

# Cryptography and Network Security

SET for E-COMMERCE  
TRANSACTIONS



# Session Meta Data

---

Author	Dr T Sree Sharmila
Reviewer	
Version Number	1.0
Release Date	6 August 2018

# Revision History

---

Revision Date	Details	Version no.
		1.0

# Agenda

---

- Credit cards
- Secure Electronic Transactions (SET) System
  - SET requirement
  - SET Transaction
  - Key technologies of SET
  - Dual Signature
  - DS verification by merchant
  - DS verification by bank
  - SET supported transaction
  - Purchase request
  - Merchant verifies purchase request
  - Purchase response message
  - Payment processing
- Summary
- Test your understanding
- References

# 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



- PKP (IBM)
- SEPP (Secure Encryption Payment Protocol)
  - MasterCard, IBM, Netscape
- STT (Secure Transaction Technology)
  - VISA, Microsoft
- SET (Secure Electronic Transactions)
  - MasterCard, VISA all parties have certificates



**OBSOLETE**



**VERY SLOW  
ACCEPTANCE**



# Agenda

---

- Credit cards
- Secure Electronic Transactions (SET) System
  - SET requirement
  - SET Transaction
  - Key technologies of SET
  - Dual Signature
  - DS verification by merchant
  - DS verification by bank
  - SET supported transaction
  - Purchase request
  - Merchant verifies purchase request
  - Purchase response message
  - Payment processing
- Summary
- Test your understanding
- References

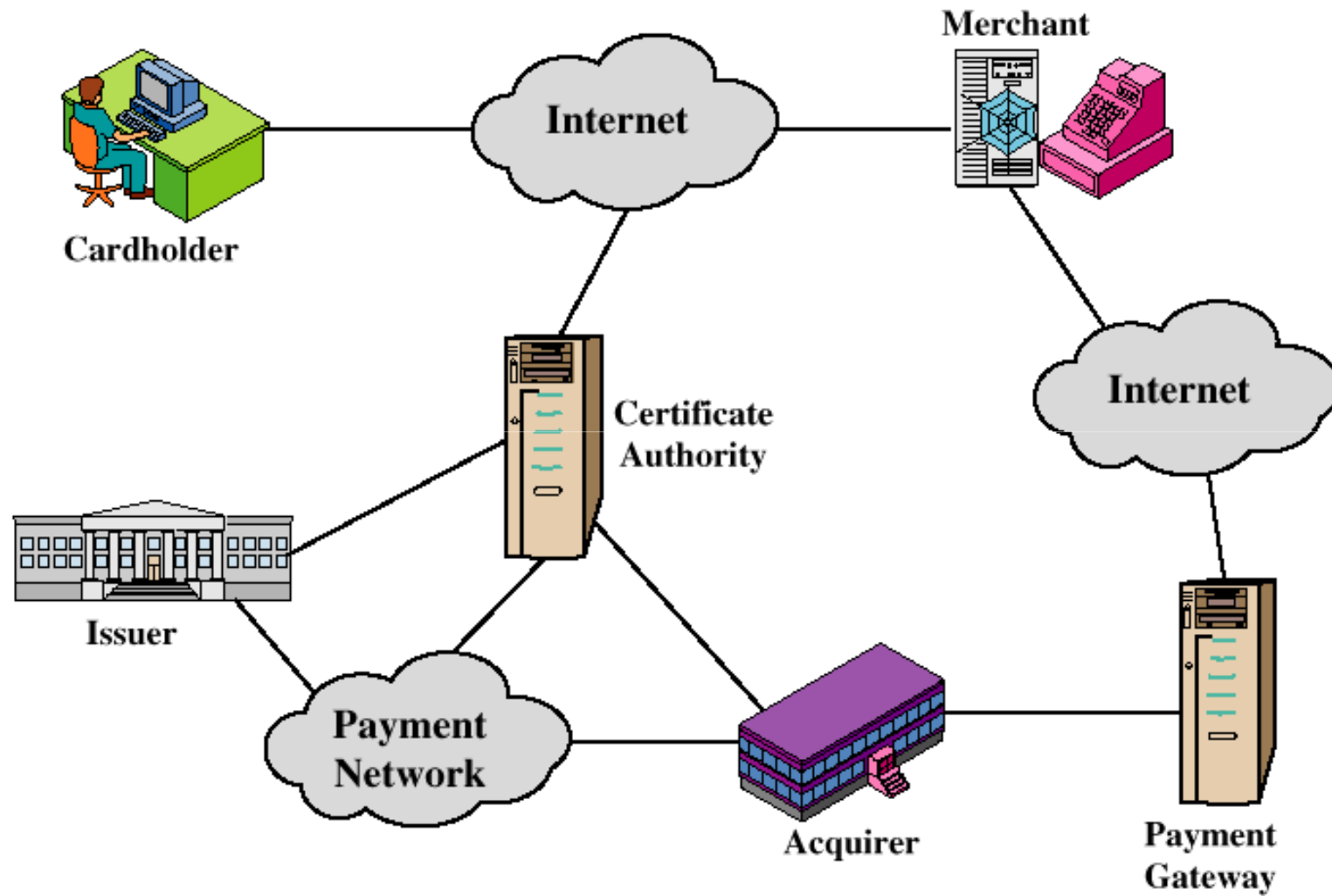
# Secure Electronic Transaction (SET)

