Network Security

Asim Rasheed

Where we are …

- Introduction to network security
- Vulnerabilities in IP
- I. CRYPTOGRAPHY
  - Symmetric Encryption and Message Confidentiality
  - Public-Key Cryptography and Message Authentication
- **II. NETWORK SECURITY APPLICATIONS**
  - Authentication Applications (Kerberos, X.509)
  - Electronic Mail Security (PGP, S/MIME)
  - IP Security (IPSec, AH, ESP, IKE)
  - **Web Security (SSL, TLS, SET)**
- III. SYSTEM SECURITY
  - Intruders and intrusion detection
  - Malicious Software (viruses)
  - Firewalls and trusted systems

Secure Electronic Transaction (SET)

Secure Electronic Transaction (SET)

- Open encryption and security specification
- Designed to protect credit card transaction, not a payment system
- A set of security protocols & formats
  - secure communications amongst parties
  - trust from use of X.509v3 certificates
  - privacy by restricted info to those who need it
- Initiated and promoted by MasterCard and Visa

SET

- Many companies were involved in the development of the specification (IBM, Microsoft, Netscape, RSA, Verisign, …)
- SET specification consists of three books:
  - Business Description
  - Programmer's Guide
  - Formal Protocol definition

History

- SET is a technical specification for securing the financial transactions on the Internet. On February 1, 1996, Visa International and MasterCard announced together with others (including Microsoft, IBM, Netscape, SAIC, GTE, RSA, Terisa Systems, and VeriSign), the development of a single technical standard for safeguarding credit card purchases made over open networks
- This standard was to be called the SET (Secure Electronic Transaction) TM specification. Prior to this effort, Visa and MasterCard were pursuing separate specifications, and the new SET specification represented a convergence of those individual efforts

History

- In mid December 1997, a new corporate entity called SET Secure Electronic Transaction LLC SETCo was formed by Visa and MasterCard to provide a structure that would govern and direct the future development of the SET Secure Electronic Transaction protocol, as well as other key functions that are required to support the implementation of this standard. In conjunction to this, agreements with American Express and JCB Co., Ltd. to become full partners in SETCo have been negotiated

SET Services

- Confidentiality
  - Cardholder account and payment information is secured as it travels across the network
  - Cardholder account and information (e.g., credit card number) is hidden from the merchant too
- Integrity
  - Messages cannot be altered in transit in an undetectable way
  - Based on digital signatures

SET Services

- Cardholder account authentication
  - Merchant can verify that the client is a legitimate user of the card
  - Based on X.509 certificates
- Merchant authentication
  - Client can authenticate the merchant and check if it is authorized to accept payment cards
  - Based on X.509 certificates

