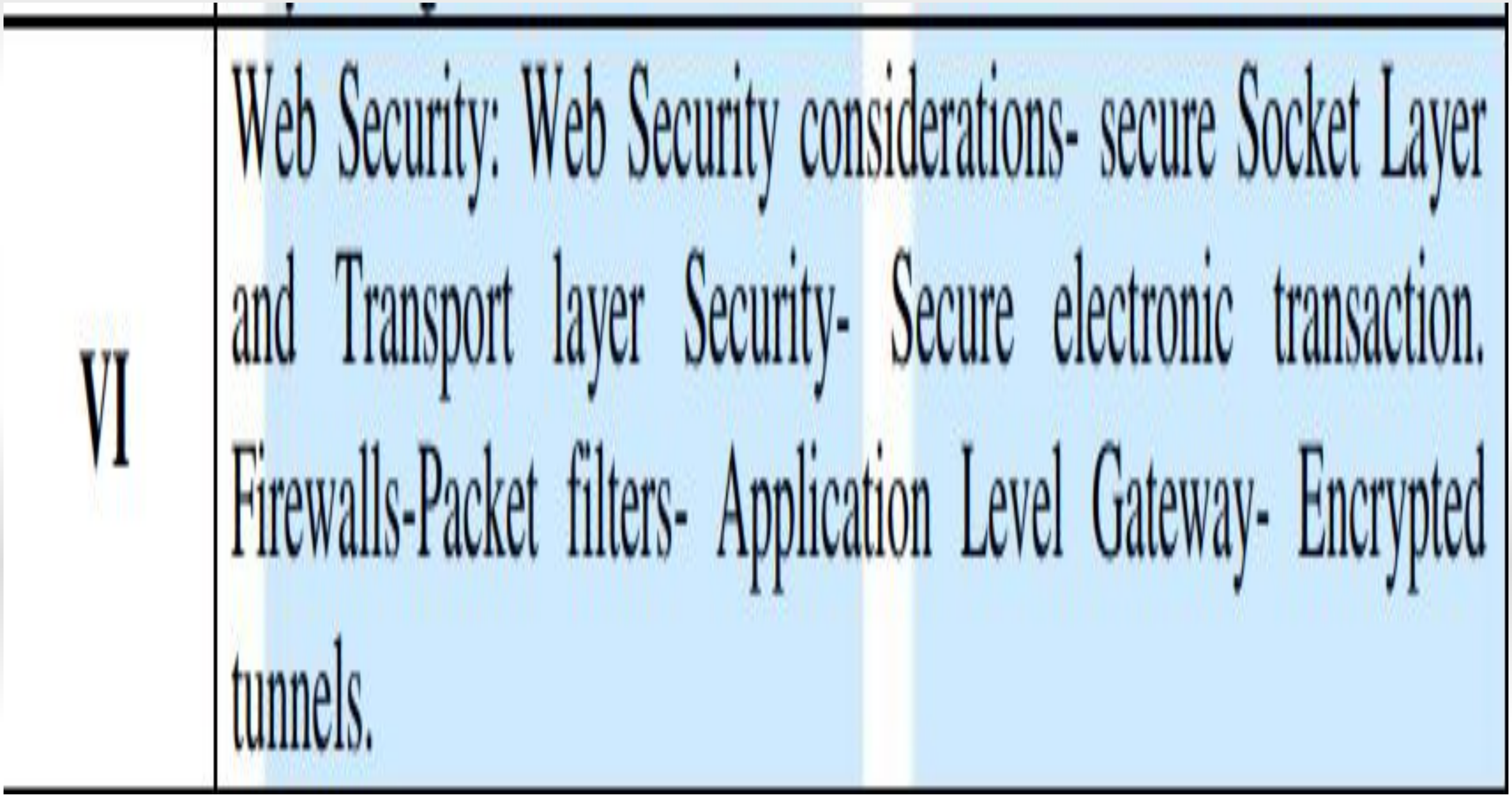


VI	Web Security: Web Security considerations- secure Socket Layer and Transport layer Security- Secure electronic transaction. Firewalls-Packet filters- Application Level Gateway- Encrypted tunnels.

