Secure Electronic Transaction

(SET)

Credit Cards on the Internet

- Problem: communicate credit card and purchasing data securely to gain consumer trust
  - Authentication of buyer and merchant
  - Confidential transmissions
- Systems vary by
  - Type of public-key encryption
  - Type of symmetric encryption
  - Message digest algorithm
  - Number of parties having private keys
  - Number of parties having certificates

Credit Card Protocols

- SSL 1 or 2 parties have private keys
- TLS (Transport Layer Security)
  - IETF version of SSL

- *i*KP (IBM)
- SEPP (Secure Encryption Payment Protocol)
  - MasterCard, IBM, Netscape
- STT (Secure Transaction Technology)
  - VISA, Microsoft

OBSOLETE

- SET (Secure Electronic Transactions)
  - MasterCard, VISA all parties have certificates

VERY SLOW ACCEPTANCE

Secure Electronic Transaction (SET)

- SET is not a payment system.
- It is a security protocol and format that enables users to design a credit card payment infrastructure on an open network.
- It is an open encryption and security specification.

Services Provided by SET

- Provides a secure communication channel among all parties involved in a transaction.
- Confidentiality: all messages encrypted
- Trust: all parties must have digital certificates.
- Privacy: information made available only when and where necessary.

SET Business Requirements

- Provide confidentiality of payment and ordering information.
- Ensure the integrity of all transmitted data.
- Provide authentication that a cardholder is a legitimate user of a credit card account.
- Provide authentication that a merchant can accept credit card transactions through its relationship with a financial institution.

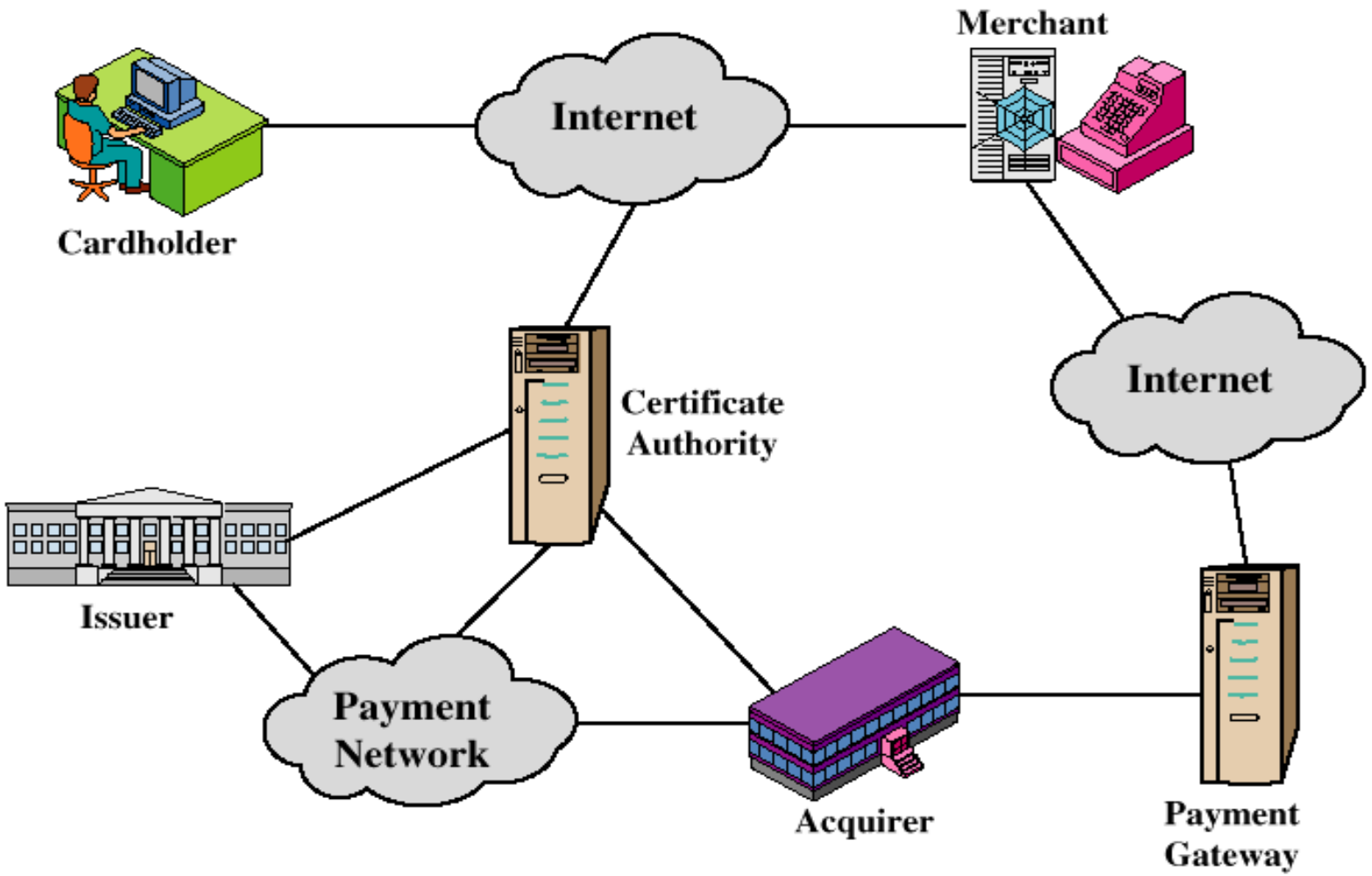
SET Business Requirements (cont'd)