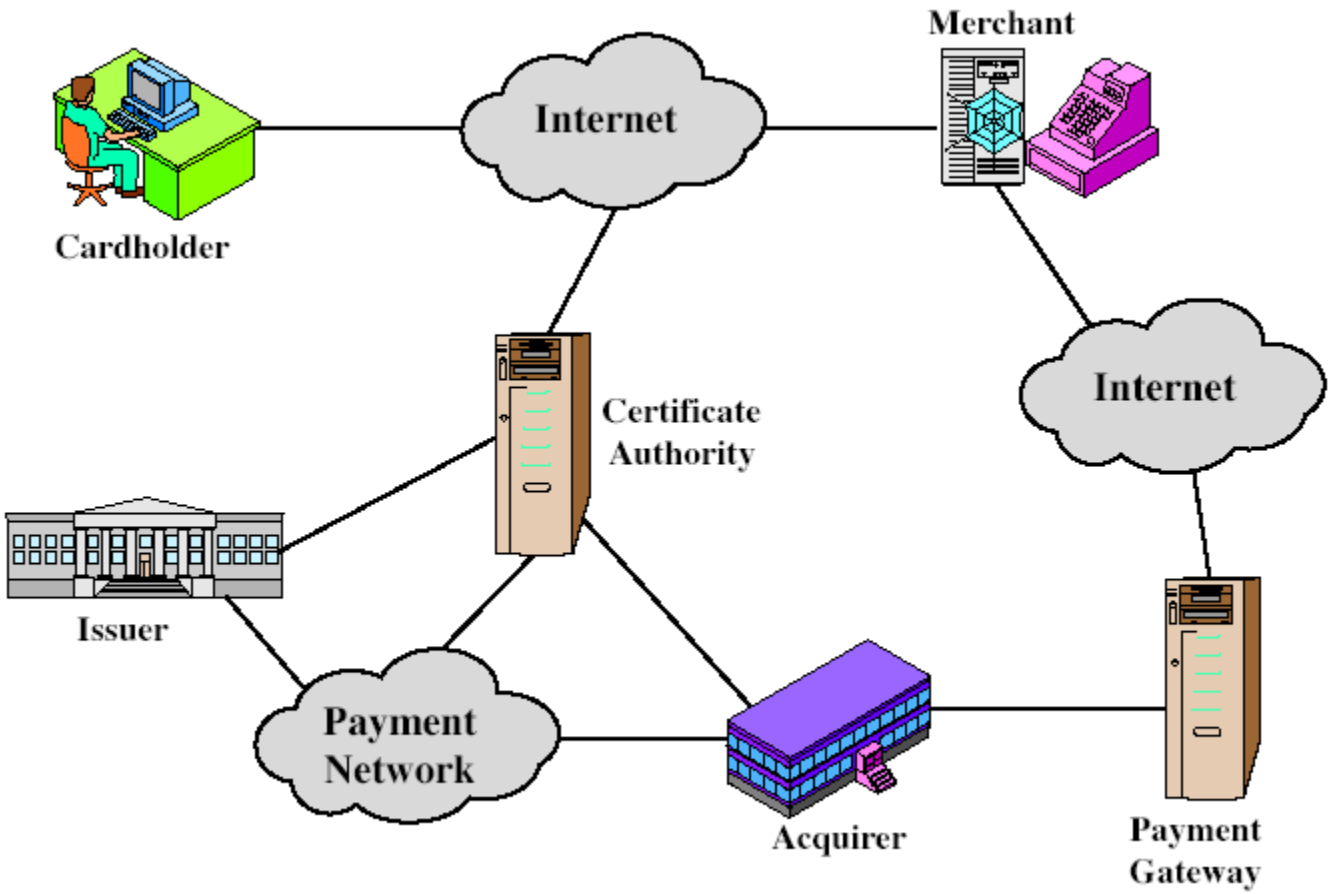
SET Participants

- Cardholder:
  - Wants to buy something on Internet
  - Authorized holder of payment card
- Merchant:
  - Person or organization providing goods or services to cardholder
- Issuer:
  - Financial institute that provides cardholder the payment card
  - Responsible for the payment of debt of the cardholders