Secure Electronic Transaction

Secure Electronic Transactions (SET)

- open encryption & security specification
- to protect credit card transactions on the Internet
- developed in 1996 by MasterCard, Visa etc

- **Secure Electronic Transaction** or SET is a system that ensures the security and integrity of electronic transactions done using credit cards in a scenario.
- SET is not some system that enables payment but it is a security protocol applied to those payments.
- It uses different encryption and hashing techniques to secure payments over the internet done through credit cards.
- The SET protocol was supported in development by major organizations like Visa, Mastercard, Microsoft which provided its Secure Transaction Technology (STT), and Netscape which provided the technology of Secure Socket Layer (SSL).

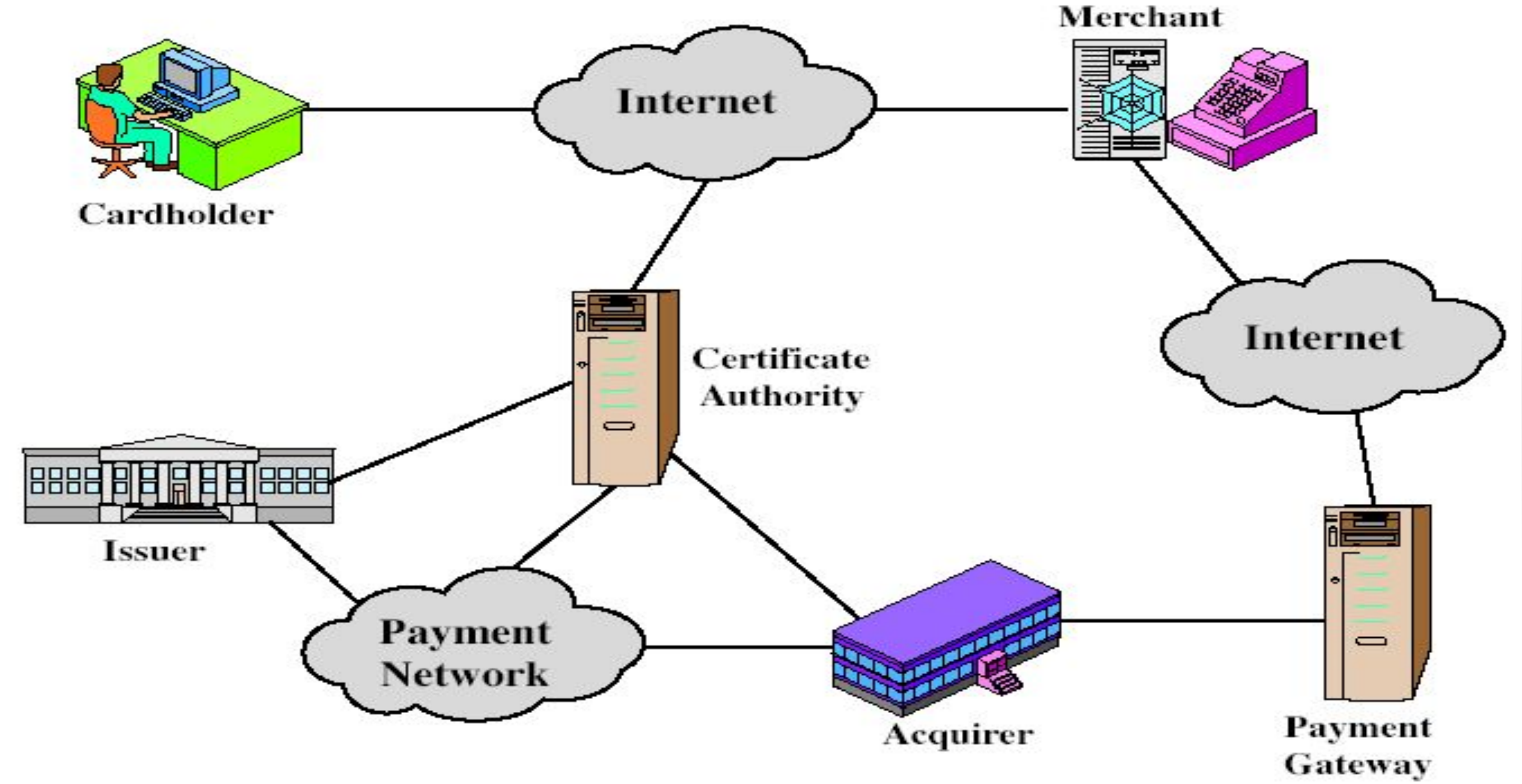
SET

- not a payment system
- rather 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

SET – Key Features

- Confidentiality of the data
- Integrity of the data
- Cardholder account authentication
- Merchant authentication

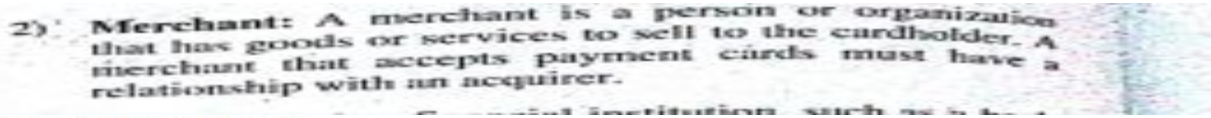
SET Participants



Participants in SET :

In the general scenario of online transactions, SET includes similar participants:

1. **Cardholder -** customer
2. **Issuer -** customer financial institution
3. **Merchant**



2) **Merchant:** A merchant is a person or organization that has goods or services to sell to the cardholder. A merchant that accepts payment cards must have a relationship with an acquirer.

4. **Acquirer -** Merchant financial
5. **Certificate authority -** Authority that follows certain standards and issues certificates(like X.509V3) to all other participants.

- **SET functionalities :**

- **Provide Authentication**
  - **Merchant Authentication** – To prevent theft, SET allows customers to check previous relationships between merchants and financial institutions. Standard X.509V3 certificates are used for this verification.
  - **Customer / Cardholder Authentication** – SET checks if the use of a credit card is done by an authorized user or not using X.509V3 certificates.

- **Provide Message Confidentiality**: Confidentiality refers to preventing unintended people from reading the message being transferred. SET implements confidentiality by using encryption techniques. Traditionally DES is used for encryption purposes.
- **Provide Message Integrity**: SET doesn’t allow message modification with the help of signatures. Messages are protected against unauthorized modification using RSA digital signatures with SHA-1 and some using HMAC with SHA-1,

SET: Sequence of Events

1. Customer opens account with credit card
2. Customer receives a certificate
3. Merchants have their own certificates
4. Customer places an order
5. Merchant is verified
6. Order and payment are sent
7. Merchant requests payment authorization
8. Merchant confirms order
9. Merchant provides goods or service
10. Merchant requests payment

the order.

