

Using TIPEM

Rhonda Racine
RSA Data Security Inc.
rhonda@rsa.com

RSA Data Security Conference
January 30, 1997



Topics

- What Is TIPEM?
- Getting Started
- TIPEM Building Blocks
- Message Processing



What Is TIPEM?

- TIPEM is an S/MIME application development toolkit



What is S/Mime?

- S/MIME = Secure MIME
- Integrates 2 well-established, flexible standards:
 - » **MIME** (Multi-purpose Internet Mail Extension, RFC 1521) and **PKCS**
- Goal of S/MIME is **INTEROPERABILITY** for secure messaging



S/MIME Status

- S/MIME WG formed at December IETF meeting
- S/MIME specification has been submitted to the IETF
 - » currently an RFC draft

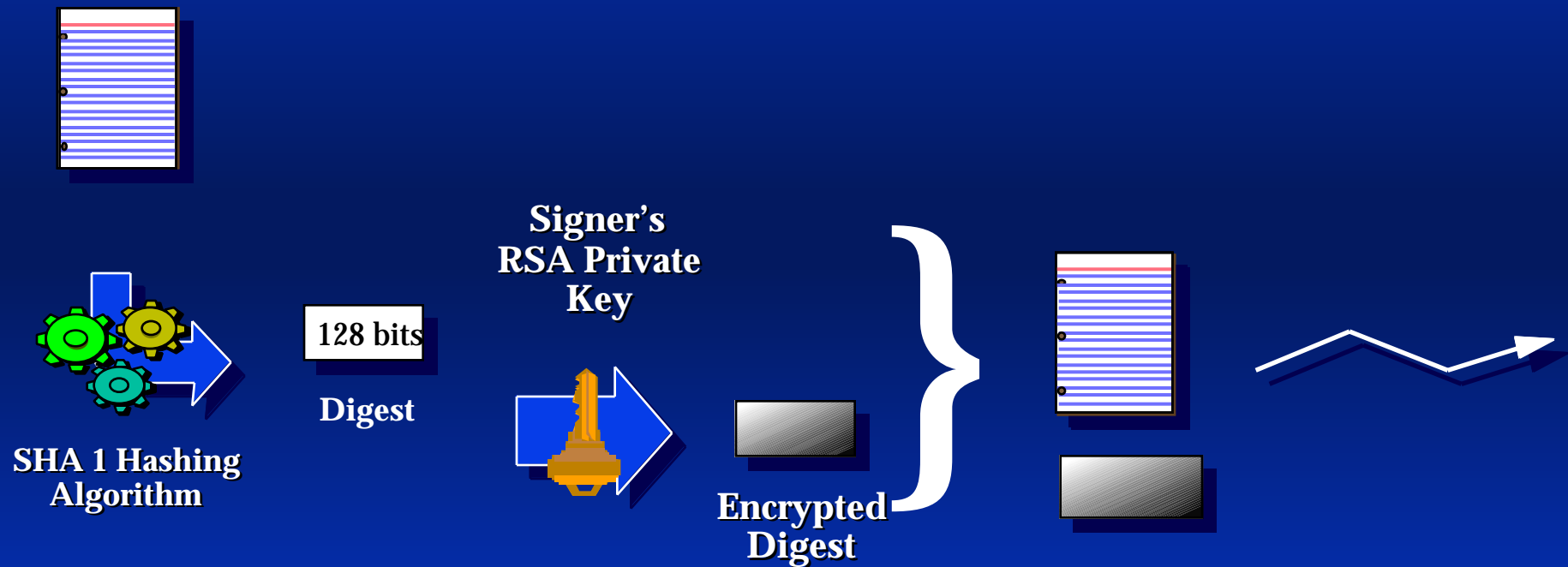


What TIPEM does

- Message integrity
- Origin authentication



Authentication: The RSA Digital Signature

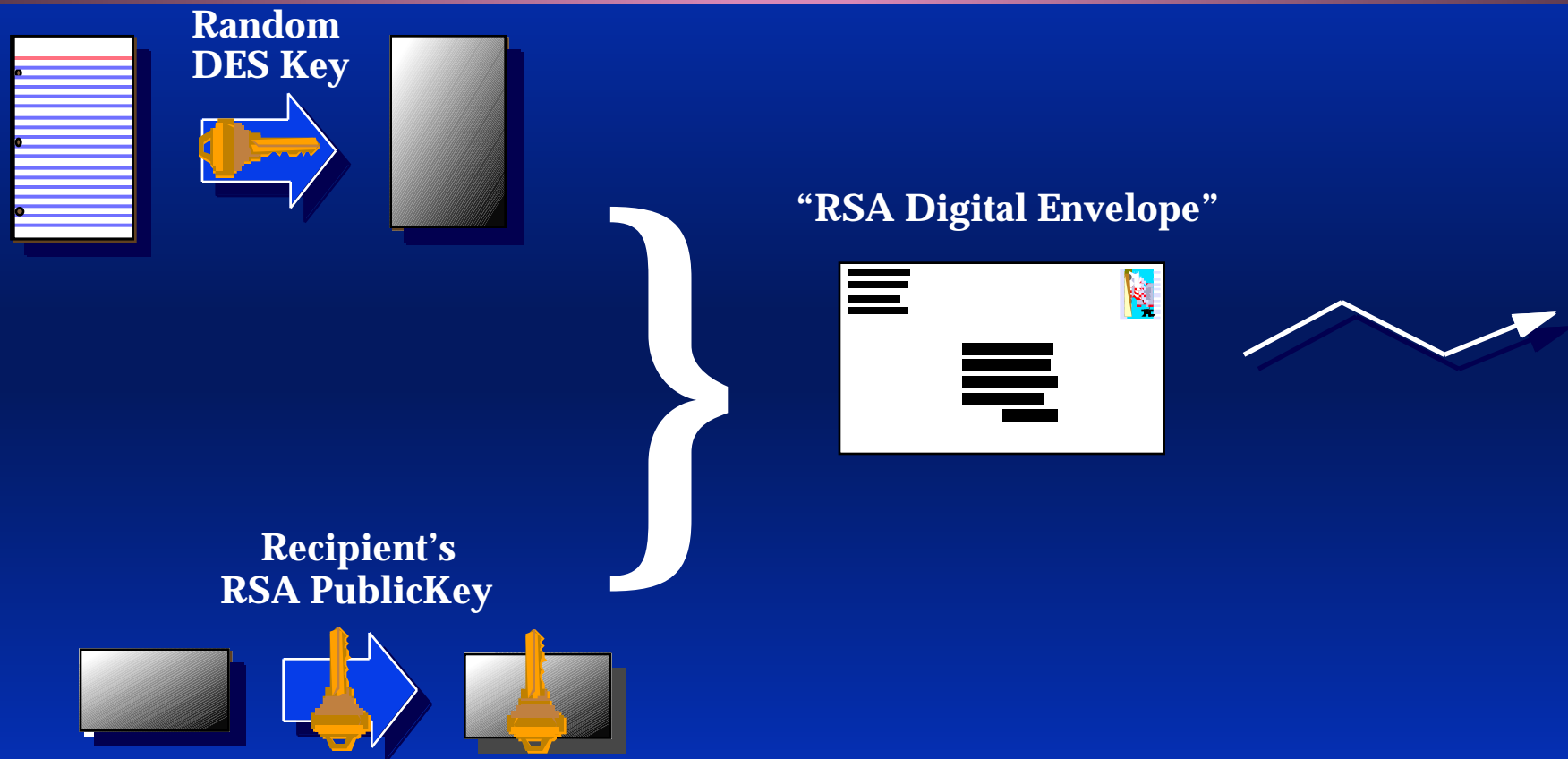


What TIPEM does

- Message integrity
- Origin authentication
- Message privacy and confidentiality



Digital Envelopes



Topics

- What Is TIPEM?
- Getting Started
- TIPEM Building Blocks
- Message Processing



Certificate

Digital Certificate

A Digital Certificate authenticates the binding between a public key and an individual, much like a company ID badge binds your name to your picture.



Getting Started

- Step 1: generate a public and private key for yourself
- Step 2: request a certificate from a Certifying Authority (CA), sending:
 - » your name
 - » your public key
 - » other information required by CA
 - » your signature



Requesting a Certificate

Input Data

“Darren Roscow”
“Martin Bishop
and Assoc.”
<public key>



private key



Object



Trust

- To establish confidence in a signer's certificate:
 - » figure out who issued it by looking at the issuer's name in the signer's certificate
 - » obtain the issuer's certificate
 - » verify the issuer's signature on the signer's certificate