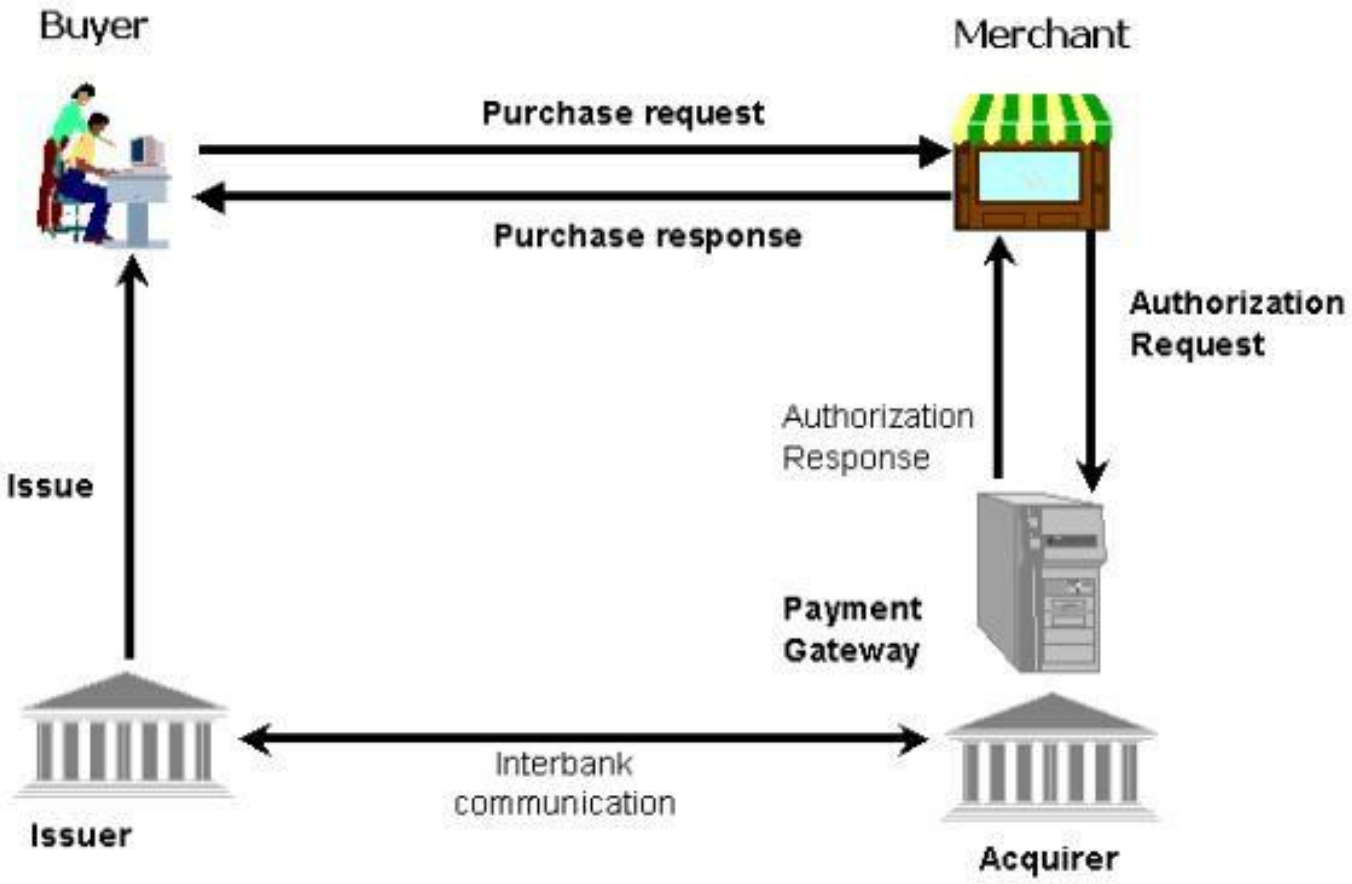
SET Participants

- Acquirer:
  - Financial institute that establishes account with merchant
  - processes payment card authorizations and payments
  - Transfers money to the merchant account
- Payment Gateway:
  - Acquirer or designated third party that processes merchant payment messages
  - Interface between the Internet and the existing bankcard payment network for authorization and payment functions
- Certification Authority:
  - Issues X.509 certificates for cardholders, merchants and payment gateways

SET Components



SET Components



SET Transaction

- Step 1: Customer opens account
  - Obtains the credit card account
- Step 2: Customer receives a certificate
  - X.509 certificate signed by the bank
  - Certificate verifies customer's public key and its expiration date
- Step 3: Merchants have their own certificates
  - Must have two certificates
  - One for signing message, one for key exchange
- Step 4: Customer places an order
  - Customer browses merchant's website
  - Sends a list of items to be purchased
  - Merchant returns an order form, with an order number

SET Transaction

- Step 5: Merchant is verified
  - Merchant sends a copy of certificate with order form
- Step 6: Order and payment are sent
  - Customer sends both order and payment information to merchant
  - Payment contains credit card details
  - Payment information is encrypted in such a way that merchant cannot read it
- Step 7: Merchant requests payment authorization
  - Payment information is sent to payment gateway
  - Checks the credit limit of cardholder
- Step 8: Merchant confirms order

