E-commerce security: SSL/TLS, SET and others.

4.2

Universidad Carlos III de Madrid
Grupo SeTI · Dpto. Informática

The need of authenticated payment

- SSL protects credit card details while they are transmitted through Internet but…
  - Why trust the Merchant? Once credit card details are obtained, fraud can be performed with them
  - Why trust the Cardholder? Fake credit card details can be sent to honest Merchant

SET: Secure Electronic Transaction

- Open encryption and security specification.
- Designed to protect credit card transactions on the Internet
- Involved companies:
  - MasterCard, Visa, IBM, Microsoft, Netscape, RSA, Terisa and Verisign
- Is not itself a payment system
- Establishes a set of security protocols and formats that enable users to employ the existing credit card payment infrastructure on an open network in a secure fashion

SET: Secure Electronic Transaction

- Main services:
  - Provides a secure communications channel among all parties involved in a transaction
  - Provides trust by the use of X.509v3 certificates
  - Ensures privacy (information is only available to parties when and where necessary)

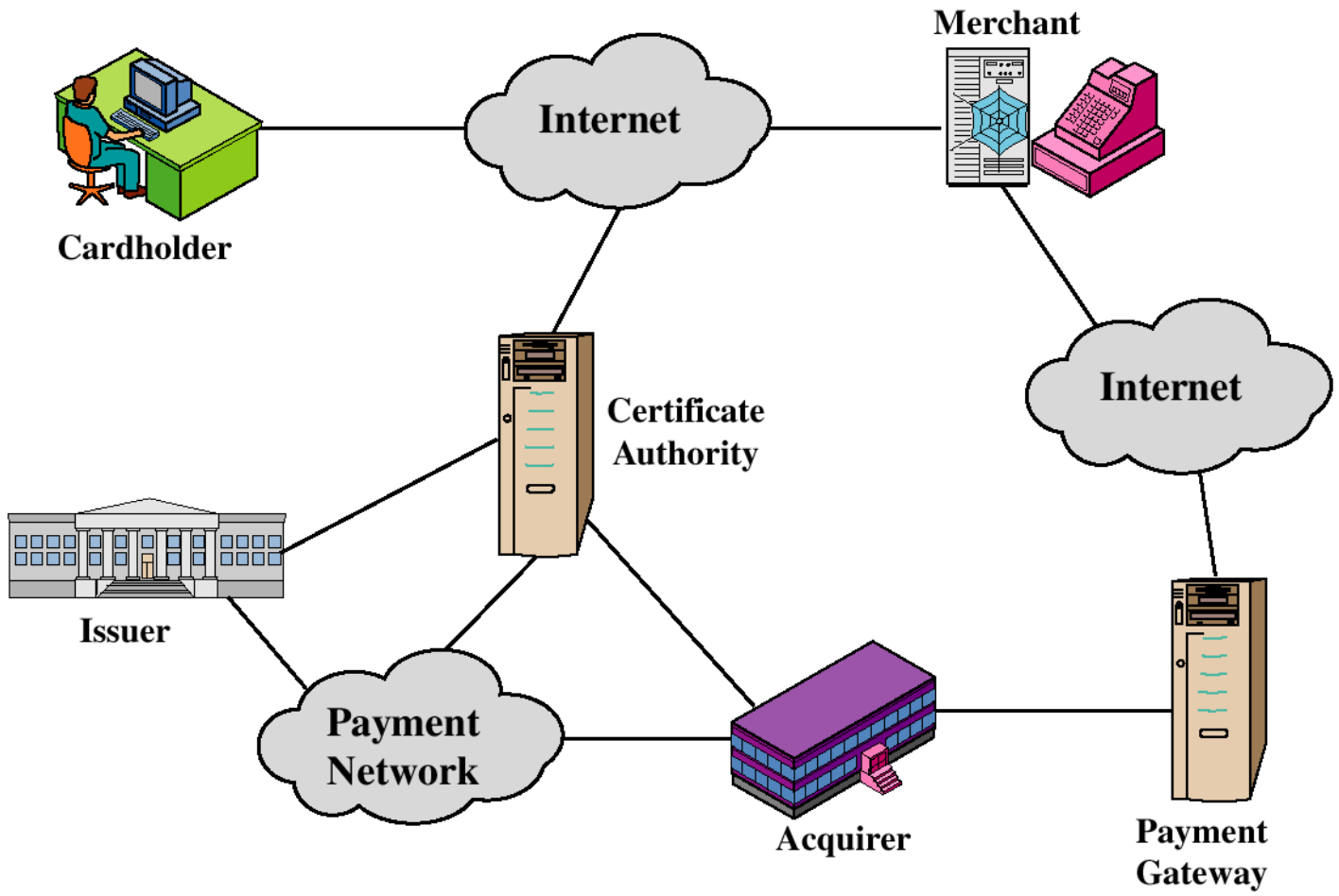
SET: Players

- Cardholder (= Consumer)
  - Authorized holder of payment card
- Merchant (= Commerce)
  - Selling goods or services
- Issuer (= Consumers bank)
  - Financial institution, provides payment cards
  - Responsible for payment of debt of cardholder
- Acquirer (= Merchants bank)
  - Financial institution, gives account to merchant, processes payments, transfers payments to merchants account.

SET: Players

- Payment Gateway
  - Played by the acquirer or third party
  - Interface between SET and existing bankcard payment networks for authorization and payment functions
  - Merchant exchanges SET messages with payment gateway over Internet
  - Payment gateway has some direct connection with the acquirer's financial processing system
- Certification Authority