---

- Developed by Visa and MasterCard
- Designed to protect credit card transactions
- Confidentiality: all messages encrypted
- Trust: all parties must have digital certificates
- Privacy: information made available only when and where necessary



## Participants in the SET System



# Agenda

---

- Credit cards
- Secure Electronic Transactions (SET) System
  - SET requirement
  - SET Transaction
  - Key technologies of SET
  - Dual Signature
  - DS verification by merchant
  - DS verification by bank
  - SET supported transaction
  - Purchase request
  - Merchant verifies purchase request
  - Purchase response message
  - Payment processing
- Summary
- Test your understanding
- References

# 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)

---

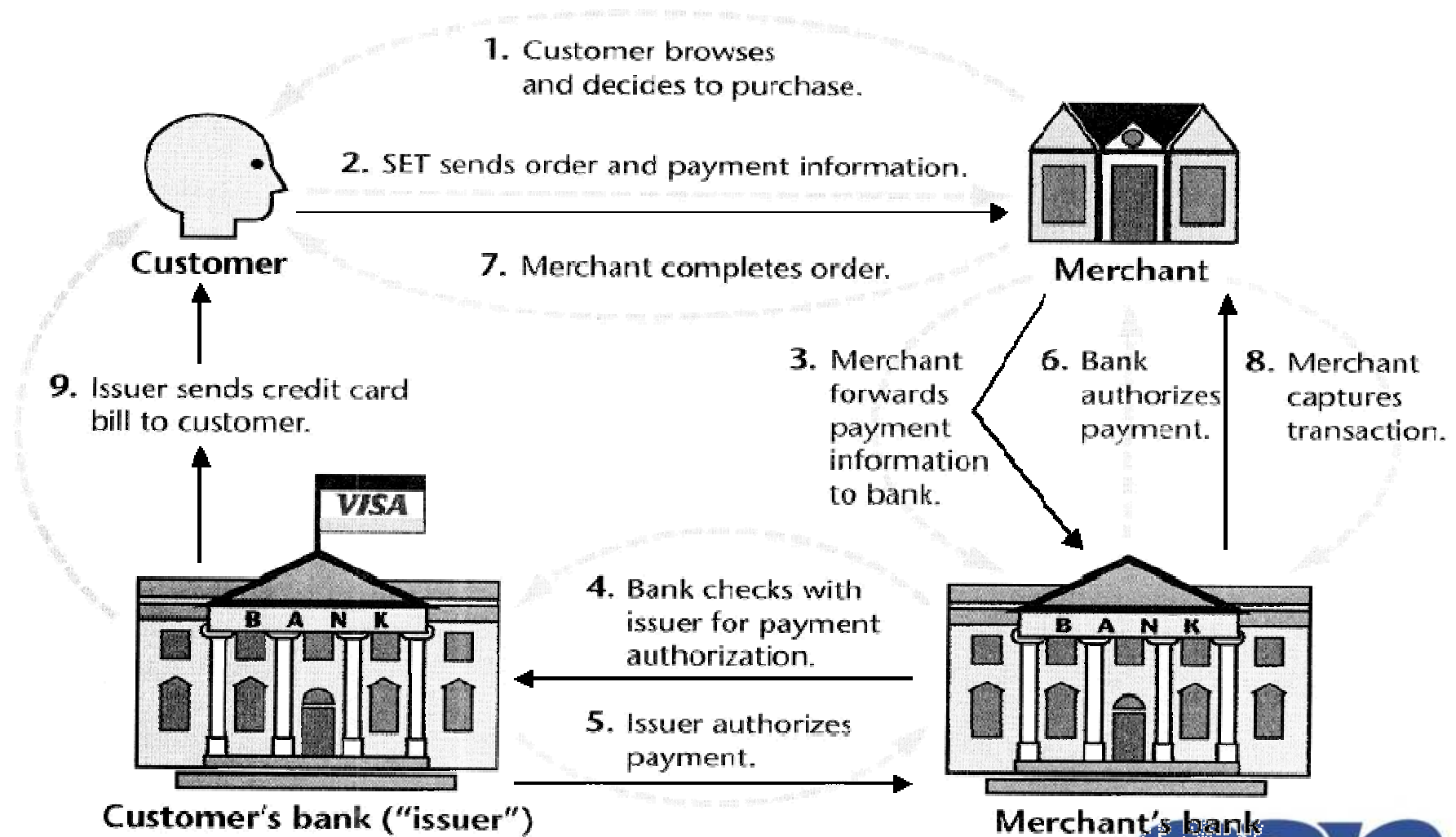
- Ensure the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction
- Create a protocol that neither depends on transport security mechanisms nor prevents their use
- Facilitate and encourage interoperability among software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