- Ensure the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction.
- Create a protocol that neither depends on transport security mechanisms nor prevents their use.
- Facilitate and encourage interoperability among software and network providers.

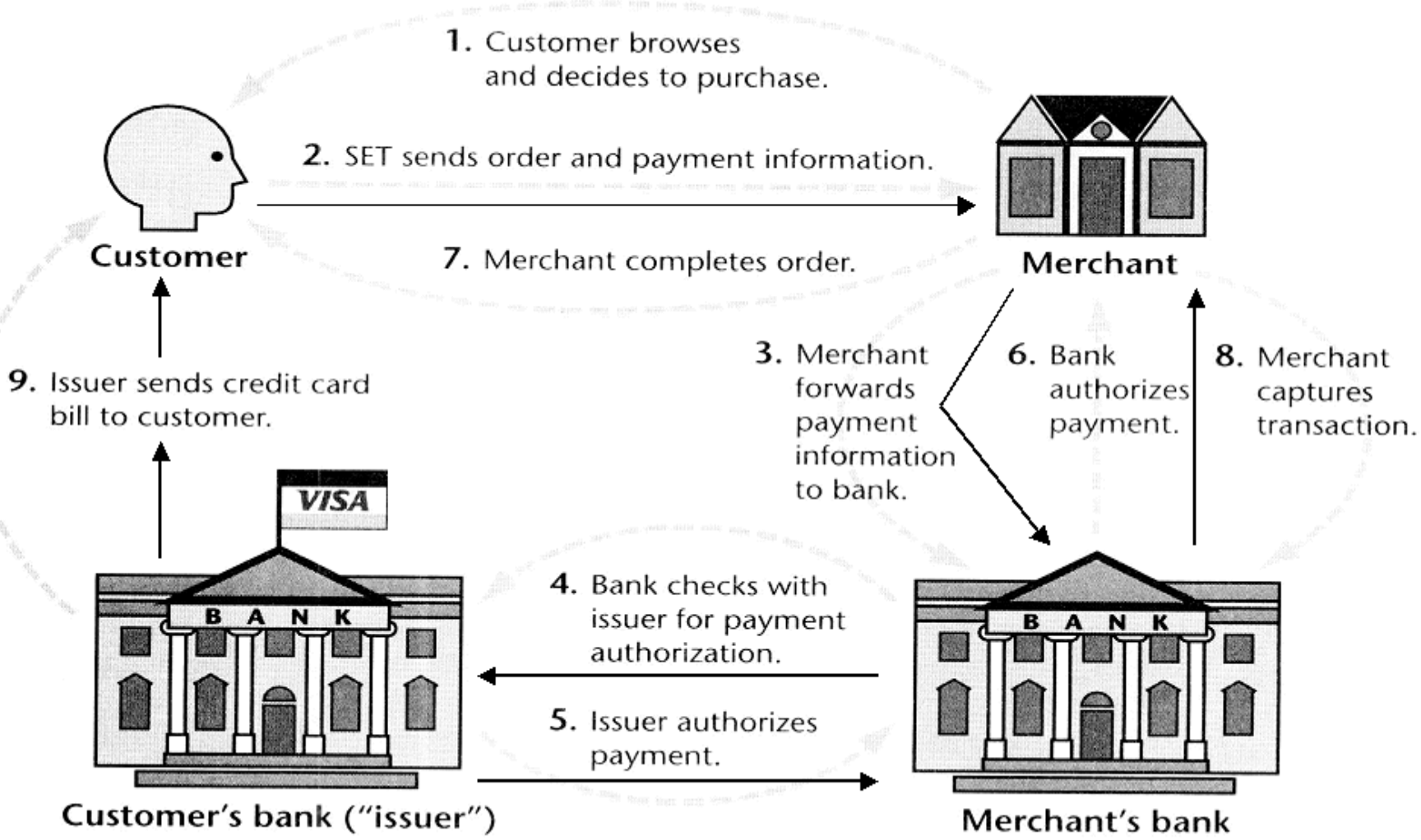
Key Technologies of SET

- Confidentiality of information: DES
- Integrity of data: RSA digital signatures with SHA-1 hash codes.
- Cardholder account authentication: X.509v3 digital certificates with RSA signatures.
- Merchant authentication: X.509v3 digital certificates with RSA signatures.
- Privacy: separation of order and payment information using dual signatures.

Participants of a SET System



SET Transactions



SET Transactions

- The customer opens an account with a card issuer.
  - MasterCard, Visa, etc.
- The customer receives a X.509 V3 certificate signed by a bank.
  - X.509 V3
- A merchant who accepts a certain brand of card must possess two X.509 V3 certificates.
  - One for signing & one for key exchange
- The customer places an order for a product or service with a merchant.
- The merchant sends a copy of its certificate for verification.

SET Transactions

- The customer sends order and payment information to the merchant.
- The merchant requests payment authorization from the payment gateway prior to shipment.
- The merchant confirms order to the customer.
- The merchant provides the goods or service to the customer.
- The merchant requests payment from the payment gateway.