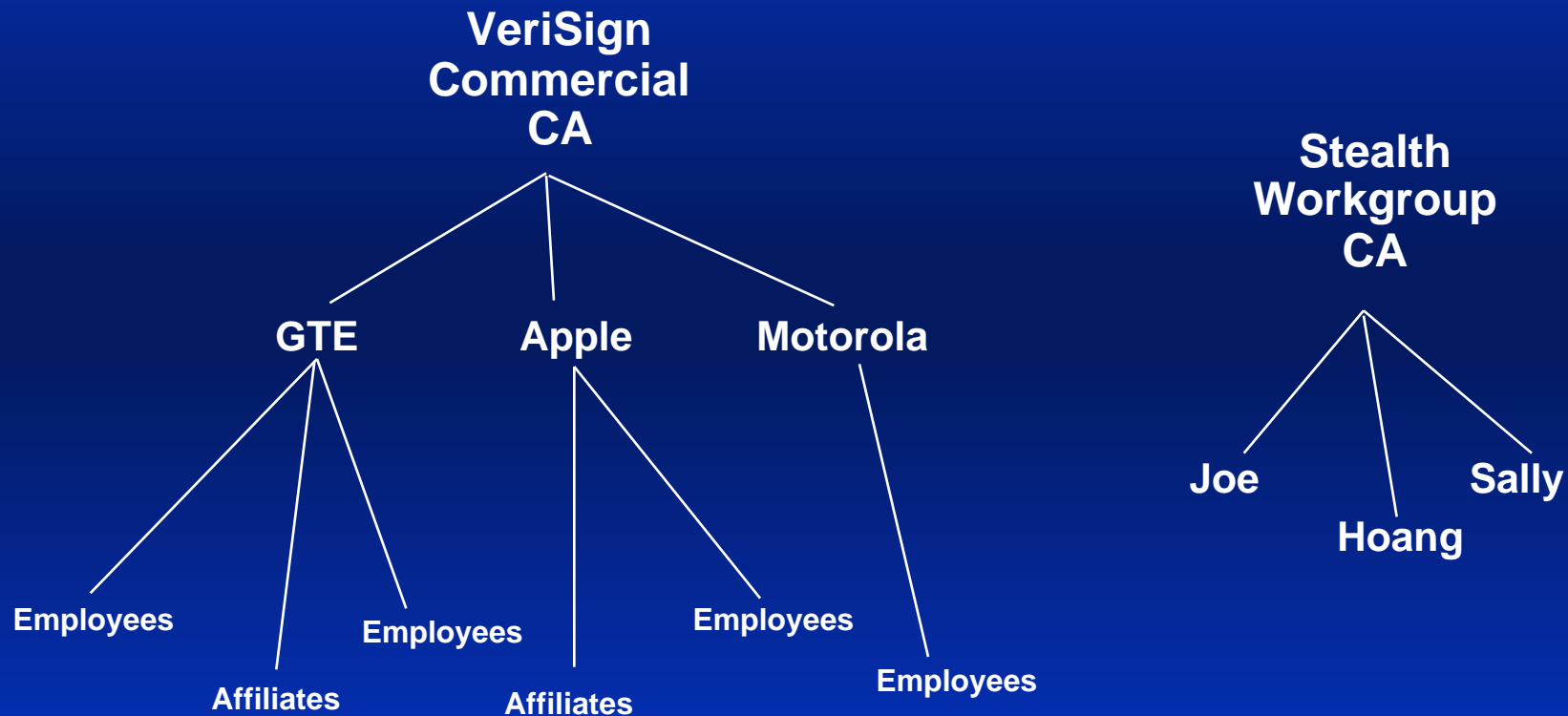


Certificate Trust Chains

- Certificate chains are a collection of certificates, where one certificate testifies to the authenticity of the previous certificate in the chain
- At the end of the chain is a top-level certification authority, called the root, with the property that it is trusted by all!



Managing Certificate Hierarchies

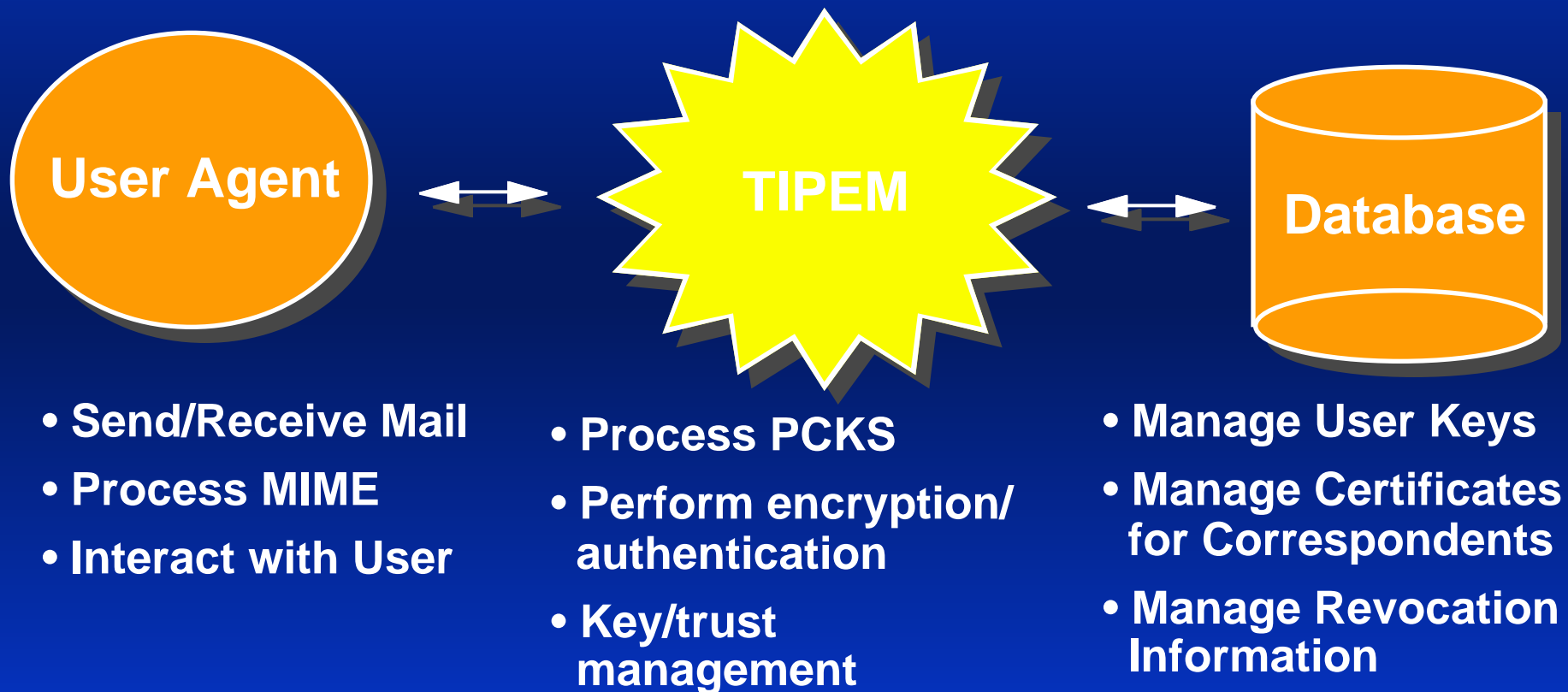


Topics

- What Is TIPEM?
- Getting Started
- TIPEM Building Blocks
- Message Processing



Implementing with TIPEM



TIPEM Building Blocks

- Message Syntax
- Name Objects
- Sets
- TIPEM Contexts
- Random Objects
- Attribute Objects



Message Syntax

- TIPEM creates and parses PKCS #7 and PKCS #10 messages.
- Cryptographic message syntax: PKCS #7
 - » digital signatures
 - » digital envelopes
- Certificate request syntax: PKCS #10



Syntax described using ASN.1 syntax notation

ASN.1, BER, DER

- Basic Encoding Rules - BER
 - » converts ASN.1 definitions into computer-readable data
 - » BER allows multiple encodings for an object
- Distinguished Encoding Rules - DER
 - » unique encoding for objects
 - » subset of BER



TIPeM and PKCS #7

- TIPeM supports the following PKCS #7 message data types:
 - » signed
 - » signed and detached
 - » enveloped
 - » signed and enveloped



Signed Message Type

- Signed

- » Message digest computed with MD5 or SHA-1
- » Syntax has a degenerate case with no signers - used for passing certificate and CRL information



Enveloped Message Type

- Message data is encrypted
- S/MIME compliance recommends:
 - RC2 and 3DES for encryption
 - RSA Public Key Cryptosystem for enveloping
- Encrypted data is then enveloped with the recipients' public keys
- Recipients use their private keys to open the envelope.

