Secure Electronic Transaction (SET) Protocol

19CSE311 Computer Security

Jevitha KP

Department of CSE

Secure Electronic Transaction (SET) Protocol

- **Secure Electronic Transaction** or SET is a system that ensures the **security and integrity of electronic transactions done using credit cards.**

- It uses different **encryption and hashing techniques** to secure payments over the internet done through credit cards.

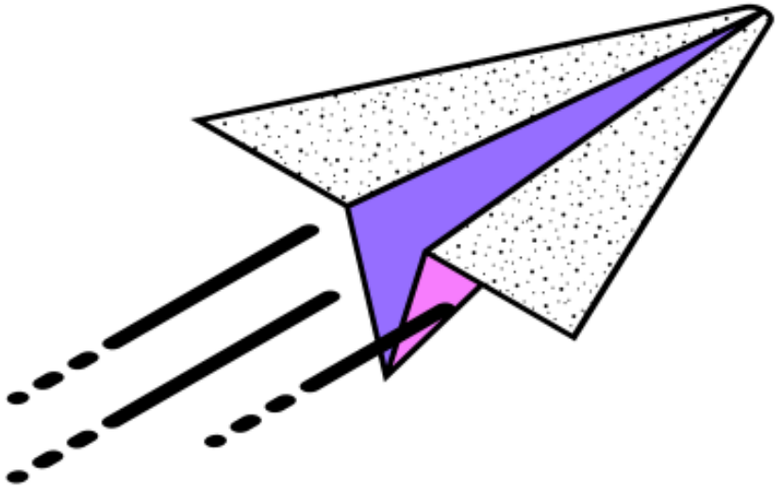
- The SET protocol was supported in development by major organizations like Visa, Mastercard, Microsoft which provided its Secure Transaction Technology (STT), and Netscape which provided the technology of Secure Socket Layer (SSL).

Secure Electronic Transaction (SET) Protocol

- SET protocol restricts the revealing of credit card details to merchants thus keeping hackers and thieves at bay.

- The SET protocol includes **Certification Authorities** for making use of standard Digital Certificates like X.509 Certificate.

Key Features of SET



- Confidentiality
- Integrity
- Cardholder Account Authentication
- Merchant Authentication
- Privacy

Requirements in SET

- The SET protocol has some requirements to meet, some of the important requirements are :

  - It has to provide **mutual authentication** i.e., customer (or cardholder) authentication by **confirming if the customer is an intended user or not**, and **merchant authentication**.

  - It has to keep the **PI (Payment Information) and OI (Order Information)** confidential by appropriate encryptions.