Dual Signature for SET

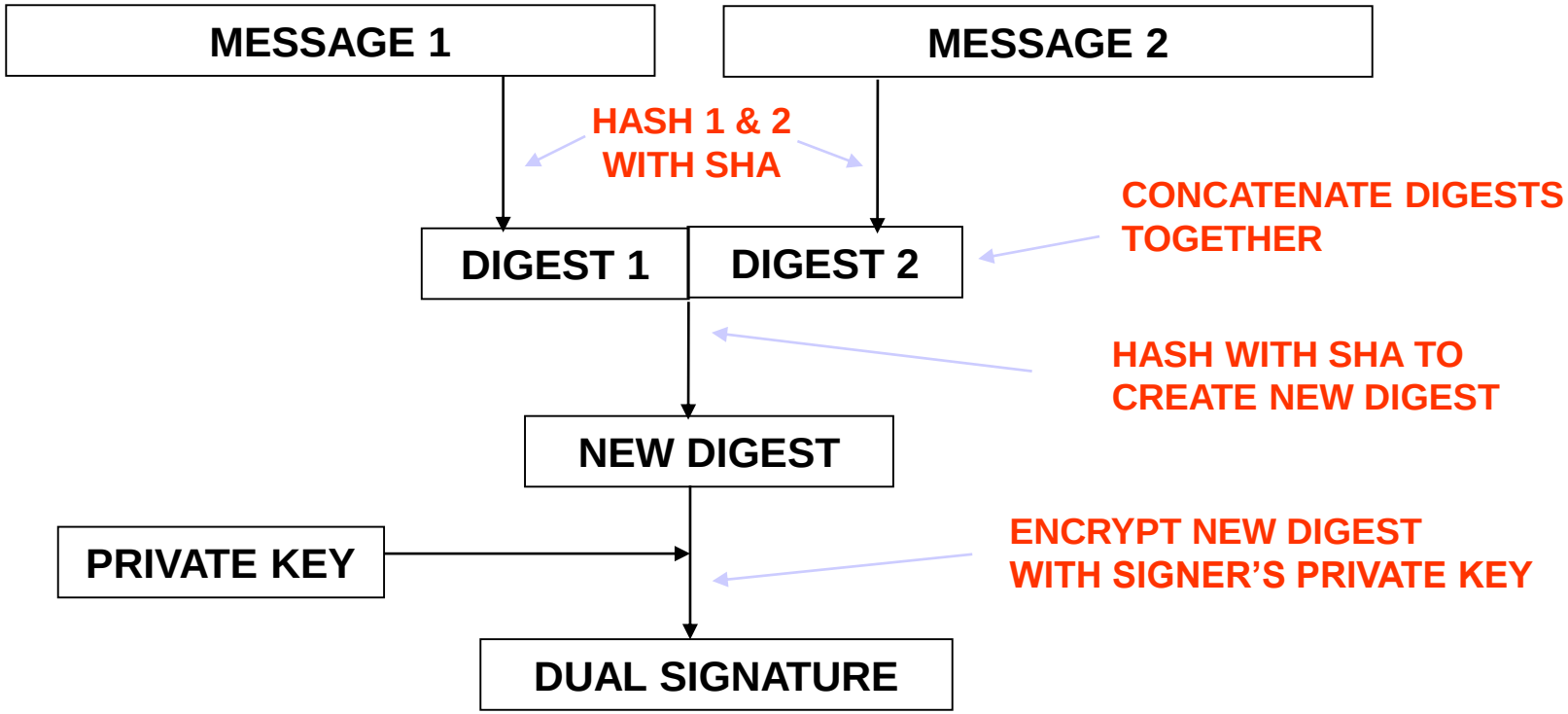
- Concept: Link Two Messages Intended for Two Different Receivers:
  - Order Information (OI): Customer to Merchant
  - Payment Information (PI): Customer to Bank
- Goal: Limit Information to A "Need-to-Know" Basis:
  - Merchant does not need credit card number.
  - Bank does not need details of customer order.
  - Afford the customer extra protection in terms of privacy by keeping these items separate.
- This link is needed to prove that payment is intended for this order and not some other one.

Why Dual Signature?