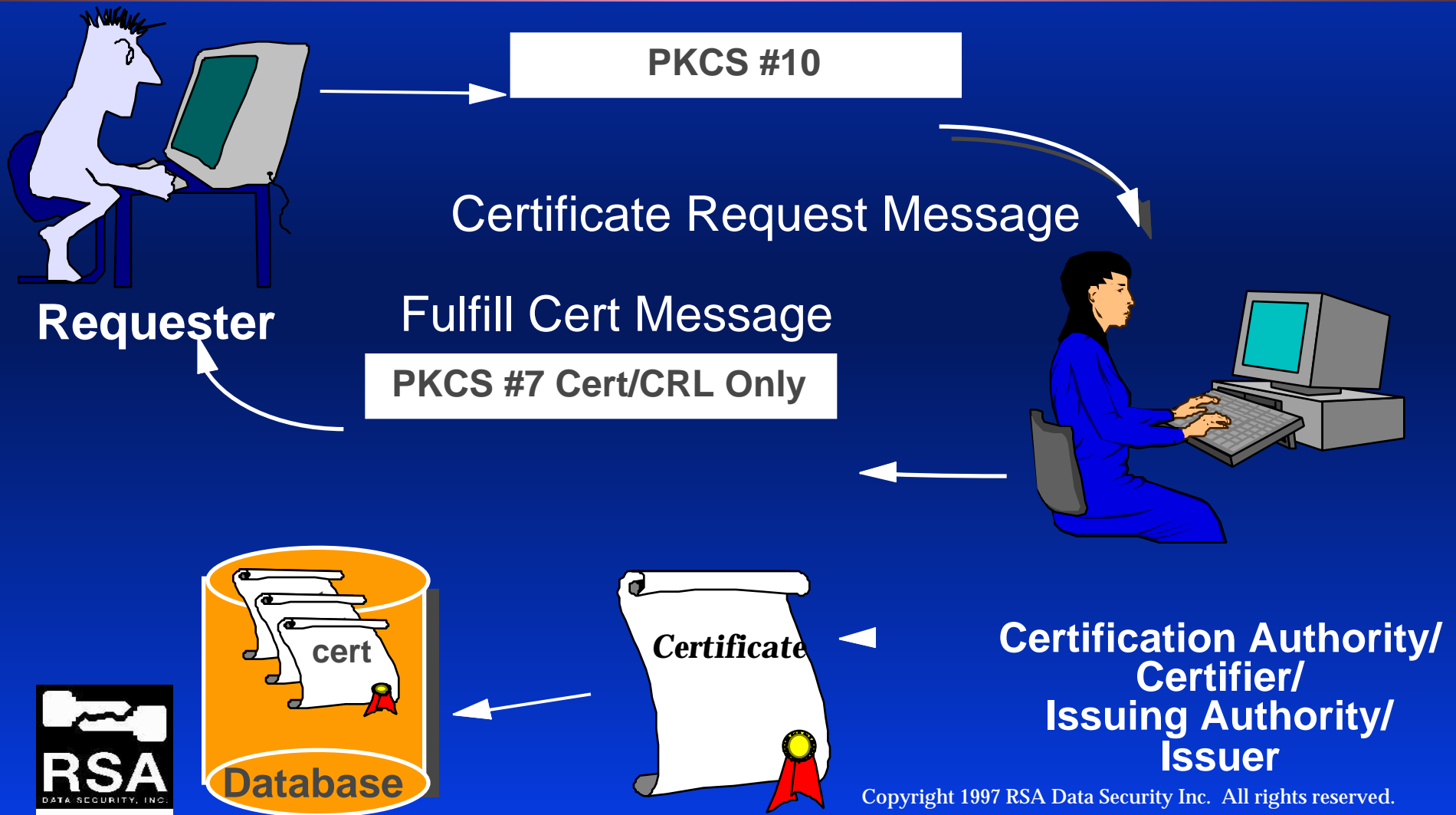


Signed and Enveloped Message Type

- Combines digital signature and digital envelope
- Similar to sequential combination of signed-data and enveloped-data
 - » S/MIME recommends sequential method: sign first, then envelope
 - signed-and-enveloped has no provision for attributes



PKCS #10: Certificate Request



TIPEM Building Blocks

- Message Syntax
- Name Objects
- Sets
- TIPEM Contexts
- Random Objects
- Attribute Objects



Name Objects

- Name Object = identity construct
- Used to represent names of entities involved in messaging
 - » recipients
 - » senders
 - » certificate authorities
- X.501 Distinguished Name



Name Objects

- Distinguished Name is presented in two equivalent forms:
 - » DER encoding
 - » a list of attribute-value assertions

objectName: myName

DER: 30 2c 31 0b ...