# Agenda

---

- Credit cards
- Secure Electronic Transactions (SET) System
  - SET requirement
  - SET Transaction
  - Key technologies of SET
  - Dual Signature
  - DS verification by merchant
  - DS verification by bank
  - SET supported transaction
  - Purchase request
  - Merchant verifies purchase request
  - Purchase response message
  - Payment processing
- Summary
- Test your understanding
- References

## 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.



# Agenda

---

- Credit cards
- Secure Electronic Transactions (SET) System
  - SET requirement
  - SET Transaction
  - Key technologies of SET
  - Dual Signature
  - DS verification by merchant
  - DS verification by bank
  - SET supported transaction
  - Purchase request
  - Merchant verifies purchase request
  - Purchase response message
  - Payment processing
- Summary
- Test your understanding
- References

# 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

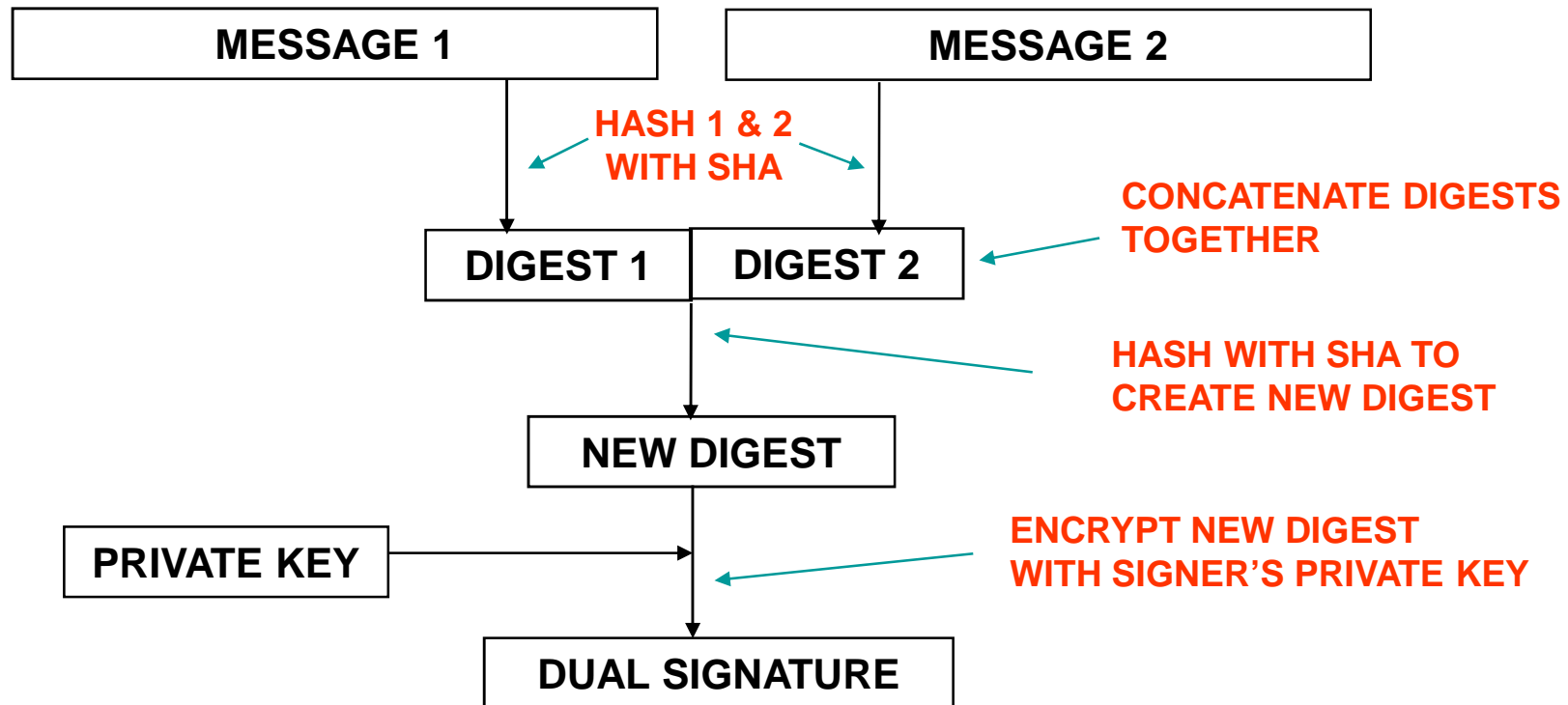
# Agenda

---