  - Issues X.509v3 certificates for cardholders, merchants and payment gateways
  - Success of SET depends on available CA infrastructure

SET: Players



Source: W. Stallings and L. Brown. Slides of Chapter 17. Cryptography and Network Security. 4th edition.

SET: Services

Confidentiality of information

- The merchant does not know the cardholders account (including credit card number) and payment information
- Conventional encryption by DES

Integrity of data

- Order information, personal data and payment instructions
- RSA digital signatures using SHA-1 hash codes
- HMAC using SHA-1

SET: Services

Cardholder account authentication

- Merchants (through Payment Gateway) can verify that a cardholder is a legitimate user of a valid account number
- X.509v3 certificates with RSA signatures

Merchant authentication

- Cardholders can verify that a merchant has a relationship with a financial institution for accepting payment cards
- X.509v3 certificates with RSA signatures

SET Transaction Flow

1. Customer opens account
   - Credit card account (VISA, MasterCard...)
   - With a bank supporting electronic payment + SET
2. Customer receives a certificate
   - Signed by the bank
   - Links customer's key pair and credit card (hash of)
3. Merchants have their own certificates (for each card brand)
   - One key pair for signing messages
   - One key pair for key exchange

SET Transaction Flow

4. Customer places an order
   - Merchant returns an order form (list of items, price)
   - Merchant sends also the customer its certificate
5. Merchant is verified
6. Order and payment are sent
   - Payment contains credit card details
   - Payment is encrypted so merchant is prevented from reading credit card info
   - Customer's certificate is also sent to enable merchant to verify customer

SET Transaction Flow

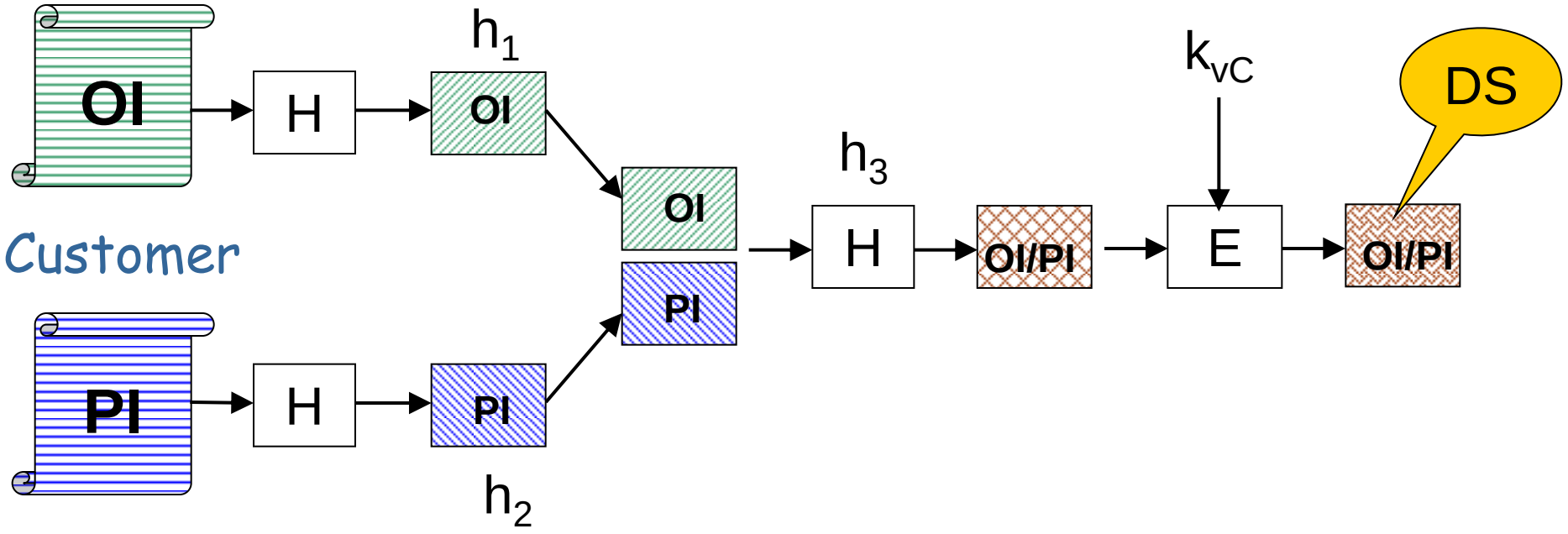
7. Merchant requests payment authorization
   - To the payment gateway