AVA's: "US", "RSA"



X.501 Distinguished Name

countryName = US

organizationName = RSA Data Security, Inc.

streetAddress = 100 Marine Parkway

localityName = Redwood City

stateOrProvinceName = California

postalCode = 94065

commonName = Rhonda Racine

organizationalUnitName = Engineering

title = Senior Crypto Engineer



TIPEM Building Blocks

- Message Syntax
- Name Objects
- Sets
- TIPEM Contexts
- Random Objects
- Attribute Objects



Sets

- Senders and recipients are represented with ME and YOU sets
- A set contains zero or more members for whom secure messages can be processed.



Sets

- Sets contain:
 - » certificates
 - » CRLs
 - » public keys
 - » private keys
 - » trust information (trusted roots)
 - » trust status (certificate and certificate chain status)



ME_SETS

- Potential senders of outgoing messages
- Potential recipients of incoming messages
- For each member in a ME_SET:
 - » private key information
 - » certificate and CRL chain to the trusted root



YOU_SETS

- Recipients of outgoing messages
- Senders of incoming messages
- For each member in a YOU_SET:
 - » public key information
 - » certificate and CRL chain to trusted root



TIPEM Building Blocks

- Message Syntax
- Name Objects
- Sets
- TIPEM Contexts
- Random Objects
- Attribute Objects

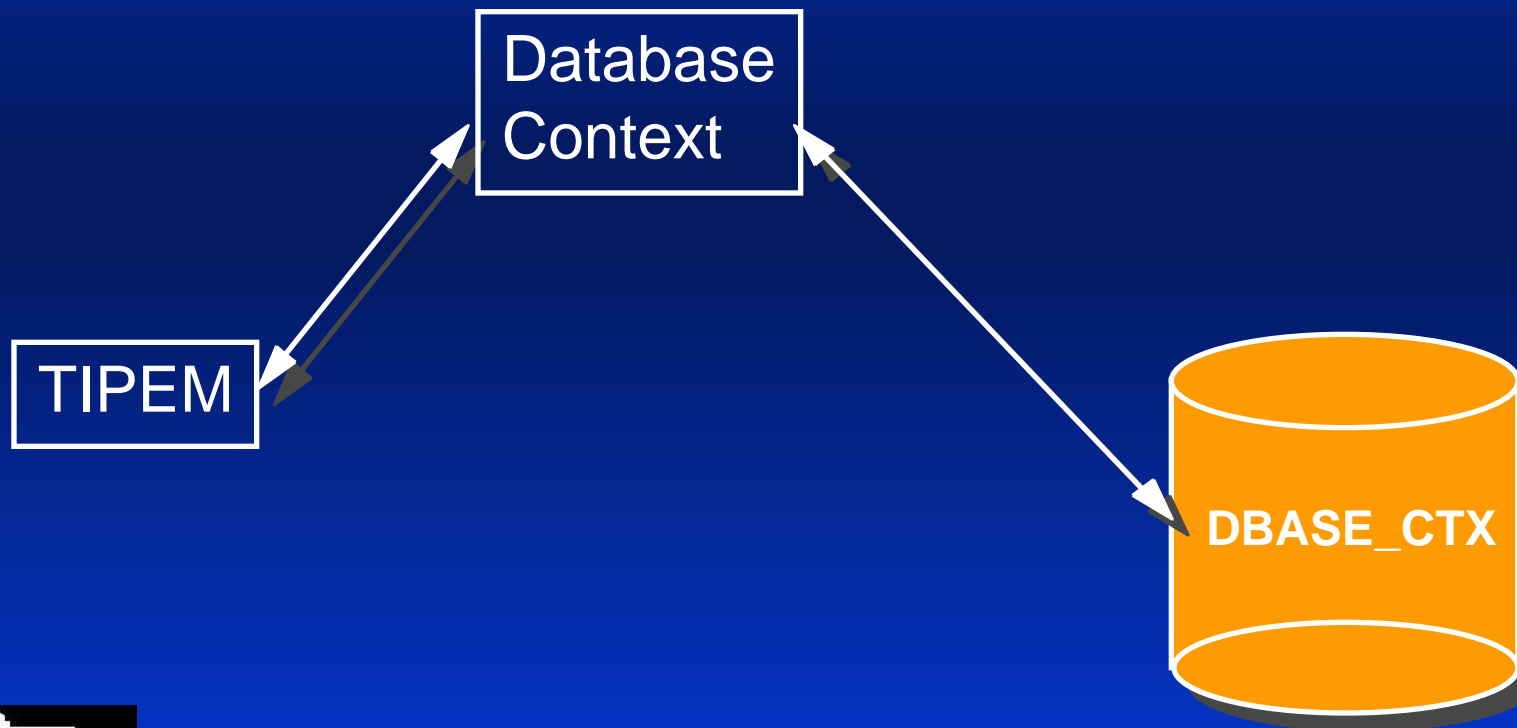


TIPeM Contexts

- A TIPeM context is an object abstraction written in C
- Programmer-defined methods for:
 - » Database storage and retrieval
 - » I/O
 - » Error processing



Database Context



Database Context

- TIPEM needs persistent storage and access procedures for:
 - » private keys
 - » certificates
 - » certificate revocation lists (CRLs)
- Access procedures TIPEM needs are:
 - » Select
 - » Insert