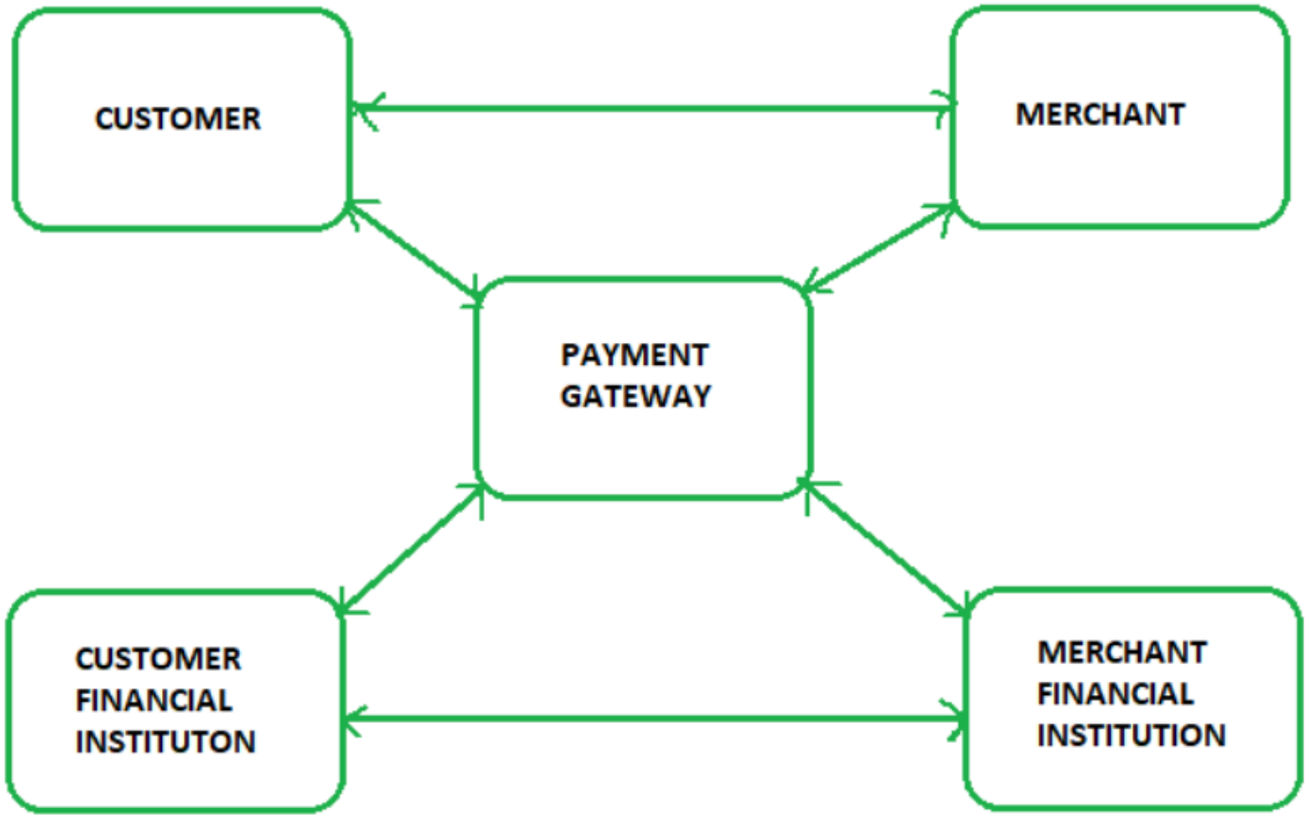
  - It has to be resistive against message modifications i.e., no changes should be allowed in the content being transmitted.