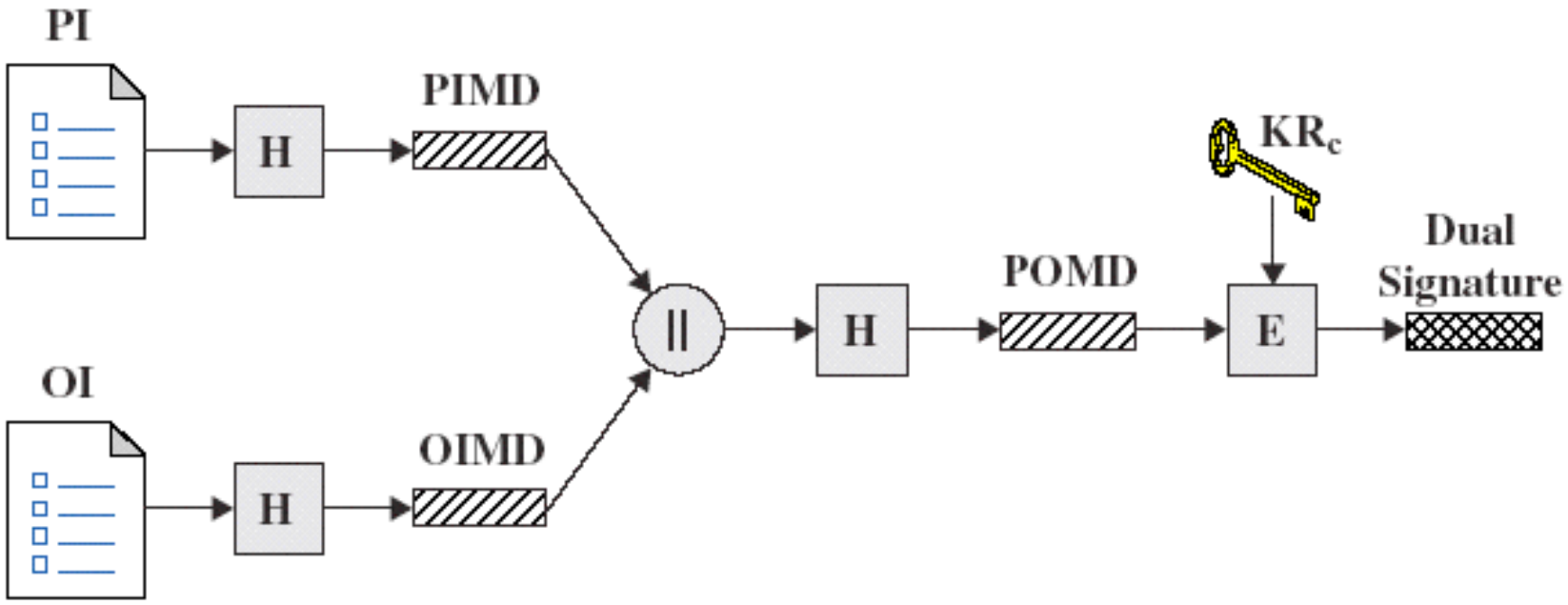
SET Transaction

- Step 9: Merchant provides goods or service
  - Merchant ships the goods to the customer
- Step 10: Merchant requests payment
  - Payment request is sent to the payment gateway

Dual Signature

- Used to link two messages intended for two different recipients
- Customer creates dual messages
  - Order information (OI) for merchant
  - Payment information (PI) for bank
- Neither party needs details of other
- But **must know they are linked**
- Use a dual signature for this
  - Signed concatenated hashes of OI & PI

Dual Signature Construction



PI = Payment Information
OI = Order Information
H = Hash function (SHA-1)
|| = Concatenation

PIMD = PI message digest
OIMD = OI message digest
POMD = Payment Order message digest
E = Encryption (RSA)
KR_c = Customer's private signature key

Dual Signature Construction

- Customer takes the hash of the PI and OI
- Hashes are concatenated and hash of the result is taken
- Hash of the result is taken
- Final hash is encrypted with sender's private key