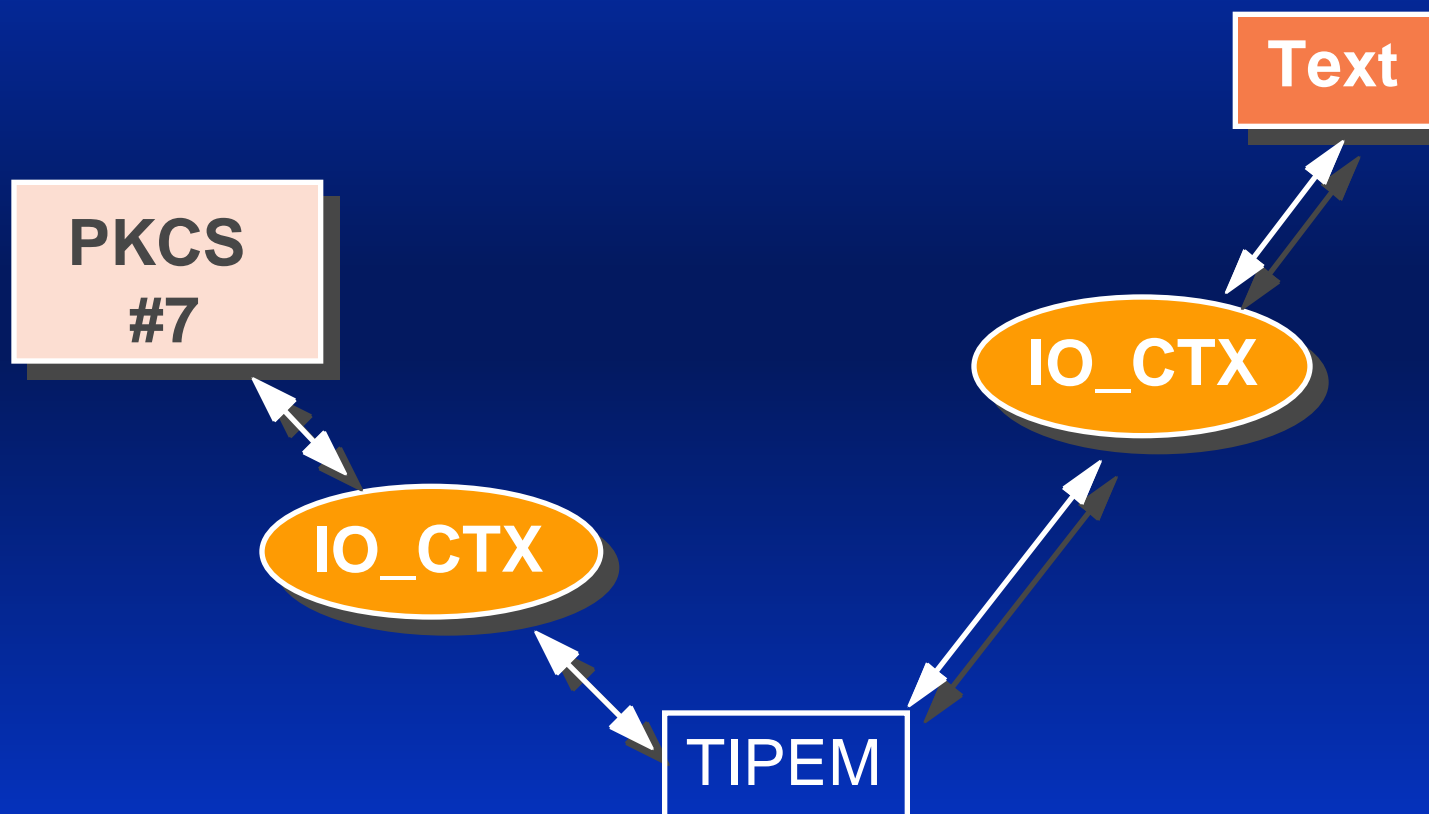


Database Context

- Programmer supplies routines to interface to any database of his/her choosing
- Examples of database context routines:
 - » select a certificate for a user
 - » select a private key
 - » insert a new valid certificate into the database



I/O Context



I/O Context

- I/O Context Procedures:

- » GetLine
- » PutLine
- » Read
- » Rewind
- » Write



Error Context

- Called each time TIPEM encounters an error.
- Programmer defines a procedure for logging errors
- Good debugging tool during development



Surrender Context

- Supply one of these when you know that a function will take a long time
 - » Example: key generation



TIPEM Building Blocks

- Message Syntax
- Name Objects
- Sets
- TIPEM Contexts
- Random Objects
- Attribute Objects



Random Objects

- Contains a seed from which a pseudo-random sequence of bytes is derived
- Random objects are used for:
 - » generating keys
 - » padding encryption blocks with random bytes



TIPEM Building Blocks

- Message Syntax
- Name Objects
- Sets
- TIPEM Contexts
- Random Objects
- Attribute Objects



Attribute Objects

- Attributes contain additional information to be included with:
 - » PKCS #7 signed messages
 - » PKCS #10 certificate request messages



Attribute Objects

- Attributes can be either signed or not
- Examples
 - » signing time
 - » challenge password
 - » email address



Topics

- What Is TIPEM?
- Getting Started
- TIPEM Building Blocks
- Message Processing



Message Processing

- Generating a key pair/certificate request
- Preparing a secure message
- Receiving a secure message