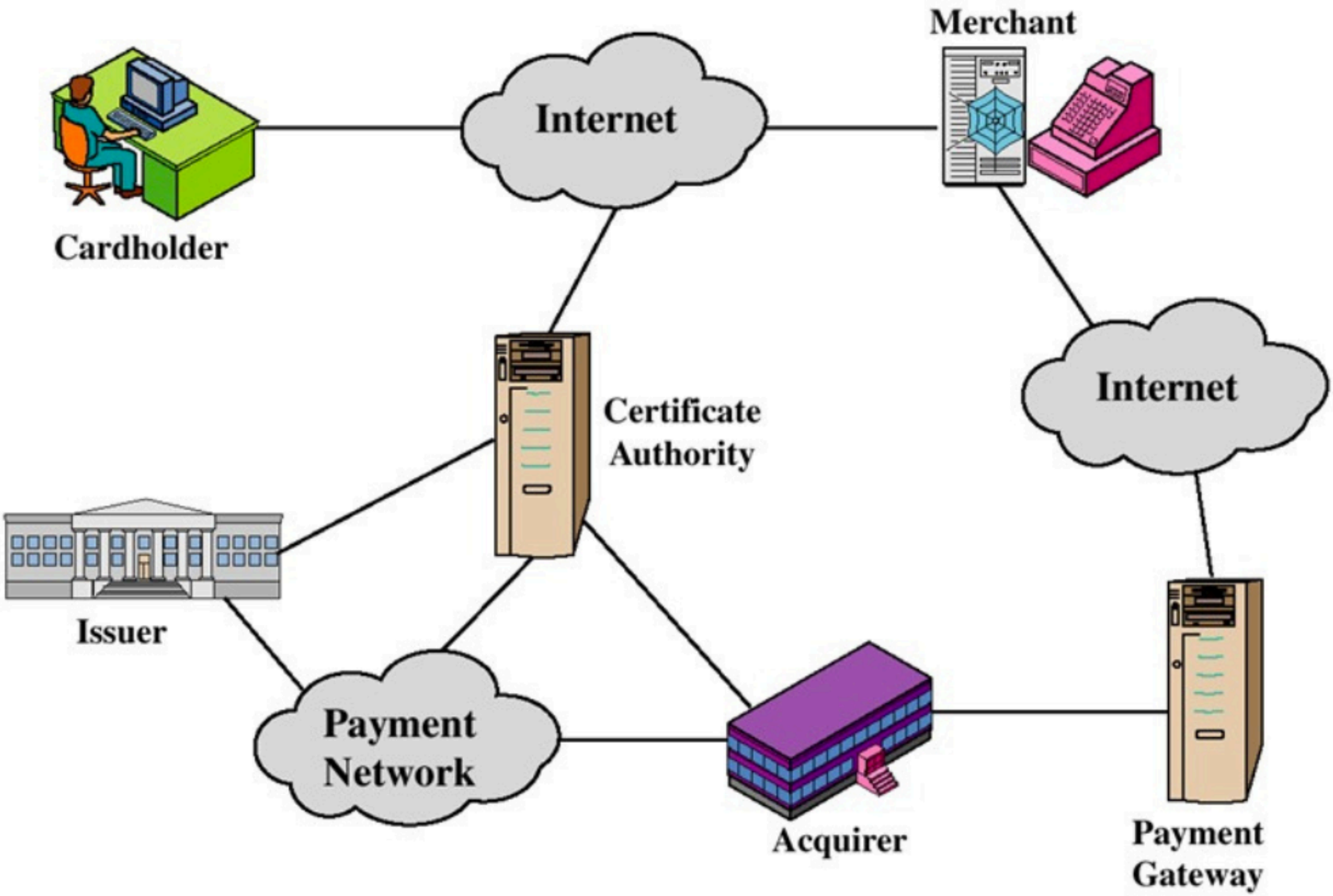
  - SET also needs to provide interoperability and make use of the best security mechanisms.