- Credit cards
- Secure Electronic Transactions (SET) System
  - SET requirement
  - SET Transaction
  - Key technologies of SET
  - Dual Signature
  - DS verification by merchant
  - DS verification by bank
  - SET supported transaction
  - Purchase request
  - Merchant verifies purchase request
  - Purchase response message
  - Payment processing
- Summary
- Test your understanding
- References

# Dual Signatures

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



## Dual Signature for SET

---

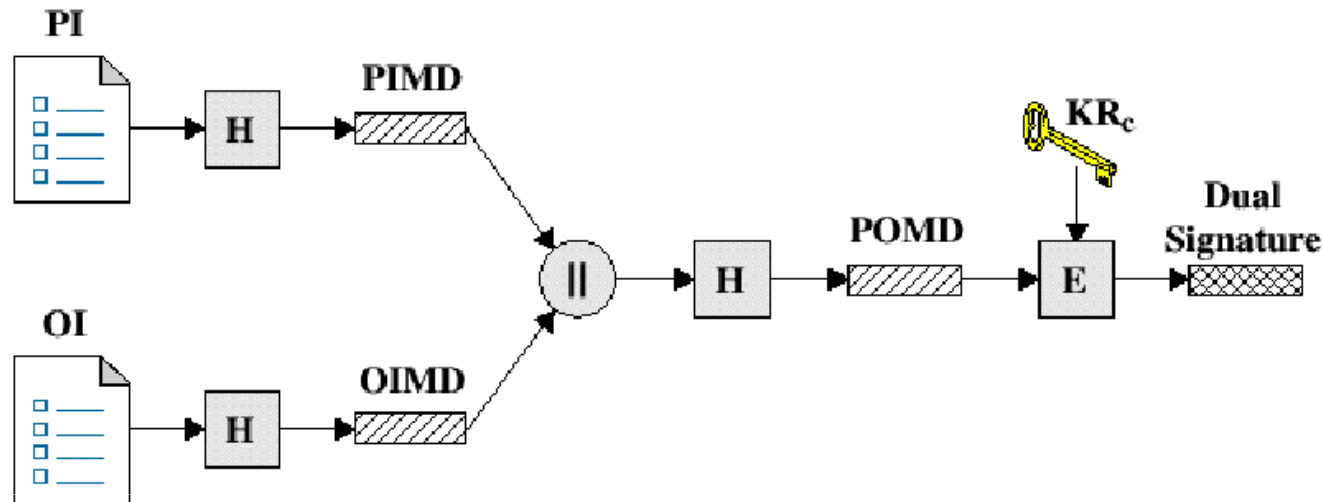
- Concept: **Link Two Messages Intended for Two Different Receivers:**
  - Order Information (OI): Customer to Merchant
  - Payment Information (PI): Customer to Bank
- Goal: **Limit Information to A “Need-to-Know” Basis:**
  - Merchant does not need credit card number.
  - Bank does not need details 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 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 a private key creating the dual signature.**

