright © 1996 RSA Data Security, Inc.