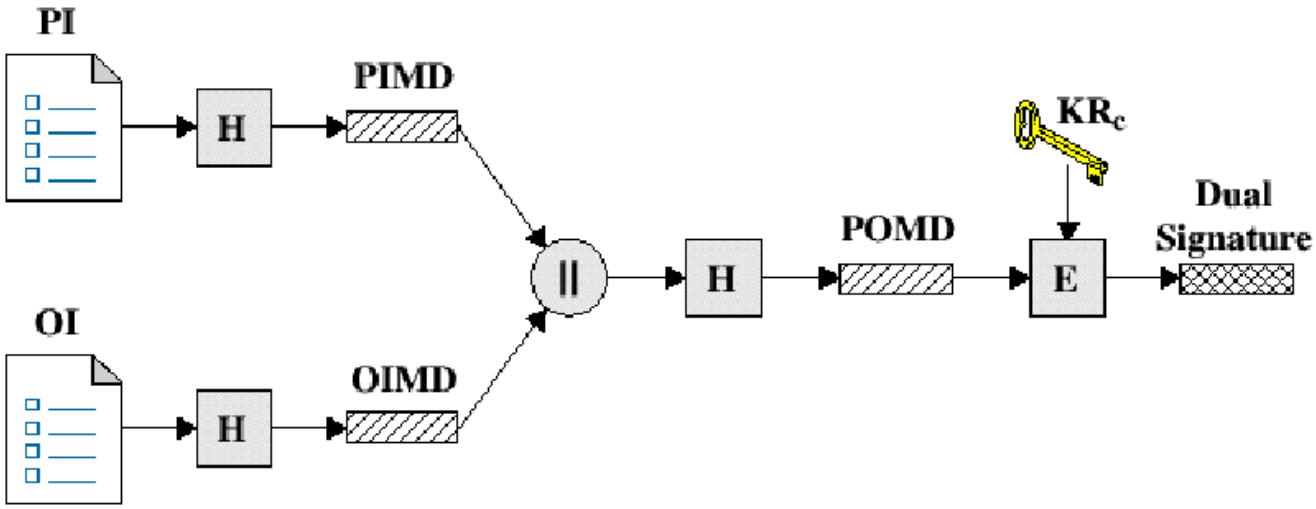
- Suppose that customers send the merchant two messages:
  - The signed order information (OI).
  - The signed payment information (PI).
  - In addition, the merchant passes the payment information (PI) to the bank.
- If the merchant can capture another order information (OI) from this customer, the merchant could claim this order goes with the payment information (PI) rather than the original.

Dual Signature

- Links two messages securely but allows only one party to read each.



Dual Signature Operation



- The operation for dual signature is as follows:
  - Take the hash (SHA-1) of the payment and order information.
  - These two hash values are concatenated [H(PI) || H(OI)] and then the result is hashed.
  - **Customer encrypts the final hash with his private key creating the dual signature.**

$$DS = E_{KRc} [H(H(PI) || H(OI))]$$

DS Verification by Merchant

- The merchant has the public key of the customer obtained from the customer's certificate.
- Now, the merchant can compute two values:

  $H(PIMD \mid\mid H(OI))$

  $D_{KUc}[DS]$
- Should be equal!

DS Verification by Bank

- The bank is in possession of DS, PI, the message digest for OI (OIMD), and the customer's public key, then the bank can compute the following:

  $H(H(PI) \,||\, OIMD)$

  $D_{KUc}\,[\,DS\,]$

What did we accomplish?

- The merchant has received OI and verified the signature.
- The bank has received PI and verified the signature.
- The customer has linked the OI and PI and can prove the linkage.

SET Supported Transactions

- Card holder registration
- Merchant registration
- Purchase request
- Payment authorization
- Payment capture
- Certificate query
- Purchase inquiry
- Purchase notification
- Sale transaction
- Authorization reversal
- Capture reversal
- Credit reversal

Purchase Request

- Browsing, Selecting, and Ordering is Done
- Purchasing Involves 4 Messages:
  - Initiate Request
  - Initiate Response
  - Purchase Request
  - Purchase Response

Purchase Request: Initiate Request

- Basic Requirements:
  - Cardholder Must Have a Copy of Certificates of Merchant and Payment Gateway.
- Customer Requests the Certificates in the Initiate Request Message, sent to the Merchant, which also includes
  - Brand of Credit Card.
  - ID Assigned to this Request/response pair by customer.
  - Nonce- to ensure timeliness.