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

# Agenda

---

- Credit cards
- Secure Electronic Transactions (SET) System
  - SET requirement
  - SET Transaction
  - Key technologies of SET
  - Dual Signature
  - DS verification by merchant
  - DS verification by bank
  - SET supported transaction
  - Purchase request
  - Merchant verifies purchase request
  - Purchase response message
  - Payment processing
- Summary
- Test your understanding
- References



## 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:

$$H(\text{PIMD} \parallel H(\text{OI}))$$

$$D_{\text{KUC}}[\text{DS}]$$

- Should be equal!

# Agenda

---

- Credit cards
- Secure Electronic Transactions (SET) System
  - SET requirement
  - SET Transaction
  - Key technologies of SET
  - Dual Signature
  - DS verification by merchant
  - DS verification by bank
  - SET supported transaction
  - Purchase request
  - Merchant verifies purchase request
  - Purchase response message
  - Payment processing
- Summary
- Test your understanding
- References

## 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:

$H(H(PI) \parallel OIMD)$

$D_{KUC} [ DS ]$

## 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.

# Agenda

---

- Credit cards
- Secure Electronic Transactions (SET) System
  - SET requirement
  - SET Transaction
  - Key technologies of SET
  - Dual Signature
  - DS verification by merchant
  - DS verification by bank
  - SET supported transaction
  - Purchase request
  - Merchant verifies purchase request
  - Purchase response message
  - Payment processing
- Summary
- Test your understanding
- References

# 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**

# Agenda

---

- Credit cards
- Secure Electronic Transactions (SET) System
  - SET requirement
  - SET Transaction
  - Key technologies of SET
  - Dual Signature
  - DS verification by merchant
  - DS verification by bank
  - SET supported transaction
  - Purchase request
  - Merchant verifies purchase request
  - Purchase response message
  - Payment processing
- Summary
- Test your understanding
- References

# 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 Copy of Certificates for Merchant and Payment Gateway
- **Customer Requests the Certificates in the Initiate Request Message to Merchant**
  - Brand of Credit Card
  - ID Assigned to this Request/response pair by customer
  - Nonce