   If the payment is authorized:
8. Merchant confirms order
   - To the customer
9. Merchant provides goods or service
10. Merchant requests payment
    - To the payment gateway, who handles details
      - Customer is billed
      - Merchant is payed

SET: Dual Signature

- Not multiple signature
- Goal: link two messages intended for two different recipients
- Cardholder calculates the hashes of OI and PI (H(OI) and H(PI))
- Cardholder signs both OIMD and PIMD
  - OI and PI get linked
- To verify the dual signature:
  - Merchant receives OI plus H(PI) (PI is not known)
  - Payment Gateway receives PI plus H(OI) (OI is not known)

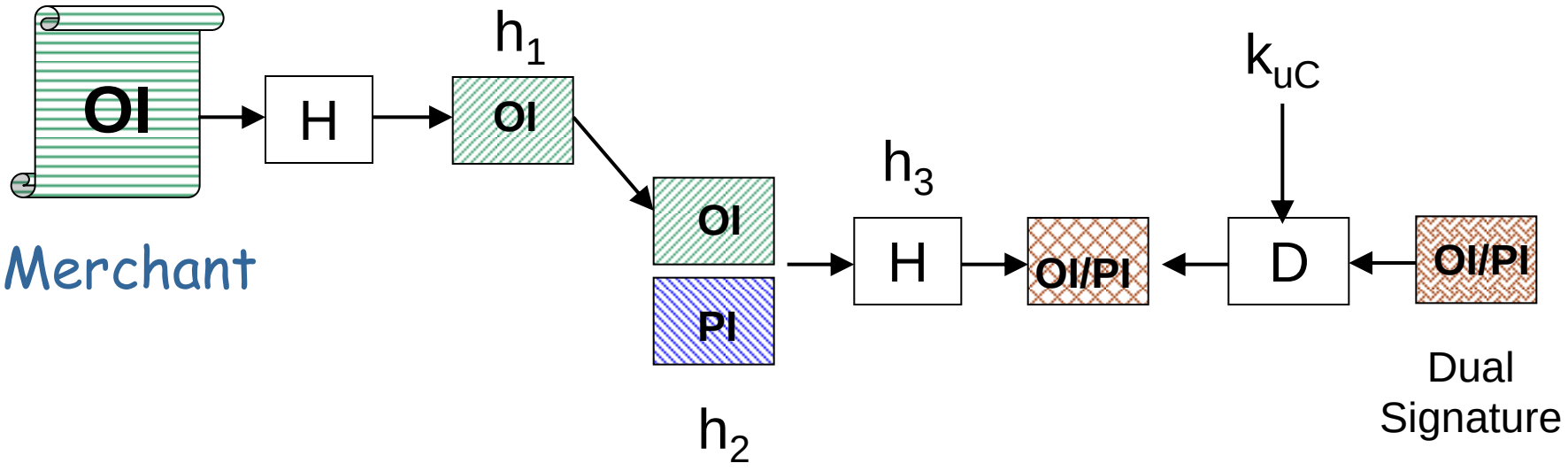
SET: Dual Signature - Generation



$h_1 = H(OI)$ $h_2 = H(PI)$ $h_3 = H(H(OI)||H(PI))$

$DS = E_{kvC}(H(H(OI)||H(PI))$

SET: Dual Signature - Verification



Create $h_1 = H(OI)$ → create $h_3 = H(H(OI)||H(PI))$

→ Decrypt DS: $D_{KuC}(DS) = h_3$ → compare

SET: Digital envelopes

- Message data M is encrypted using a randomly generated key k_s
  - E (k_S, M)
- "Digital envelope" of the message M refers to the key k_s being further encrypted using the recipient's public key k_{uR}
  - E (k_{uR}, k_S)
- Both items are sent to the recipient:
  - E (k_S, M) || E (k_{uR}, k_S)
- The recipient decrypts the digital envelope using a private key k_{vR} and then uses the symmetric key to unlock the original message