Purchase Request: Initiate Response

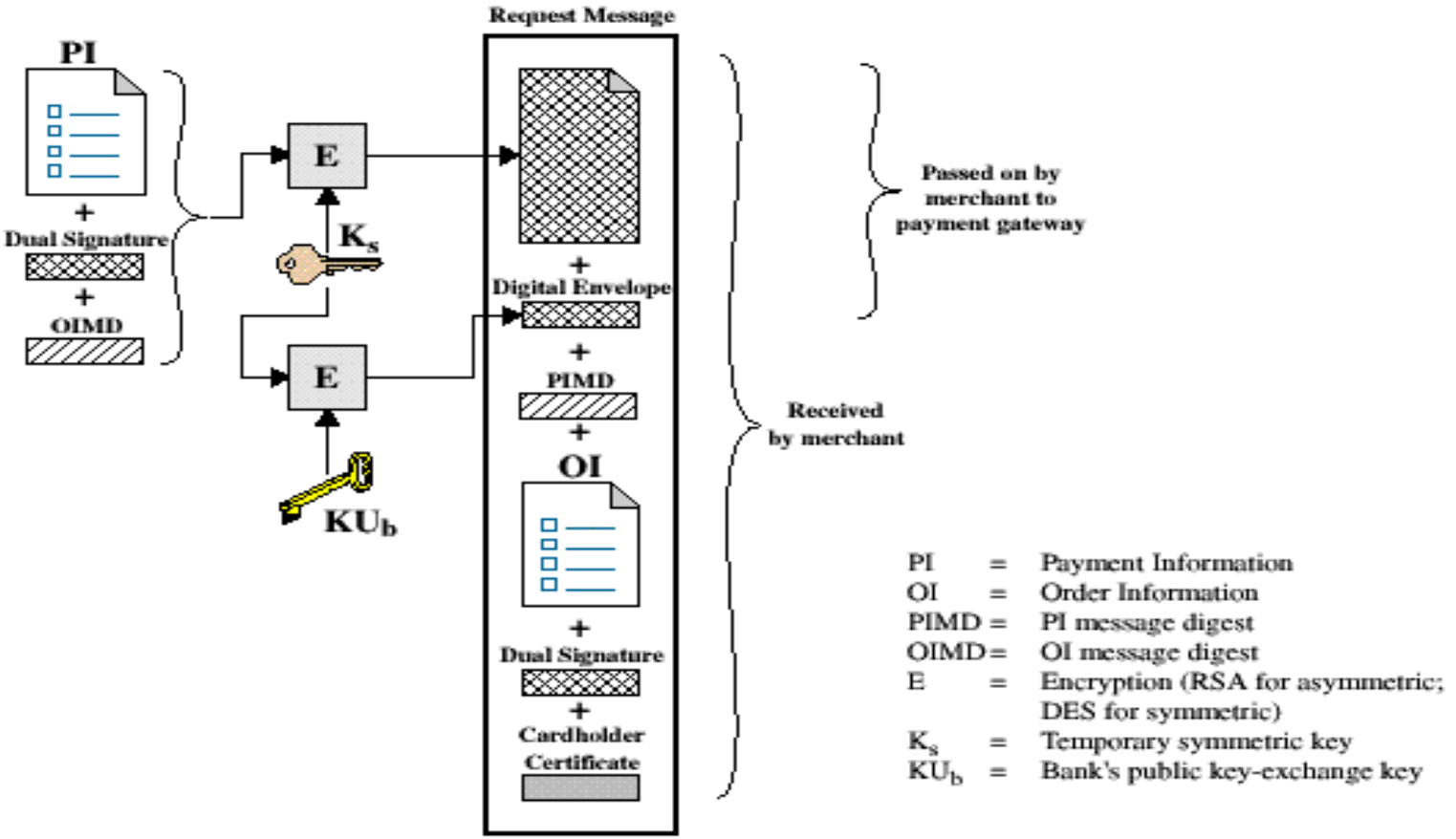
- Merchant Generates a Response and Signs it with Private Signature Key that includes
  - Customer Nonce
  - Merchant Nonce (Returned in Next Message)
  - Transaction ID for Purchase Transaction
- In Addition …
  - Merchant's Signature Certificate
  - Payment Gateway's Key Exchange Certificate

Purchase Request

- Cardholder verifies two certificates using their respective CA signatures and Creates the OI and PI.
- OI does not contain explicit order data such as the number and price of items.
- The transaction id generated by the merchant is placed in both the OI and PI.
- Purchase message Includes:
  - Purchase-related Information.
  - Order-related Information.
  - Cardholder Certificate.