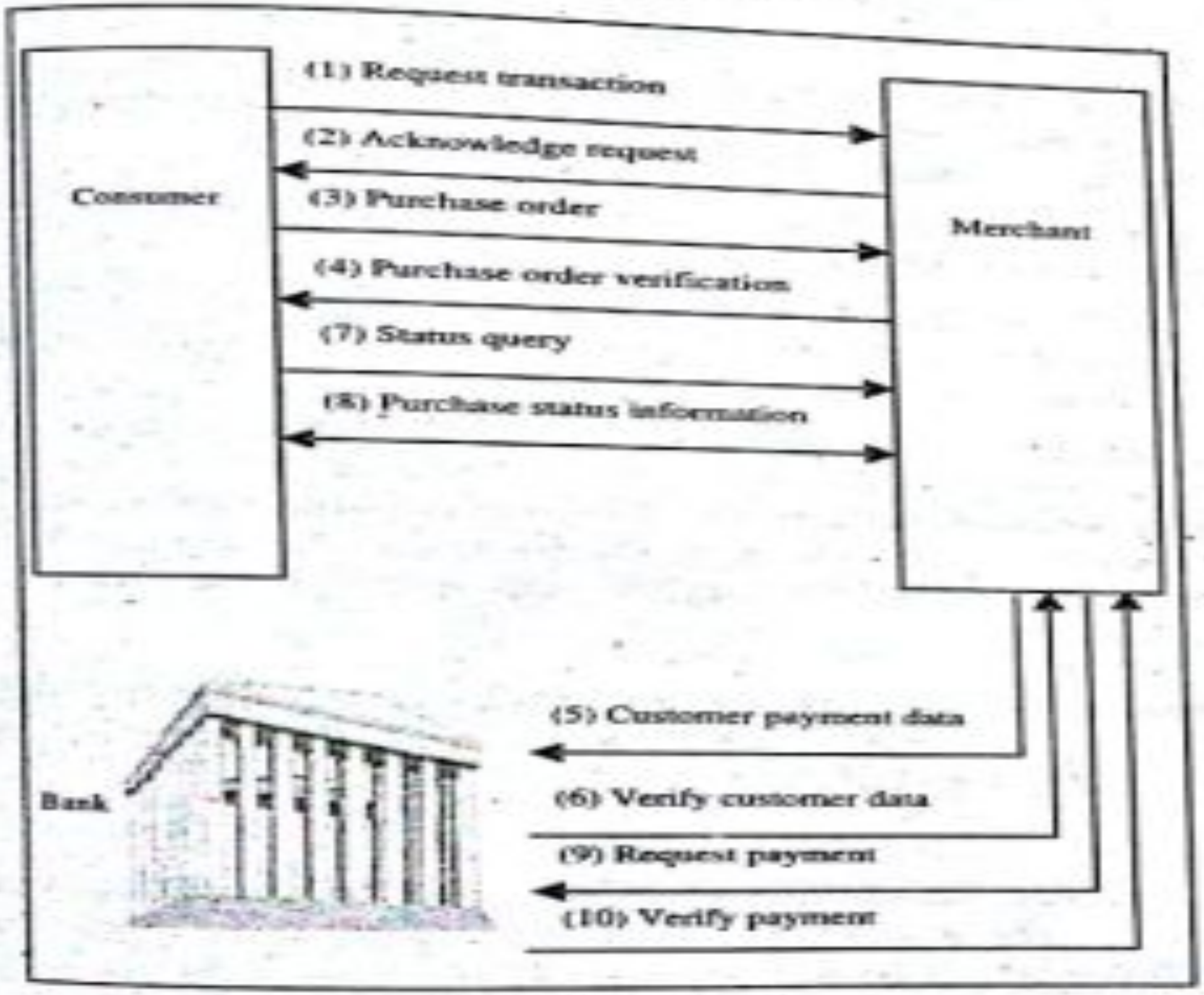