## Purchase Request: Initiate Response

---

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

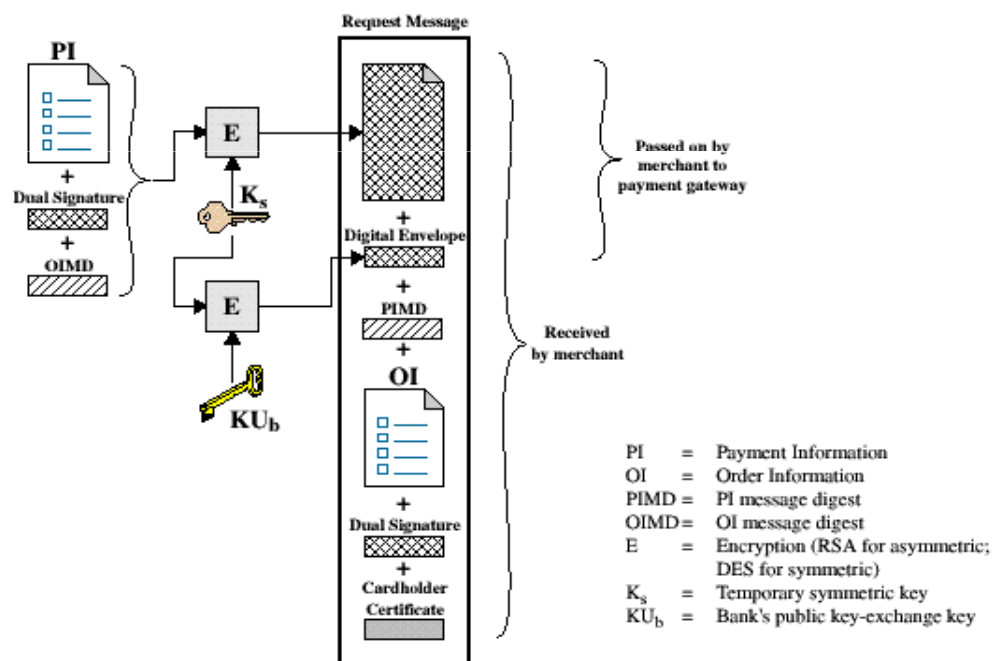
# Purchase Request: Purchase Request

---

- Cardholder Verifies Two Certificates Using Their CAs and Creates the OI and PI.
- Message Includes:
  - Purchase-related Information
  - Order-related Information
  - Cardholder Certificate

# Purchase Request

- The cardholder generates a one-time symmetric encryption key,  $K_s$ ,



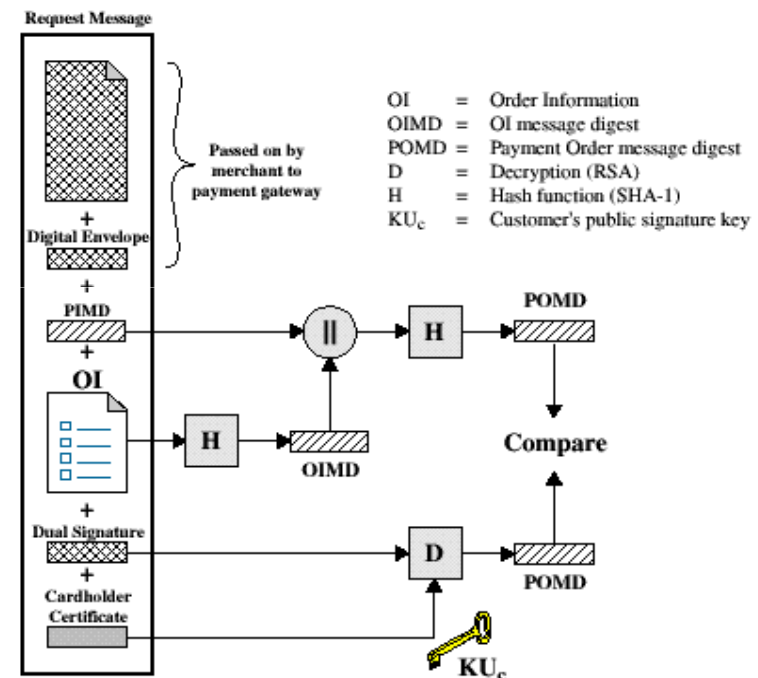
# Agenda

---

- Credit cards
- Secure Electronic Transactions (SET) System
  - SET requirement
  - SET Transaction
  - Key technologies of SET
  - Dual Signature
  - DS verification by merchant
  - DS verification by bank
  - SET supported transaction
  - Purchase request
  - Merchant verifies purchase request
  - Purchase response message
  - Payment processing
- Summary
- Test your understanding
- References