Participants in SET

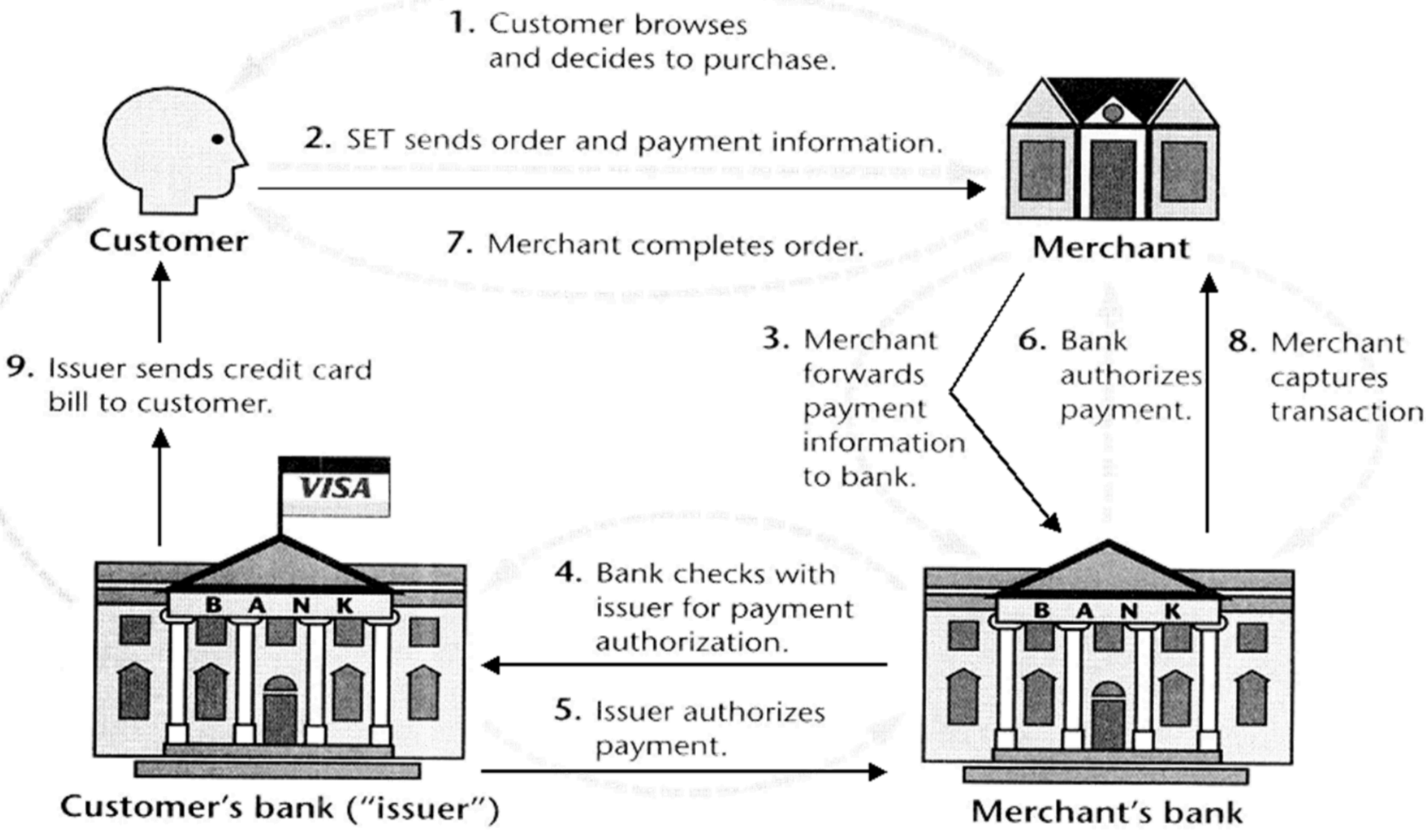
- Cardholder – customer
- Issuer – customer financial institution
- Merchant
- Acquirer – Merchant financial institution
- Payment Gateway
- Certificate authority – Authority that follows certain standards and issues certificates(like X.509v3) to all other participants.

Participants in SET




Merchant
Internet
Cardholder
Certificate
Authority
Internet
Issuer
Payment
Network
Acquirer
Payment
Gateway

SET


1. Customer browses and decides to purchase.
2. SET sends order and payment information.
Customer
7. Merchant completes order.
Merchant
3. Merchant forwards payment information to bank.
6. Bank authorizes payment.
8. Merchant captures transaction.
9. Issuer sends credit card bill to customer.
VISA
BANK
4. Bank checks with issuer for payment authorization.
5. Issuer authorizes payment.
BANK
Customer's bank ("issuer")
Merchant's bank

SET Functionalities

- **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.

SET Functionalities

- **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.