SET: Main transaction types

1. Purchase request
2. Payment authorization
3. Payment capture

SET: Purchase Request

- Four messages:
  - C -> M: Initiate Request
  - M -> C: Initiate Response
  - C -> M: Purchase Request
  - M -> C: Purchase Response

SET: Purchase Request

Step 1:

- Cardholder requests certificates from merchant and payment gateway
- Message includes:
  - brand of customers credit card
  - message identification number (ID)
  - non-repeatable number, N_C

SET: Purchase Request

Step 2:

- The non-repeatable number, N_C
- A non-repeatable number produced by the merchant, N_M
- A transaction identifier, TID
- Signed response: $E(k_{vM}, (N_C \| N_M \| TID))$ sent together with:
  - Signature certificate of Merchant, C_{SM}
  - Key exchange certificate of the Payment Gateway, C_{CPG}

SET: Purchase Request

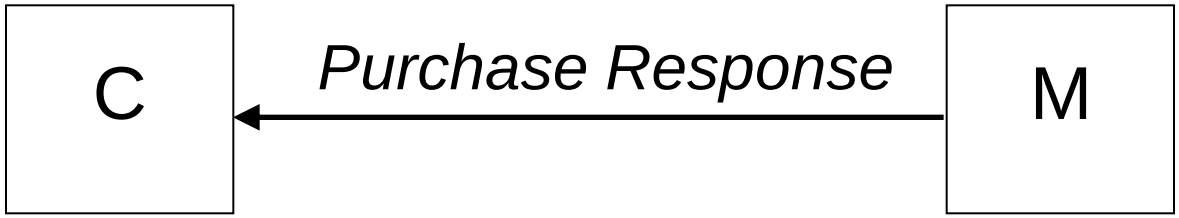
Step 3:

- Cardholder creates OI, PI (both with TID), session key k_S, DS and sends to merchant:
  1. Order related information:
     - OI || DS || H (PI)
  2. Payment related information:
     - E (k_S, (PI || DS || H (OI))) || E (k_{uPG}, k_S)
  3. Signature cardholder certificate, C_{SC}

passed on by merchant to PG

SET: Purchase Request

Step 4:

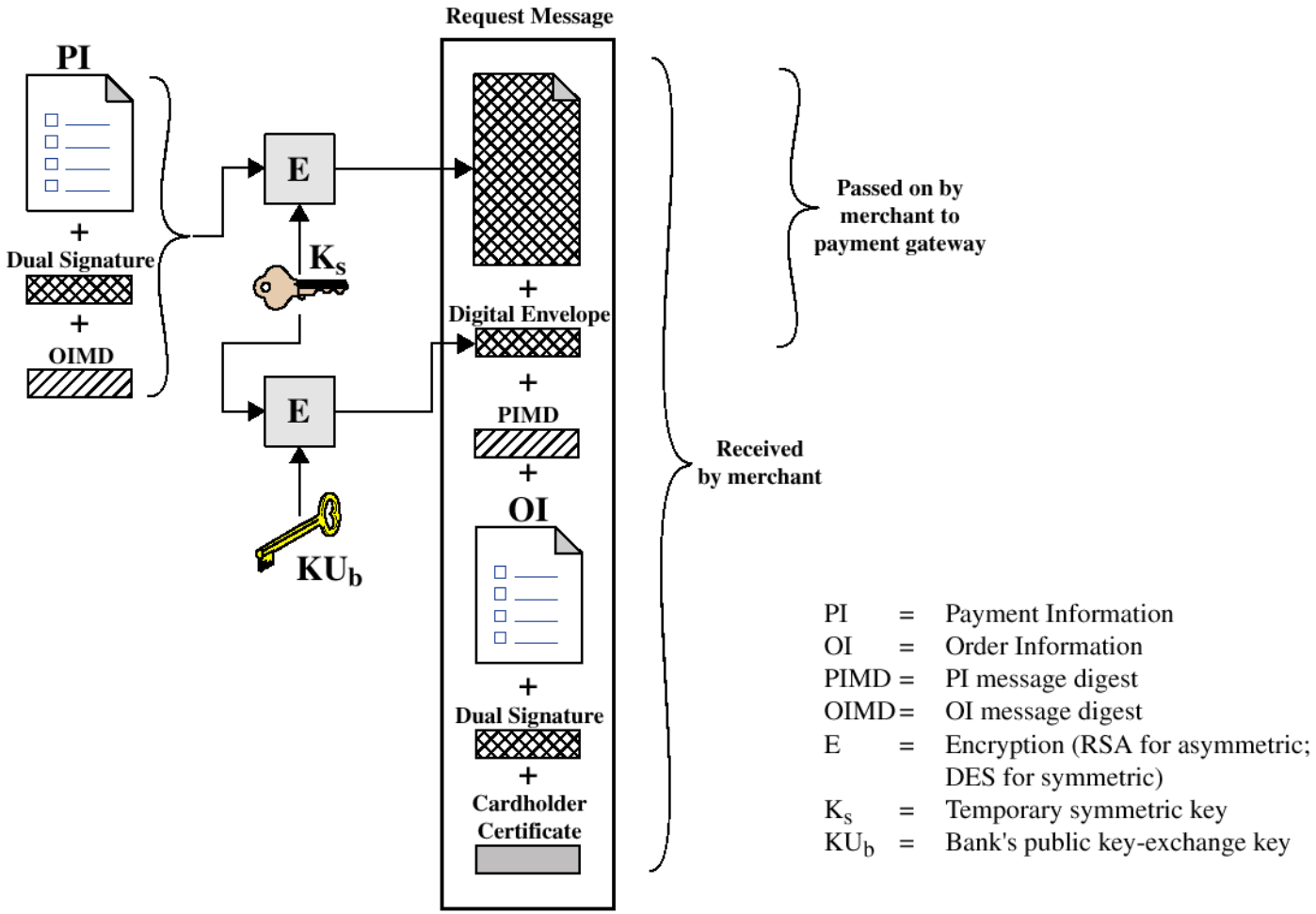


- Merchant after…
  - verifying Cardholder certificates and Dual Signature using k_{uC}
  - processing the order
  - forwarding the payment information to PG for authorization

…sends purchase response to Customer, including:

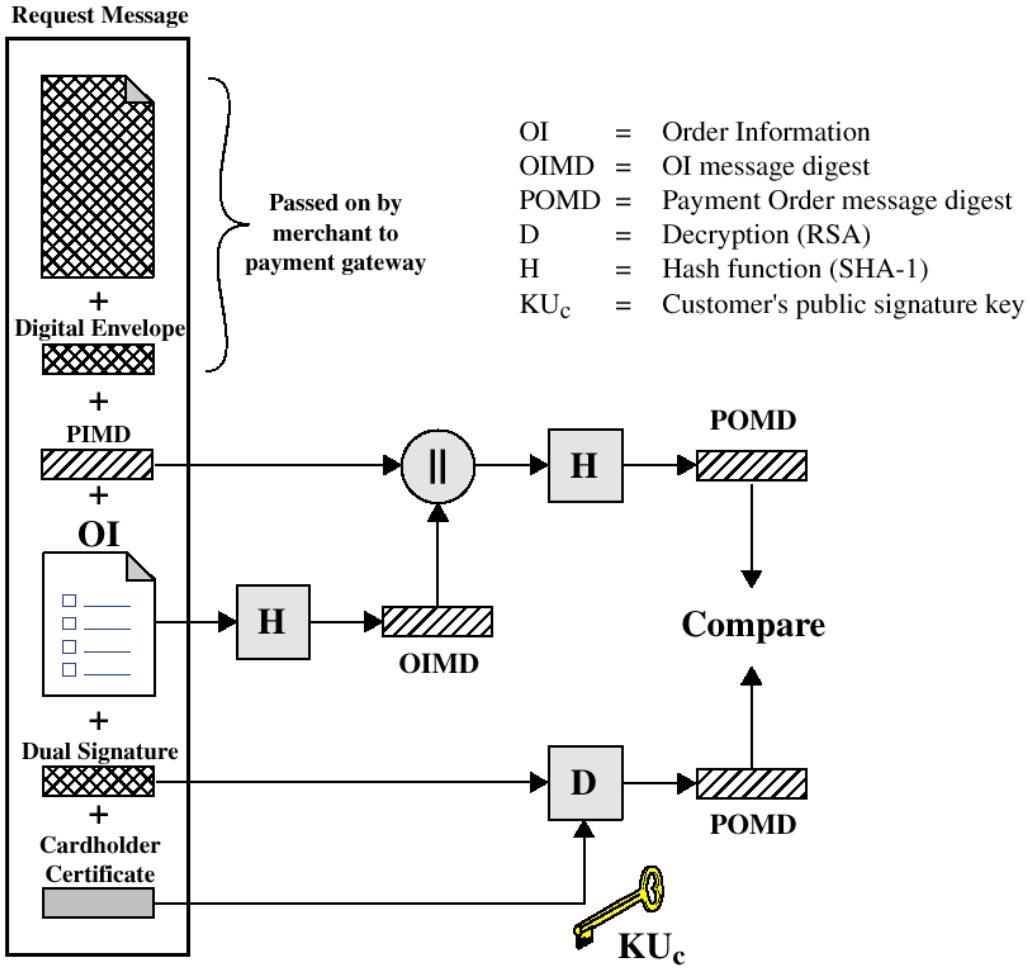
- Transaction identifier (TID), order acknowledge OACK, the signature of both, and merchant's signature certificate (C_{SM}):
  - $E(k_{vM}, (OACK \,||\, TID)), C_{SM}$