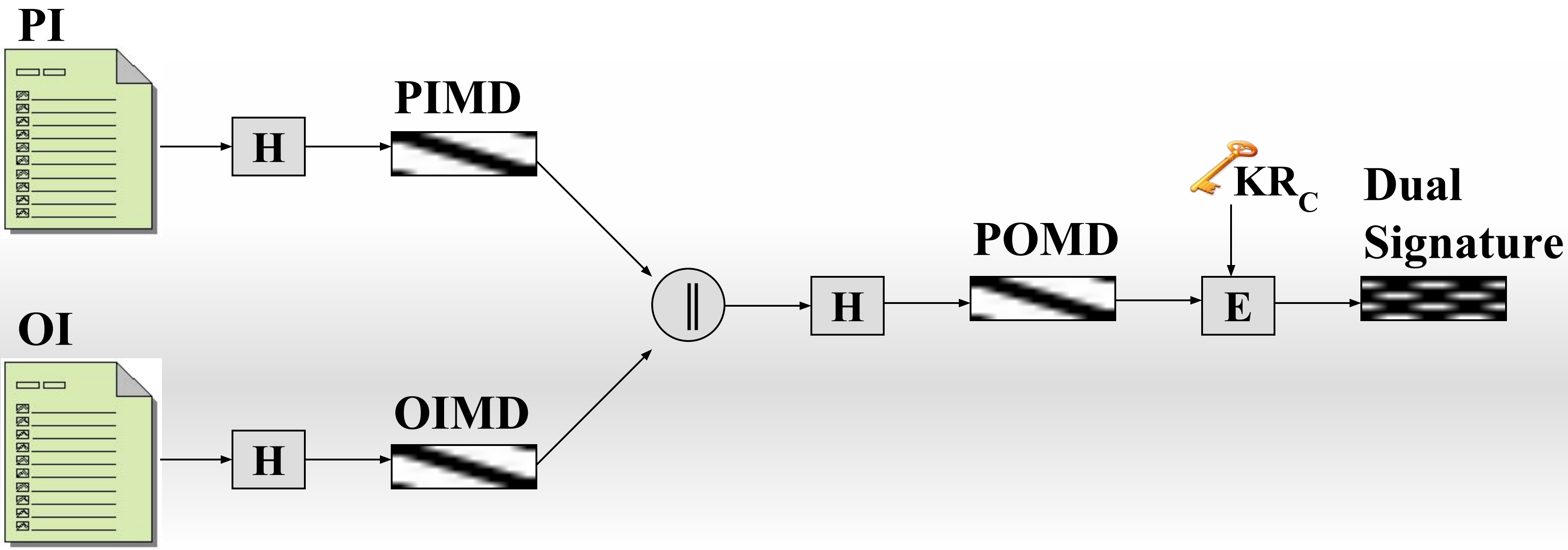