Payment Processing

- Purchase Request
- Payment Authorization
- Payment Capture

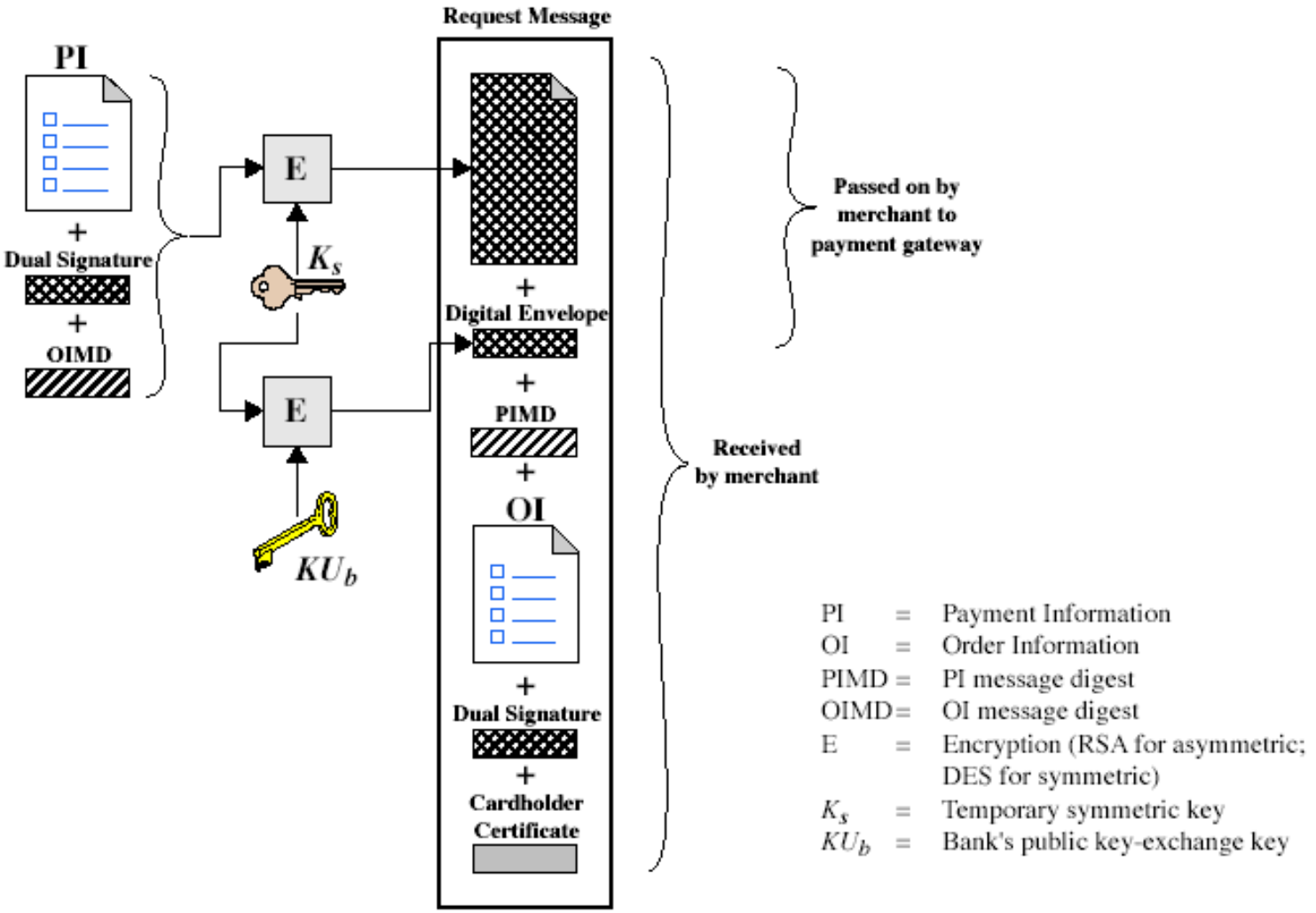
Purchase Request

- Forwarded to payment gateway
- Message consists of
- Purchase Related Information
  - PI
  - Dual Signature
  - OI Message Digest
  - Digital Envelope: Formed by encrypting Session key with Public Key-exchange key of payment gateway