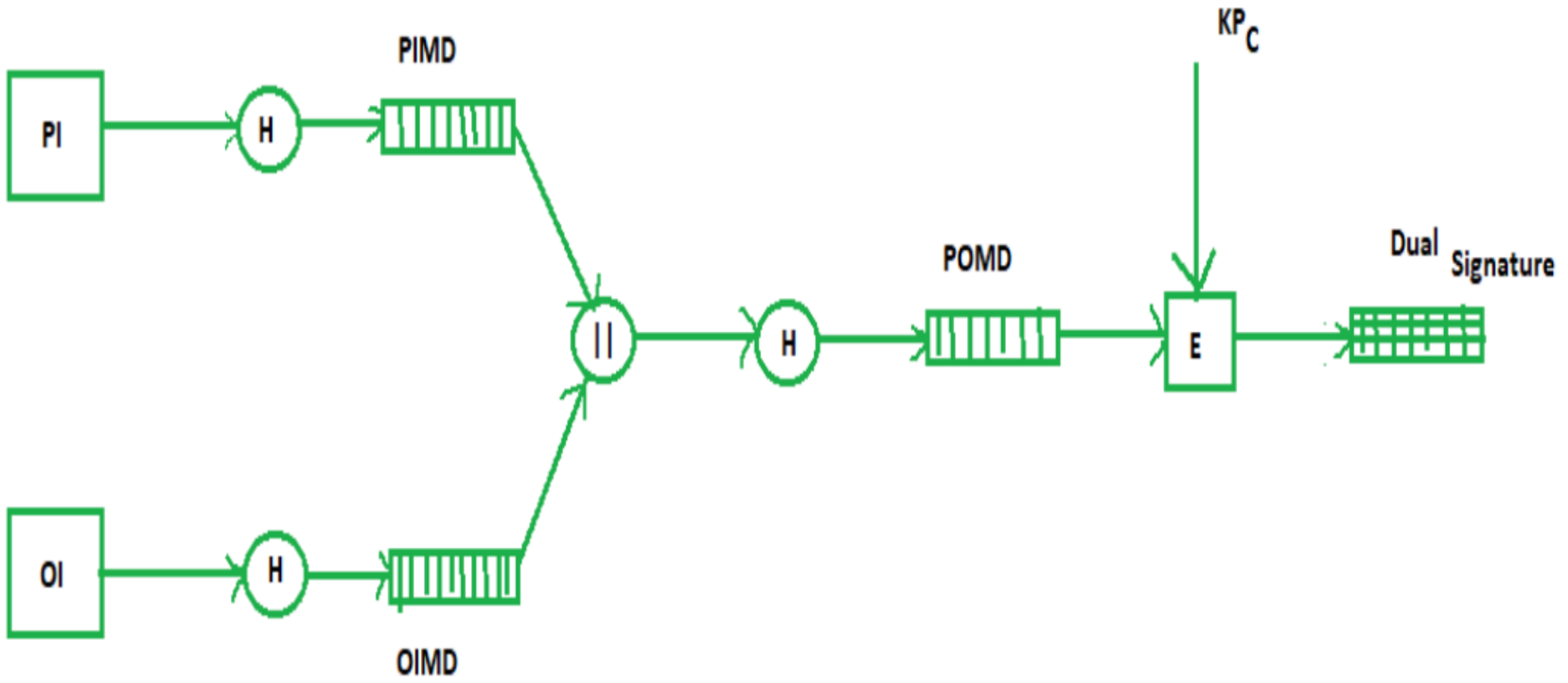
SET Functionalities

- **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,

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
- Sending them separately is an easy and more secure way, but sending them in a connected form resolves any future dispute possible.