Figure 6.6: SET Operations

Dual Signature



- The dual signature is a concept introduced with SET, which aims at connecting two information pieces meant for two different receivers :
  Order Information (OI) for merchant
  Payment Information (PI) for bank
- You might think sending them separately is an easy and more secure way, but sending them in a connected form resolves any future dispute possible. Here is the generation of dual signature:

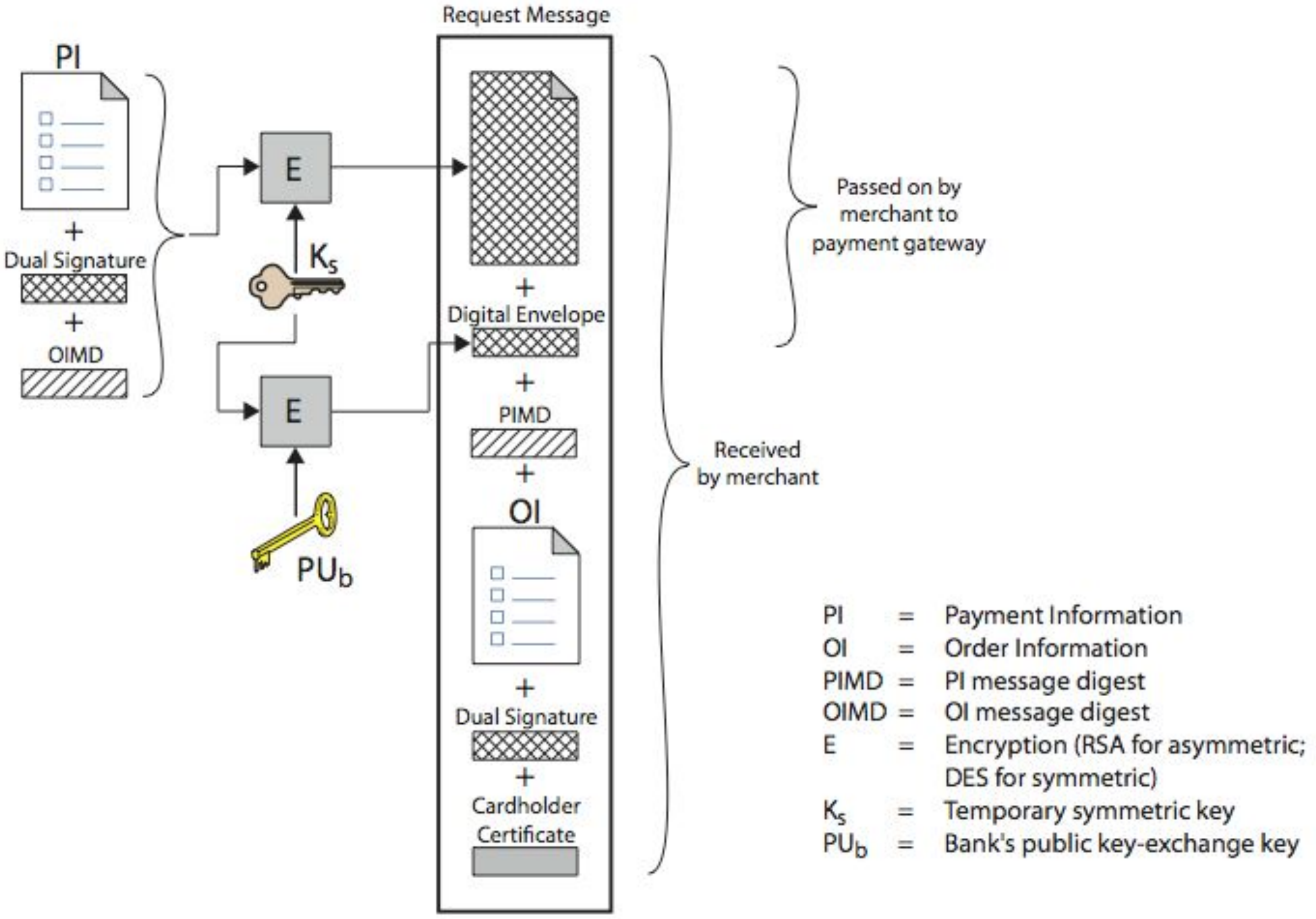
SET Payment Processing

- Purchase request.
- Payment authorization.
- Payment capture.