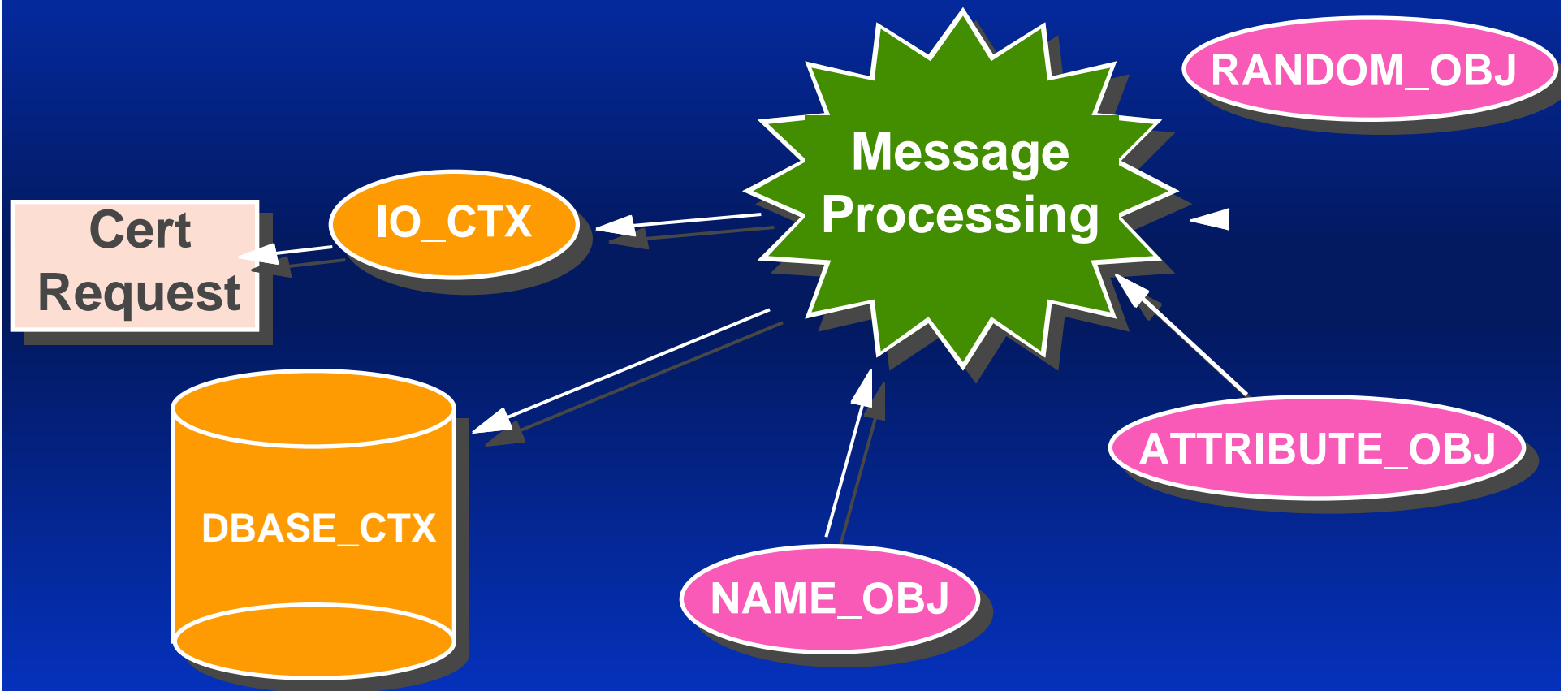


Generating a Keypair/ Certificate Request

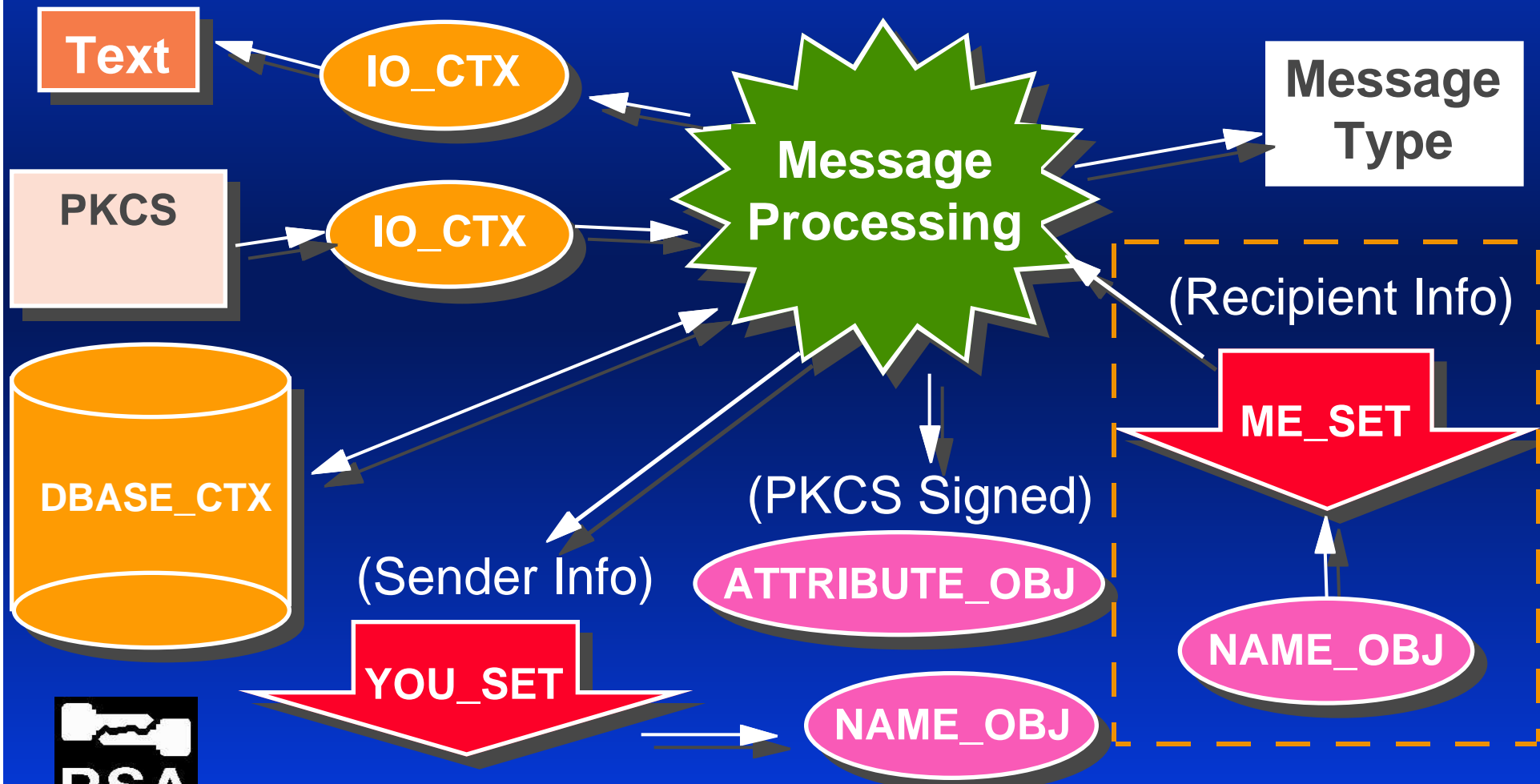
- Generate an RSA Keypair and
compose a certificate request
 - » `GeneratePKCS_RSARequest()`