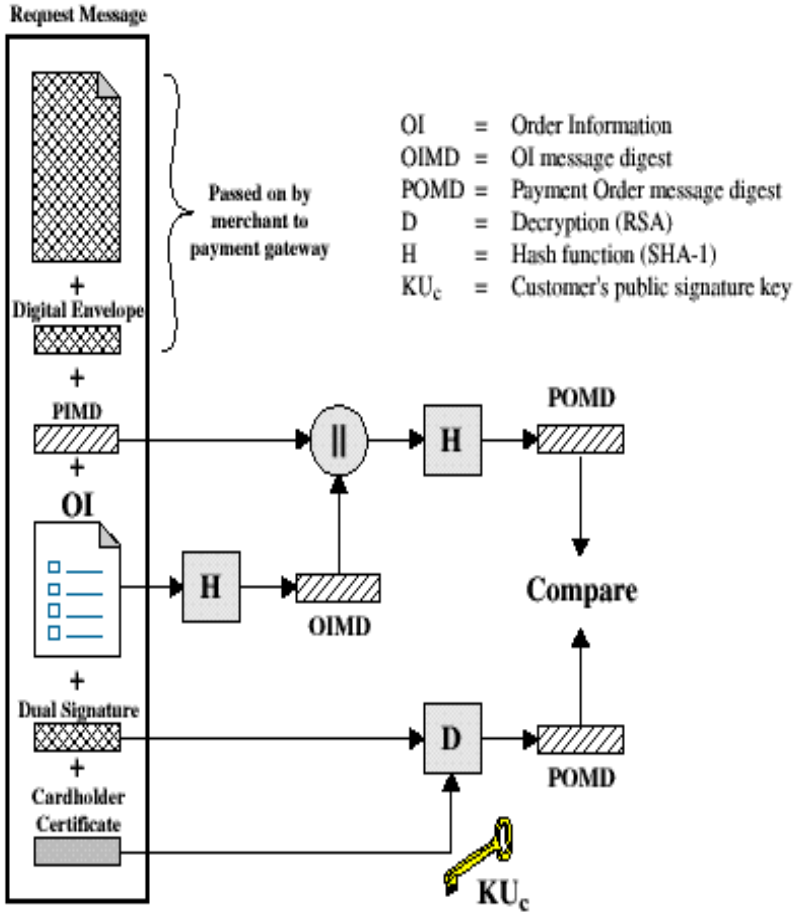
Purchase Request

- The cardholder generates a one-time symmetric encryption key, Ks.



