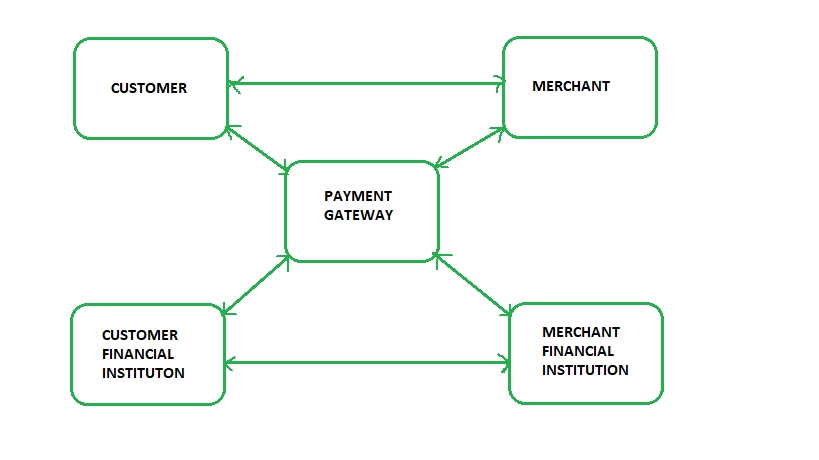
**Secure Electronic Transaction** :

* SET is a security protocol designed to ensure the security and integrity of electronic transactions conducted using credit cards. Unlike a payment system, SET operates as 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, and Microsoft which provided its Secure Transaction Technology (STT)
* SET protects sensitive credit card details from merchants, minimizing the risk of theft and hacking. It incorporates Certification Authorities and standard digital certificates, such as X.509, to enhance transaction security.



**Requirements in SET Protocol**:

1. **Mutual Authentication**: Ensures both customer (cardholder) and merchant authentication to confirm their legitimacy.
2. **Confidentiality**: Protects Payment Information (PI) and Order Information (OI) through encryption.
3. **Message Integrity**: Prevents unauthorized modifications to transmitted content.
4. **Interoperability**: Ensures compatibility across systems and implements robust security mechanisms.

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

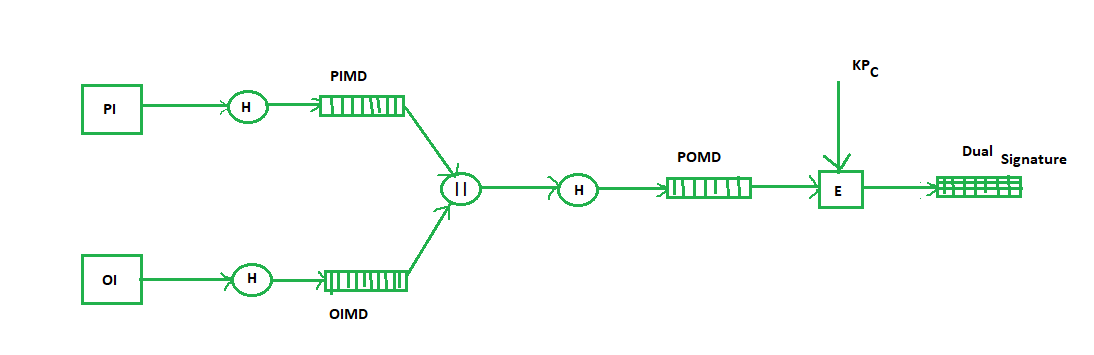
1. **Cardholder –** customer
2. **Issuer –** customer financial institution
3. **Merchant**
4. **Acquirer –** Merchant financial
5. **Certificate authority –** Authority that follows certain standards and issues certificates(like X.509V3) to all other participants.

**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.
* **Message Integrity**: Protects against unauthorized message modifications using RSA digital signatures with SHA-1 and, in some cases, HMAC with SHA-1.

**Dual Signature in SET**:

The dual signature is a unique feature of the SET protocol designed to securely link **Order Information (OI)** for the merchant and **Payment Information (PI)** for the bank while keeping them separate for confidentiality. This ensures both pieces of information are connected in a way that prevents disputes without revealing sensitive data to unintended parties.