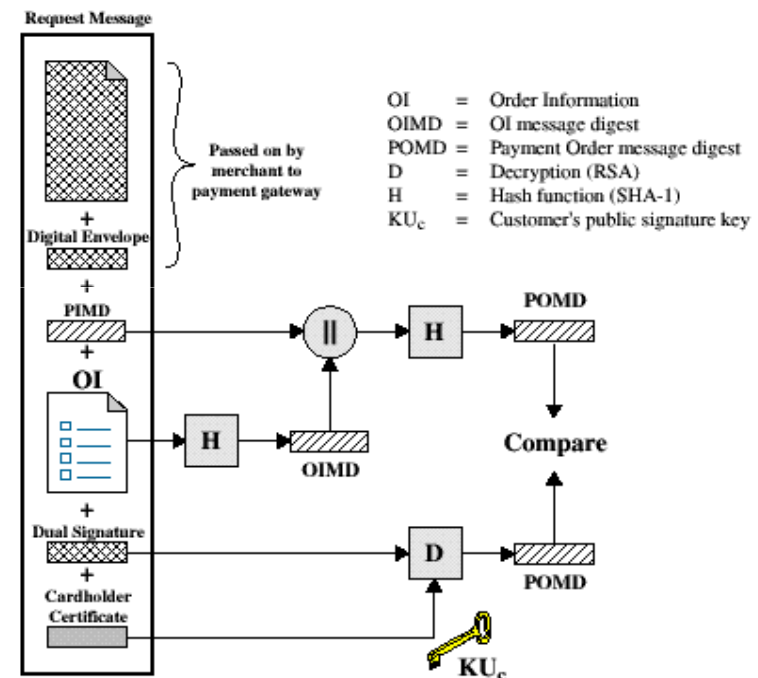
## Merchant Verifies Purchase Request

- 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.



# Agenda

---

- Credit cards
- Secure Electronic Transactions (SET) System
  - SET requirement
  - SET Transaction
  - Key technologies of SET
  - Dual Signature
  - DS verification by merchant
  - DS verification by bank
  - SET supported transaction
  - Purchase request
  - Merchant verifies purchase request
  - Purchase response message
  - Payment processing
- Summary
- Test your understanding
- References



# Purchase Response Message

---

- Message that Acknowledges the Order and References Corresponding Transaction Number
- Block is
  - Signed by Merchant Using its Private Key
  - Block and 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

# Agenda

---

- Credit cards
- Secure Electronic Transactions (SET) System
  - SET requirement
  - SET Transaction
  - Key technologies of SET
  - Dual Signature
  - DS verification by merchant
  - DS verification by bank
  - SET supported transaction
  - Purchase request
  - Merchant verifies purchase request
  - Purchase response message
  - Payment processing
- Summary
- Test your understanding
- References

# Payment Process

---

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

# Payment Authorization

---

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

## Payment Authorization (cont'd)

---

- Authorization-related information
  - An authorization block including:
    - A transaction ID
    - Signed with merchant's private key
    - Encrypted one-time session key
- Certificates
  - Cardholder's signature key certificate
  - Merchant's signature key certificate
  - Merchant's key exchange certificate

## Payment: Payment Gateway

---

- Verify All Certificates
- Decrypt Authorization Block Digital Envelope to Obtain Symmetric Key and Decrypt Block
- Verify Merchant Signature on Authorization Block
- Decrypt Payment Block Digital Envelope to Obtain Symmetric Key and Decrypt Block
- Verify Dual Signature on Payment Block
- Verify Received Transaction ID Received from Merchant Matches PI Received from Customer
- Request and Receive Issuer Authorization

# Authorization Response

---

- Authorization Response Message
  - Authorization-related Information
  - Capture Token Information
  - Certificate

# Agenda

---

- Credit cards
- Secure Electronic Transactions (SET) System
  - SET requirement
  - SET Transaction
  - Key technologies of SET
  - Dual Signature
  - DS verification by merchant
  - DS verification by bank
  - SET supported transaction
  - Purchase request
  - Merchant verifies purchase request
  - Purchase response message
  - Payment processing
- Summary
- Test your understanding
- References



# Summary

---

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

# Agenda

---

- Credit cards
- Secure Electronic Transactions (SET) System
  - SET requirement
  - SET Transaction
  - Key technologies of SET
  - Dual Signature
  - DS verification by merchant
  - DS verification by bank
  - SET supported transaction
  - Purchase request
  - Merchant verifies purchase request
  - Purchase response message
  - Payment processing
- Summary
- Test your understanding
- References

# Test your understanding

---

1) Explain SET in detail.

# Agenda

---

- Credit cards
- Secure Electronic Transactions (SET) System
  - SET requirement
  - SET Transaction
  - Key technologies of SET
  - Dual Signature
  - DS verification by merchant
  - DS verification by bank
  - SET supported transaction
  - Purchase request
  - Merchant verifies purchase request
  - Purchase response message
  - Payment processing
- Summary
- Test your understanding
- References

# References

---

1. William Stallings, Cryptography and Network Security, 6th Edition, Pearson Education, March 2013.
2. Charlie Kaufman, Radia Perlman and Mike Speciner, "Network Security", Prentice Hall of India, 2002.