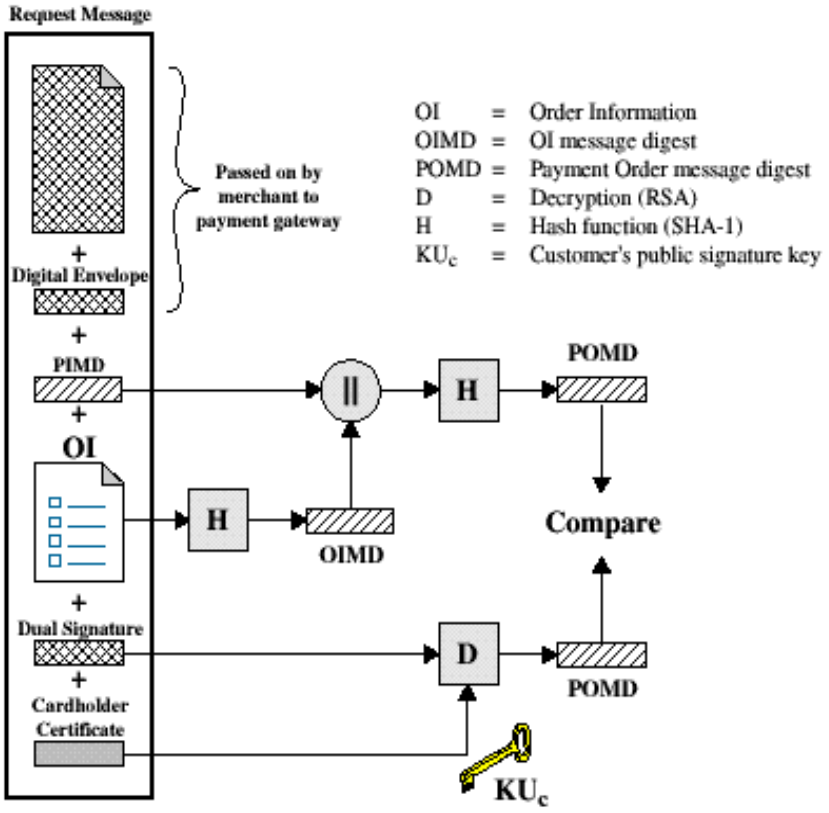
Merchant Verifies Purchase Request

- When the merchant receives the Purchase Request message, it performs the following actions:
  - Verify the cardholder certificates by means of its CA signatures.
  - Verifies the dual signature using the customer's public key signature.



Merchant Verification (cont'd)

- Processes the order and forwards the payment information to the payment gateway for authorization.
- Sends a purchase response to the cardholder.



Purchase Response Message

- Message that Acknowledges the Order and References the Corresponding Transaction Number.
- Block is
  - Signed by the Merchant using its Private Signature Key
  - Block and its Signature are Sent to Customer Along with Merchant's Signature Certificate.
- Upon Reception
  - Verifies Merchant Certificate
  - Verifies Signature on Response Block
  - Takes the Appropriate Action

Payment Process

- The payment process is broken down into two steps:
  - Payment authorization
    - Authorization Request
    - Authorization Response
  - Payment capture

Authorization Request

- The merchant sends an authorization request message to the payment gateway consisting of the following:
  - Purchase-related information: This information was obtained from customer and consists of
    - PI
    - Dual signature calculated over the PI & OI and signed with customer's private key.
    - The OI message digest (OIMD)
    - The digital envelop

Payment Authorization (cont'd)

- Authorization-related information: This information is generated by the merchant and consists of
  - An authorization block that includes
    - the transaction ID, Signed with merchant's private key and encrypted one-time session key generated by merchant.
    - A digital envelop: contains one-time key encrypted with payment gateway's public key-exchange key.
- Certificates
  - Cardholder's signature key certificate (to verify dual signature)
  - Merchant's signature key certificate (to verify merchant signs)
  - Merchant's key exchange certificate (needed in the payment gateway's response)

Payment: Payment Gateway

- Verifies All Certificates.
- Decrypts Digital Envelope of the Authorization Block to Obtain Symmetric Key and then Decrypts the Block.
- Verify Merchant's Signature on the Authorization Block.
- Decrypts Digital Envelope of the Payment Block to Obtain Symmetric Key and Decrypts the Payment Block.
- Verifies Dual Signature on the Payment Block.
- Verifies that the Transaction ID Received from Merchant Matches that in PI Received from Customer.
- Requests and Receives Issuer Authorization

Authorization Response

- Authorization Response Message
  - Authorization-related Information
    - ✓ An authorization block, signed with the gateway's private signature key and encrypted with a one-time symmetric key generated by gateway.
    - ✓ Digital envelop that contains one-time symmetric key encrypted with the merchant's public key exchange key.
  - Capture Token Information
    - ✓ This information will be used to effect payment later.
    - ✓ A signed, encrypted capture token together with a digital envelop.
    - ✓ It must be returned by merchant, as is, with a payment request.

Authorization Response

Certificate

- ✓ Gateway's signature key certificate.

With the authorization from the gateway, the merchant can provide the goods or service to the customer.

SET Overhead

Simple purchase transaction:

- Four messages between merchant and customer
- Two messages between merchant and payment gateway
- 6 digital signatures
- 9 RSA encryption/decryption cycles
- 4 DES encryption/decryption cycles
- 4 certificate verifications

Scaling:

- Multiple servers need copies of all certificates