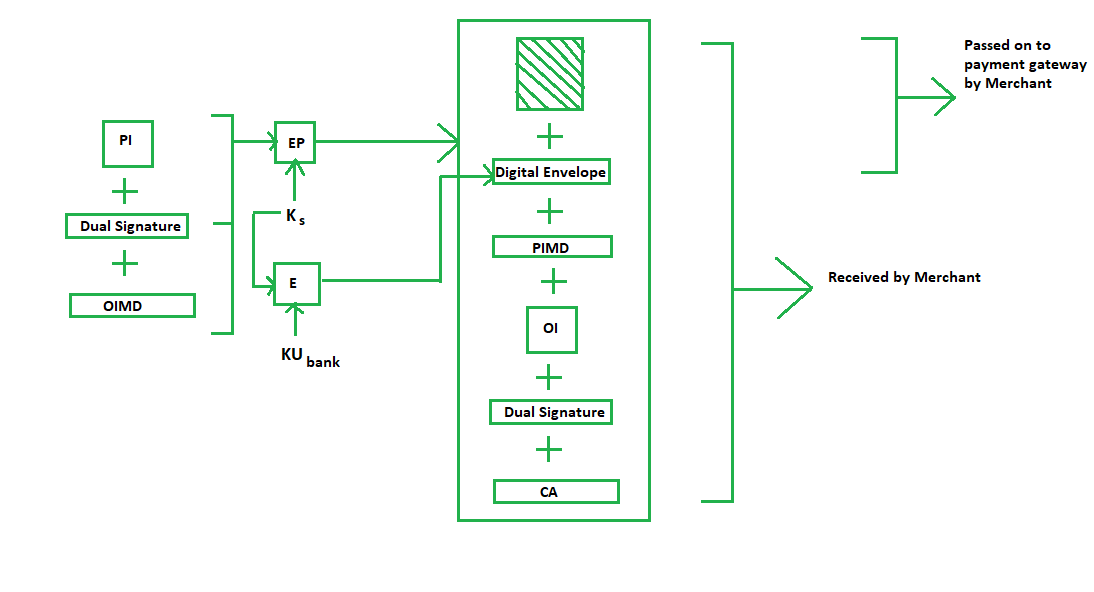


Where,  
  
 PI stands for payment information  
 OI stands for order information  
 PIMD stands for Payment Information Message Digest  
 OIMD stands for Order Information Message Digest  
 POMD stands for Payment Order Message Digest  
 H stands for Hashing  
 E stands for public key encryption  
 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)

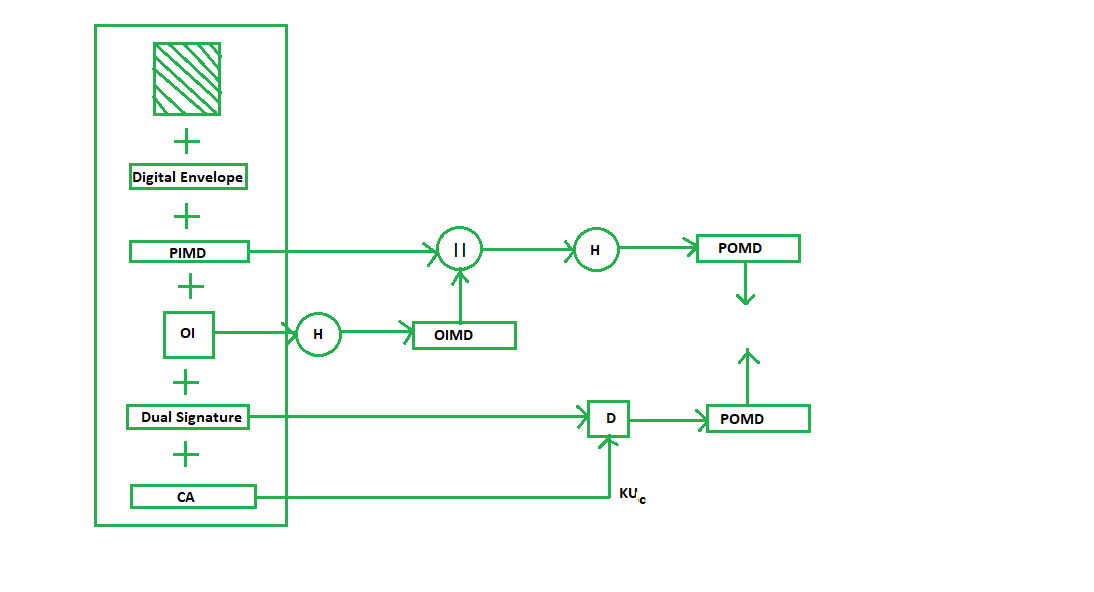
The purchase request is generated as follows:



Here,  
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 the Merchant Side**:

1. **Verification of POMD (Proof of Message Digest)**:
   * The merchant generates a **POMD** by hashing the **PIMD** (Payment Information Message Digest).
   * The dual signature, which was encrypted using the customer’s private key, is decrypted using the customer’s public key (**KUC**) to extract the **POMD**.
2. **Comparison**:
   * The merchant compares the locally generated **POMD** with the decrypted **POMD**.
   * If both match, the request is validated, confirming the integrity of the payment and order information.



**Payment Authorization and Payment Capture**:

1. **Payment Authorization**:
   * The merchant verifies and ensures that the payment details are valid and that the payment will be received.
   * This involves sending a payment authorization request to the payment gateway.
2. **Payment Capture**:
   * After authorization, the merchant initiates the payment capture process by generating specific request blocks.
   * The payment gateway processes this request and transfers the authorized payment to the merchant’s account.

**Advantages of Secure Electronic Transaction (SET)**

1. **High Security:** Keeps your credit card details safe during online transactions.
2. **Authentication:** Ensures both you and the merchant are genuine, reducing fraud.
3. **Confidentiality:** Keeps payment and order information private.
4. **Integrity:** Makes sure the data sent isn't tampered with.
5. **Standardization:** Uses widely accepted protocols, making it reliable.
6. **Fraud Reduction:** Limits the exposure of credit card info to merchants, cutting down on fraud.

**Disadvantages of Secure Electronic Transaction (SET)**

1. **Complexity:** It's complicated to set up and manage.
2. **Costly:** Requires special hardware and software, which can be expensive.
3. **Slower Performance:** Security processes can slow down transactions.
4. **Limited Support:** Not all merchants use it, so it's not universal.
5. **Difficult Certificate Management:** Keeping digital certificates up-to-date can be tough.
6. **User Experience:** Extra security steps can make it harder for users.

**Applications :**

1. **Online Shopping:** Ensures secure credit card payments when you buy stuff online.
2. **Internet Banking:** Protects your transactions and information when you use online banking services.
3. **Mobile Payments:** Keeps your payments safe when you use mobile payment apps.
4. **Payment Processing:** Secures the transfer of payment details between sellers and banks.
5. **Business Transactions:** Protects big online transactions between companies.
6. **Government Payments:** Secures online payments for government services like taxes and fees.