Purchase Request

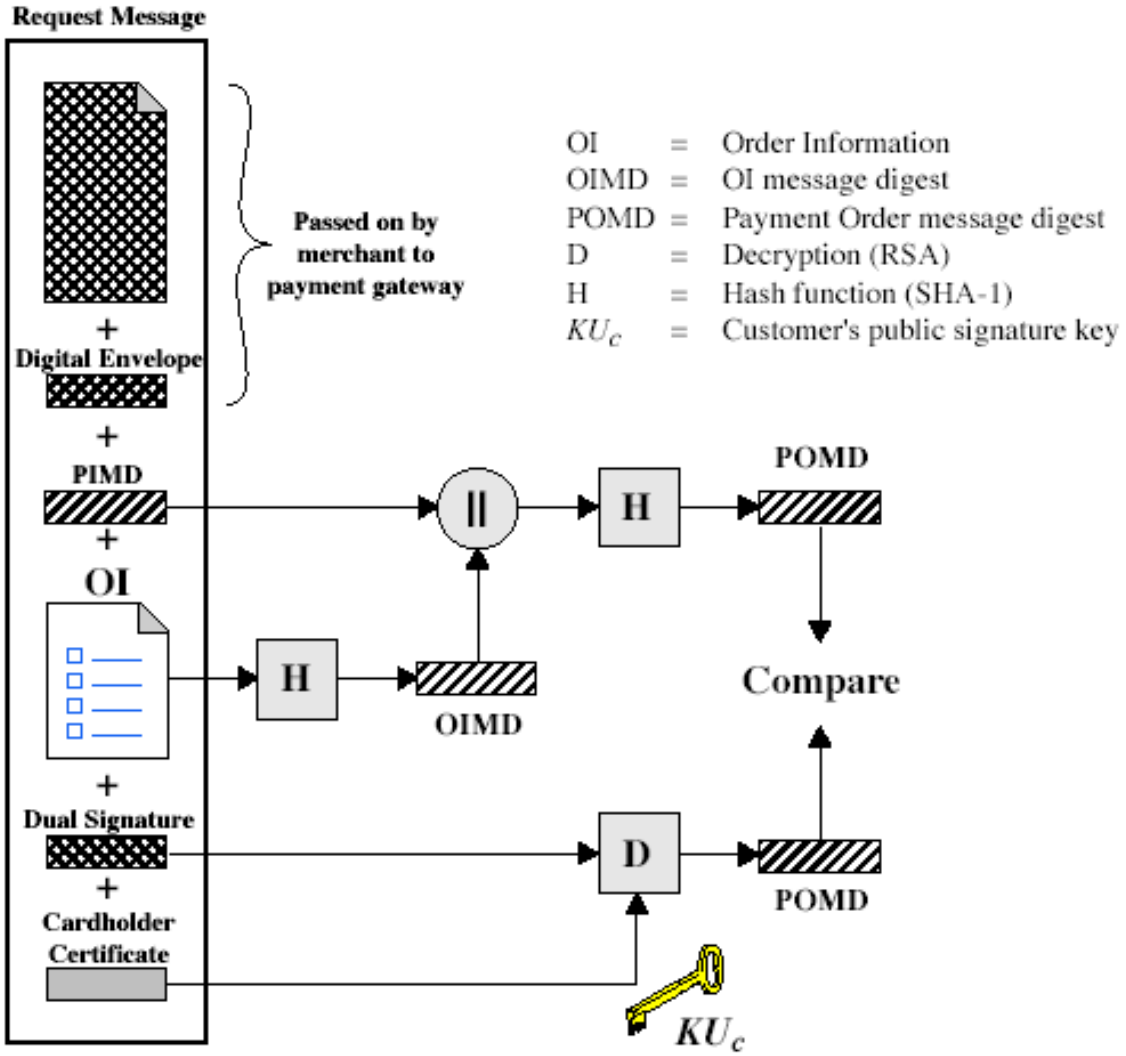
- Order Related Information consists of
  - OI
  - Dual Signature
  - PI message digest (PIMD)
- Cardholder Certificate
  - Contains cardholder's public signature key
  - Needed by merchant and by payment gateway

Purchase Request – Customer



PI = Payment Information
OI = Order Information
PIMD = PI message digest
OIMD = OI message digest
E = Encryption (RSA for asymmetric; DES for symmetric)
K_s = Temporary symmetric key
KU_b = Bank's public key-exchange key

Purchase Request – Merchant



Purchase Request – Merchant

- Verifies cardholder certificates using CA signatures
- Verifies dual signature using customer's public signature key to ensure order has not been tampered with in transit & that it was signed using cardholder's private signature key
- Processes order and forwards the payment information to the payment gateway for authorization (described later)
- Sends a purchase response to cardholder

Payment Gateway Authorization

- Verifies all certificates
- Decrypts digital envelope of authorization block to obtain symmetric key & then decrypts authorization block
- Verifies merchant's signature on authorization block
- Decrypts digital envelope of payment block to obtain symmetric key & then decrypts payment block
- Verifies dual signature on payment block