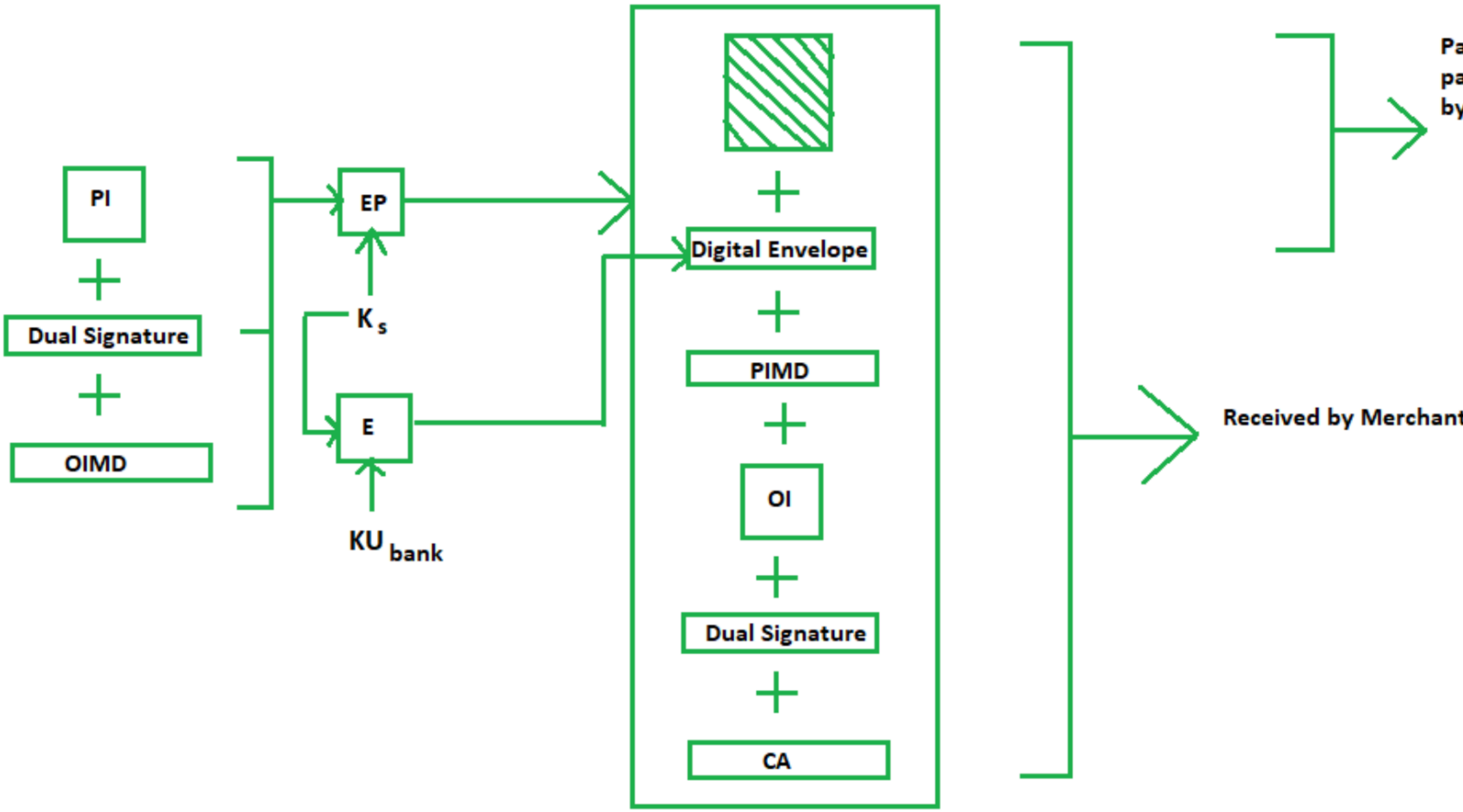
Dual Signature



PI stands for payment information
OI stands for order information
PIMD stands for Payment Information Message Digest
OIMD stands for Order Information Message Digest
POMD stands for Payment Order Message Digest
H stands for Hashing
E stands for public key encryption
KPc is customer's private key
|| stands for append operation
Dual signature, DS= E(KPc, [H(H(PI)||H(OI))])