SET: Purchase Request Generation



Source: W. Stallings and L. Brown. Slides of Chapter 17. Cryptography and Network Security. 4th edition.

SET: Purchase Request Verification



Source: W. Stallings and L. Brown. Slides of Chapter 17. Cryptography and Network Security. 4th edition.

SET: Payment Authorization

- Two messages:
  - M -> PG: Authorization Request
  - PG -> M: Authorization Response

SET: Payment Authorization

- Step 1:

- Purchase related info
  - $E(k_s, (PI \,||\, DS \,||\, H(OI))) \;||\; E(k_{uPG}, k_s)$
- Authorization related info of Merchant (AI_M)
  - $AI_M = E(k_{sM}, (TID \,||\, E(k_{vM}, TID))) \,||\, E(k_{uPG}, k_{sM})$
- Certificates: $C_{SC} \,||\, C_{SM} \,||\, C_{CM}$

SET: Payment Authorization

- The Payment Gateway performs:
  - Verifies certificates
  - Decrypts digital envelope for AI_M: k_S
  - Decrypts AI_M
  - Verifies merchant's digital signature on AI_M
  - Decrypts digital envelope for PI: k_{sM}
  - Decrypts PI
  - Verifies customer's dual signature
  - Verifies merchant's and customer's TID match
  - Requests and receives and authorization from the issuer

SET: Payment Authorization

Step 2:

- Authorization related info of Payment Gateway, AI_{PG}
- Capture token information, CTI
- C_{SPG}
- $AI_{PG} = E(k_{sPG}, (A \,||\, E(k_{vPG}, A))) \,||\, E(k_{uM}, k_{sPG})$
- $CTI = E(k_{sPG}, (CT \,||\, E(k_{vPG}, CT))) \,||\, E(k_{uM}, k_{sPG})$
- A: Authorization, CT: Capture Token

SET: Payment Capture

- Two messages:
  - M -> PG : Capture Request
  - PG -> M: Capture Response

SET: Payment Capture

Step 1:

- CRqB = Q || TID || CTI; Q: Quantity of purchase
- E ($k_{s'M}$, (CRqB || E (k_{vM}, CRqB))) || E (k_{uPG}, $k_{s'M}$)
- C_{SM} , C_{CM}

SET: Payment Capture

- The Payment Gateway performs:
  - Decrypts and verifies capture request block (CRqB)
  - Decrypts and verifies capture token info (CTI)
  - Checks for consistency between CRqB and CTI
  - Creates a clearing request that is sent to the issuer over the private payment network
  - Then, funds are transfered to merchant's account

SET: Payment Capture

Step 2:

- E (k_{vPG}, (CRsB))
- C_{SPG}
- Merchant stores the capture response to be used for reconciliation with payment received from the acquirer

SET: Non repudiation

- Authentication is achieved by the use of digital signatures
- This helps to provide non-repudiation

SET in Practice

- High computational costs:
  - Number of messages
  - Digital signatures, RSA encryption/decryption cycles, DES encryption/decryption cycles, certificate verifications
- Cardholder side:
  - Install SET software for cardholder wallet
  - Arrange credit card account (supporting SET, providing certificate)
- Merchant side:
  - Install software for merchants selling point and integrate it into web-based ordering system
- Payment gateway
  - Install software for payment gateway server