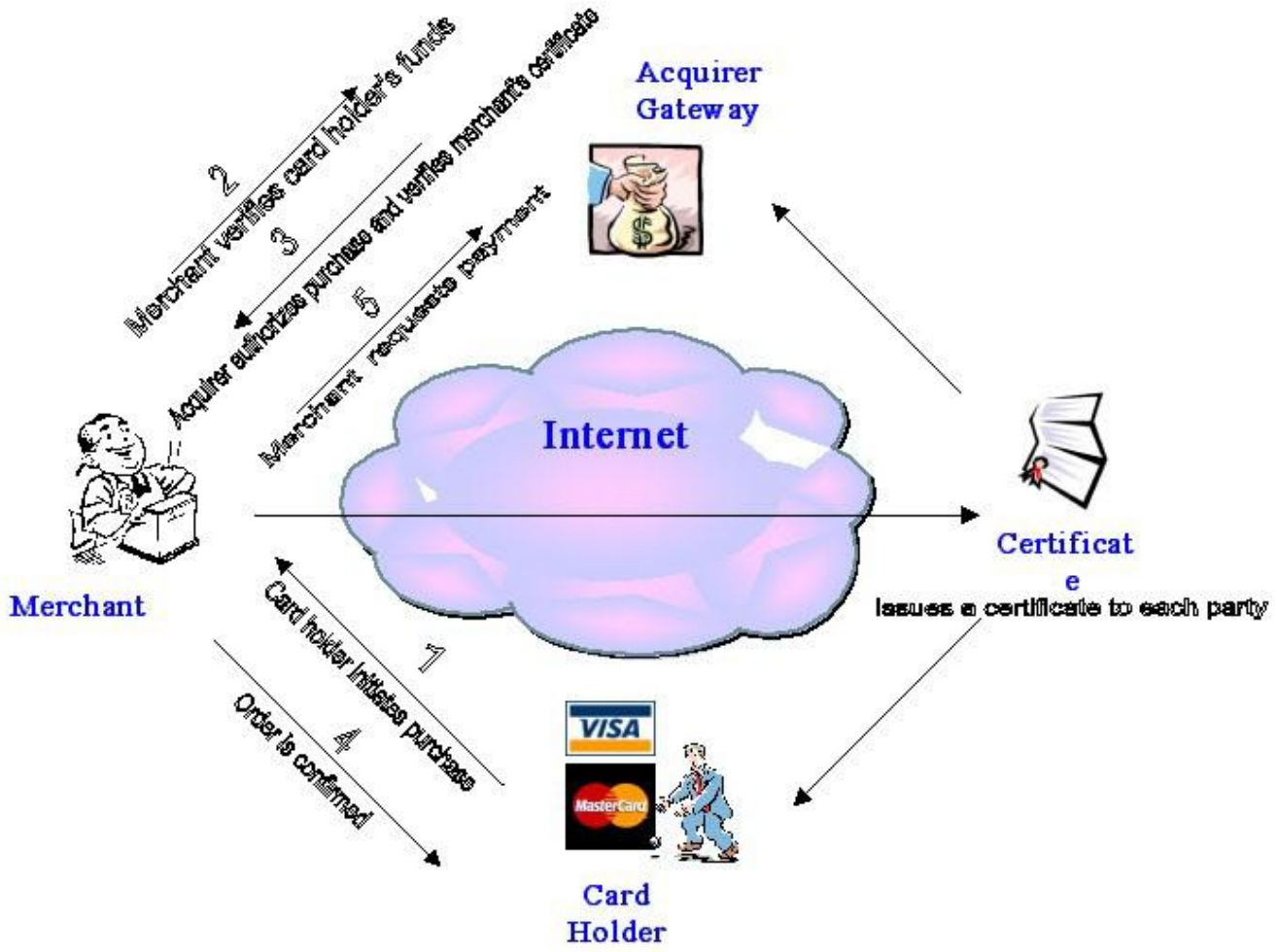
Payment Gateway Authorization

- Verifies that transaction ID received from merchant matches that in PI received (indirectly) from customer
- Requests & receives an authorization from issuer
- Sends authorization response back to merchant

Payment Capture

- Merchant sends payment gateway a payment capture request
- Capture Request includes the payment amount, transaction ID and the token
- Gateway checks and verifies request
- Then causes funds to be transferred to merchants account
- Notifies merchant using capture response

Payment Capture



How Safe is SET?

- With SET, parties involved in a transaction only get information that is necessary for them to complete their side of the transaction. The online merchant does not get the credit card number.
- This goes directly to the credit institution who just informs the merchant whether the transaction has been approved or not.
- SET reduces the risk of the merchant misusing a credit card or accidentally giving access to a hacker.

Any question ?