SET Purchase Request

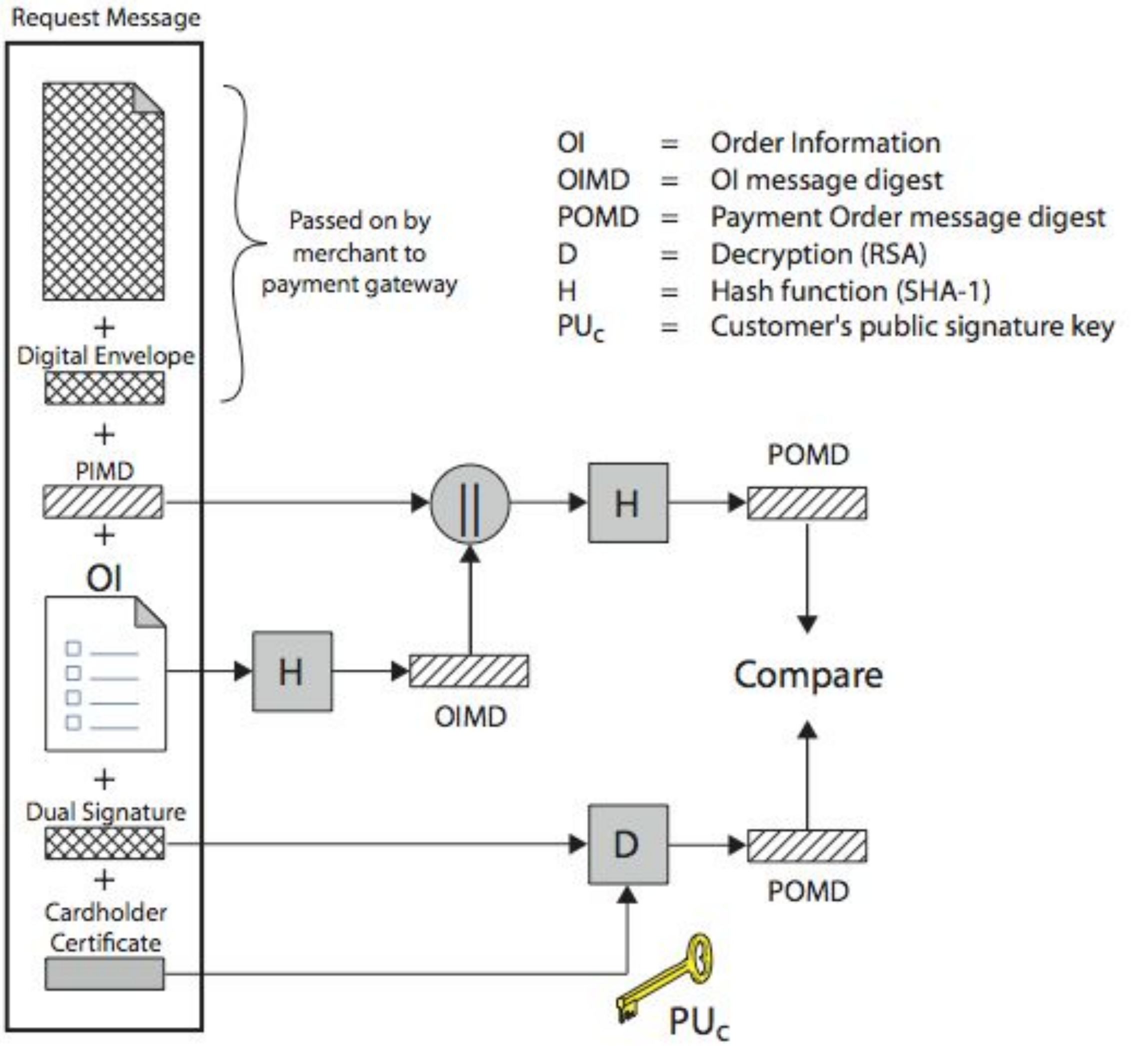
- SET purchase request exchange consists of four messages
  1. Initiate request - get certificates
  2. Initiate response - signed response
  3. Purchase request - of OI & PI
  4. Purchase response - ack order

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
PU_b	=	Bank's public key-exchange key

Purchase Request – Merchant



OI	=	Order Information
OIMD	=	OI message digest
POMD	=	Payment Order message digest
D	=	Decryption (RSA)
H	=	Hash function (SHA-1)
PU_c	=	Customer's public signature key

Purchase Request – Merchant

1. Verifies cardholder certificates using CA signatures
2. 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
3. Processes order and forwards the payment information to the payment gateway for authorization (described later)
4. Sends a purchase response to cardholder

Payment Authorization

- Ensures that the transaction is approved by the issuer
- Guarantee that merchant receive payment
- Consists of two messages:
  1. Authorization request
  2. Authorization response

Authorization Request

1. Purchase-related information [received from custmr]
   - The PI
   - Dual signature
   - OIMD
   - The digital envelop
2. Authorization-related information [merchant gentd]
   - Authorization block
   - A digital envelop
3. Certificates

Payment Gateway Authorization

1. verifies all certificates
2. decrypts digital envelope of authorization block to obtain symmetric key & then decrypts authorization block
3. verifies merchant's signature on authorization block
4. decrypts digital envelope of payment block to obtain symmetric key & then decrypts payment block
5. verifies dual signature on payment block
6. verifies that transaction ID received from merchant matches that in PI received (indirectly) from customer
7. requests & receives an authorization from issuer
8. sends authorization response back to merchant

Authorization Response

- Authorization-related information
- Capture token information
- Certificate

Note:-With the authorization from the gateway, the merchant can provide the goods and services to the customer.

Payment Capture

- Merchant sends payment gateway a payment capture request
- Gateway checks request
- Clearing request send to the issuer.
- Funds are transferred to merchants account
- Notifies merchant using capture response