Generating a Keypair/ Certificate Request



Receiving a PKCS Message

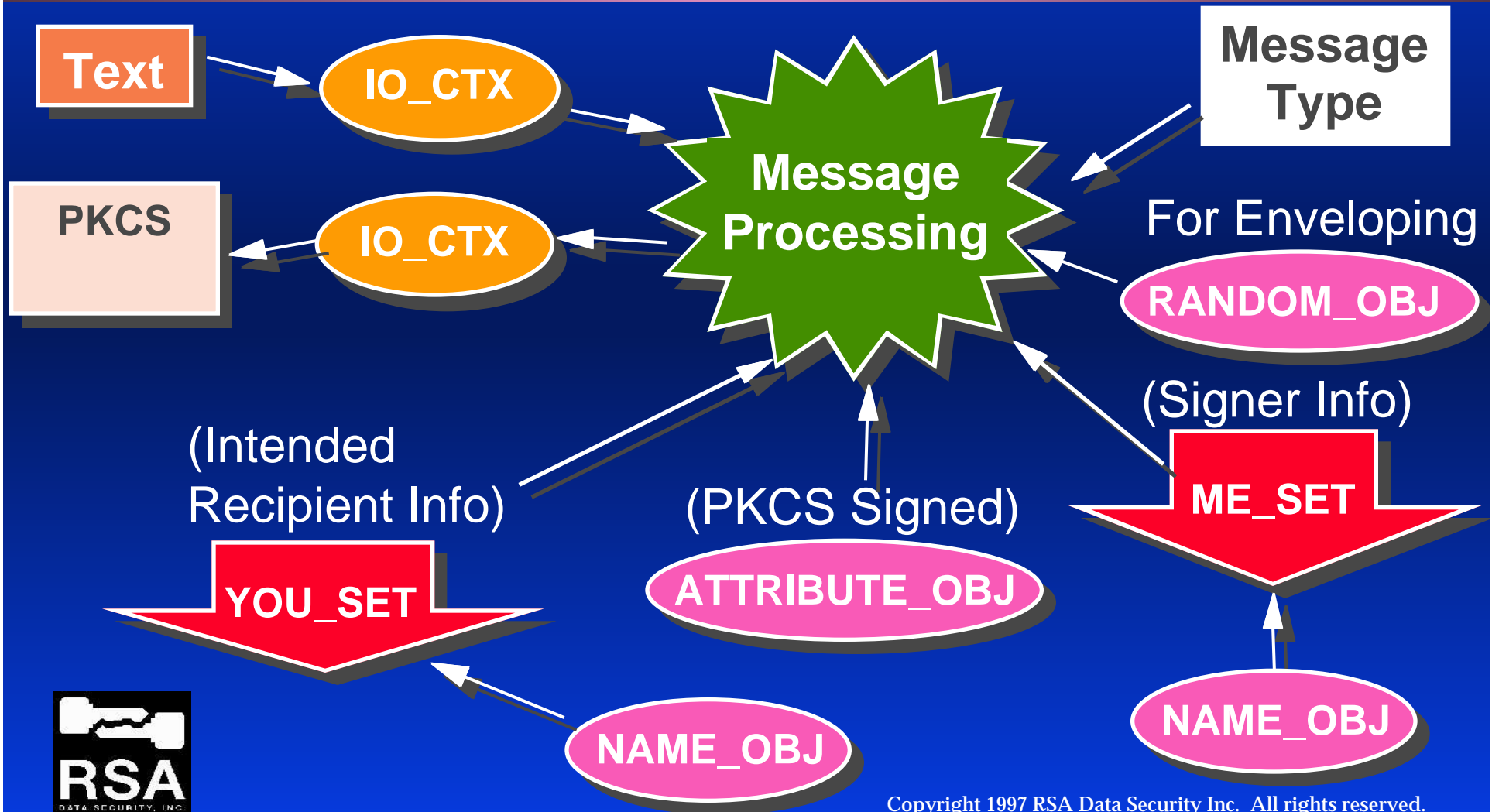


Receiving a PKCS Message

- Signed message type
 - » verify the signature
- Enveloped message type:
 - » check and open the enveloped message
- ReceivePKCSMessage()



Preparing a PKCS Message



Beyond Secure Email...

- EDI
- health care
- human resources
- education
- ...