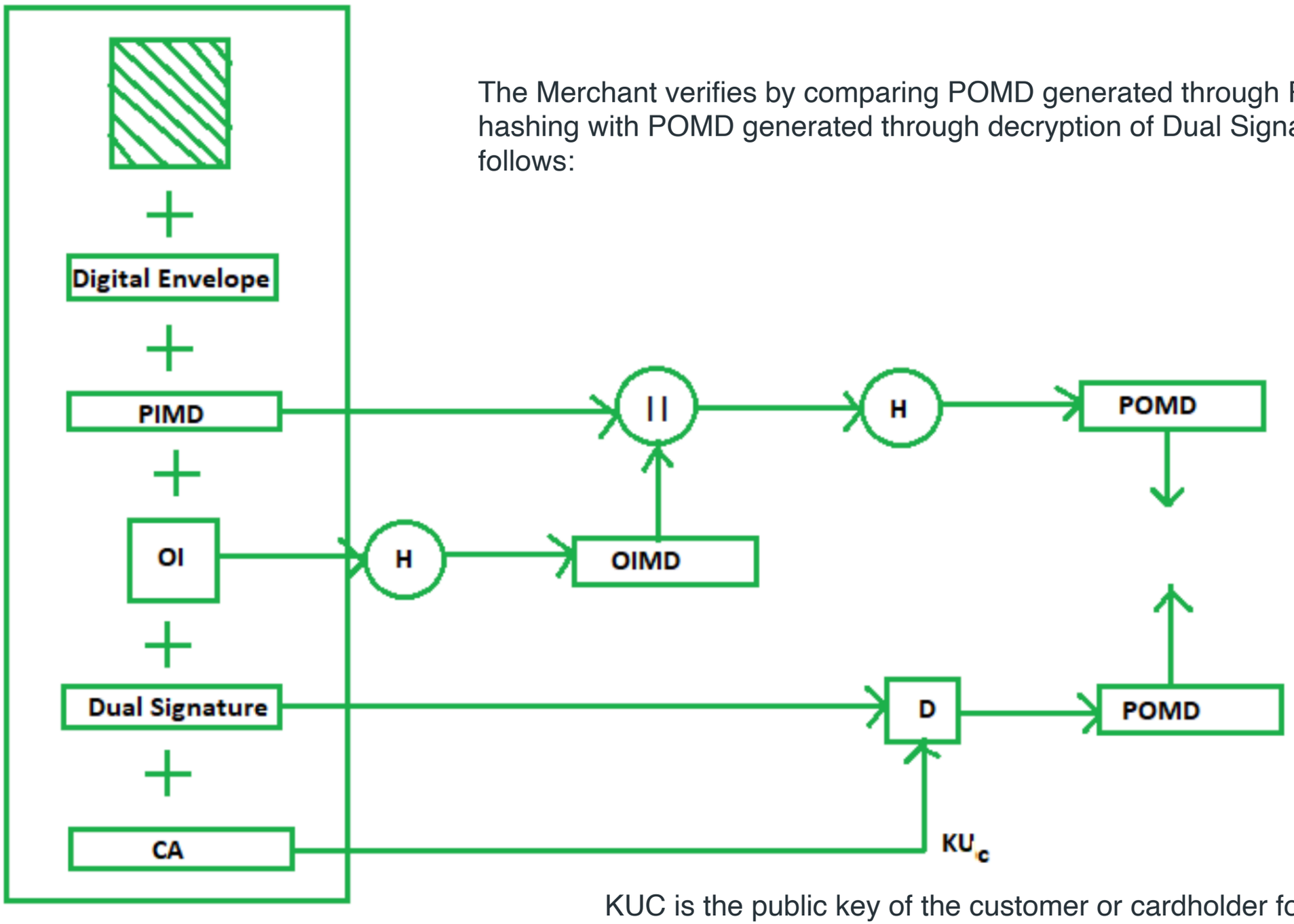
Purchase Request Generation

- The process of purchase request generation requires three inputs:
  - Payment Information (PI)
  - Dual Signature
  - Order Information Message Digest (OIMD)



PI, OIMD, OI all have the same meanings as before.
The new things are :
EP which is symmetric key encryption
Ks is a temporary symmetric key
KUbank is public key of bank
CA is Cardholder or customer Certificate
Digital Envelope = E(KUbank, Ks)

Purchase Request Validation on Merchant Side



The Merchant verifies by comparing POMD generated through PIMD hashing with POMD generated through decryption of Dual Signature as follows:

KUC is the public key of the customer or cardholder for decryption ‘D’.

Payment Authorization and Payment Capture

- Payment authorization as the name suggests is the **authorization of payment information** by the merchant which ensures payment will be received by the merchant.

- **Payment capture** is the process by which a merchant receives payment which includes again generating some request blocks to gateway and payment gateway in turn issues payment to the merchant.