Semester: VI Subject: CSS Academic Year: 2023-2024

SET: (SECURE ELECTRONIC TRASACTION):

- It is used to protect data for electronic transaction.
- It provides security for both personal information and financial informations.

Services of SET:

- Confidentiality (user data).
- Integrity (Data should not be altered).
- Card Holder Authentication. (valid card or not).
- Merchant Authentication. (Able to accept the cards or not).

SET Participants:

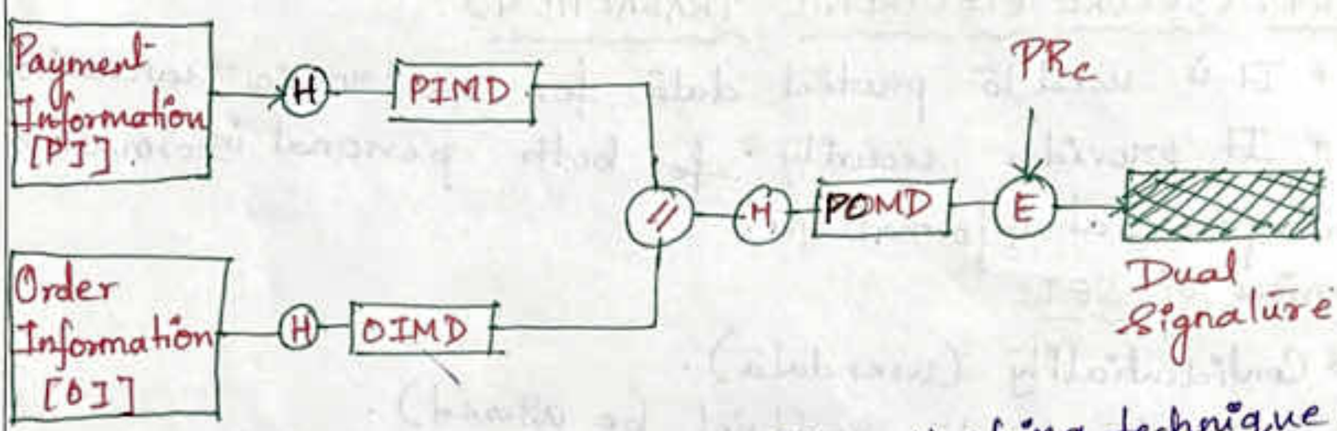
- Card Holder.
- Merchant.
- Issuer — Bank of Card Holder.
- Acquirer - Financial Institution related to merchant.
- Payment Gateway - Master Card/ Viesa card.
- Certificate Authority - Trusted Third Party certificates:
  - ↳ Card Holder Name.
  - ↳ Public Key of customer.

Dual Signature:

The dual signature is created to achieve the integrity. The information of user is divided into 2 parts.

Information
- Payment Information (PI) → Bank. (Plain Text of PI. MD of OI)
- Order Information (OI) → Merchant. PT of OI, M.D of PI.

Semester : VI Subject : CSS Academic Year: 2023-2024.



* PI stands for Paymenl Information. Hashing technique. SHA-1. is applied on PI and PIMD [Paymenl Information Message Digest] is generated.

* OI stands for Order Information. Hashing Technique SHA-1 is applied on OI and OIMD [Order Information Message Digest] is generated.

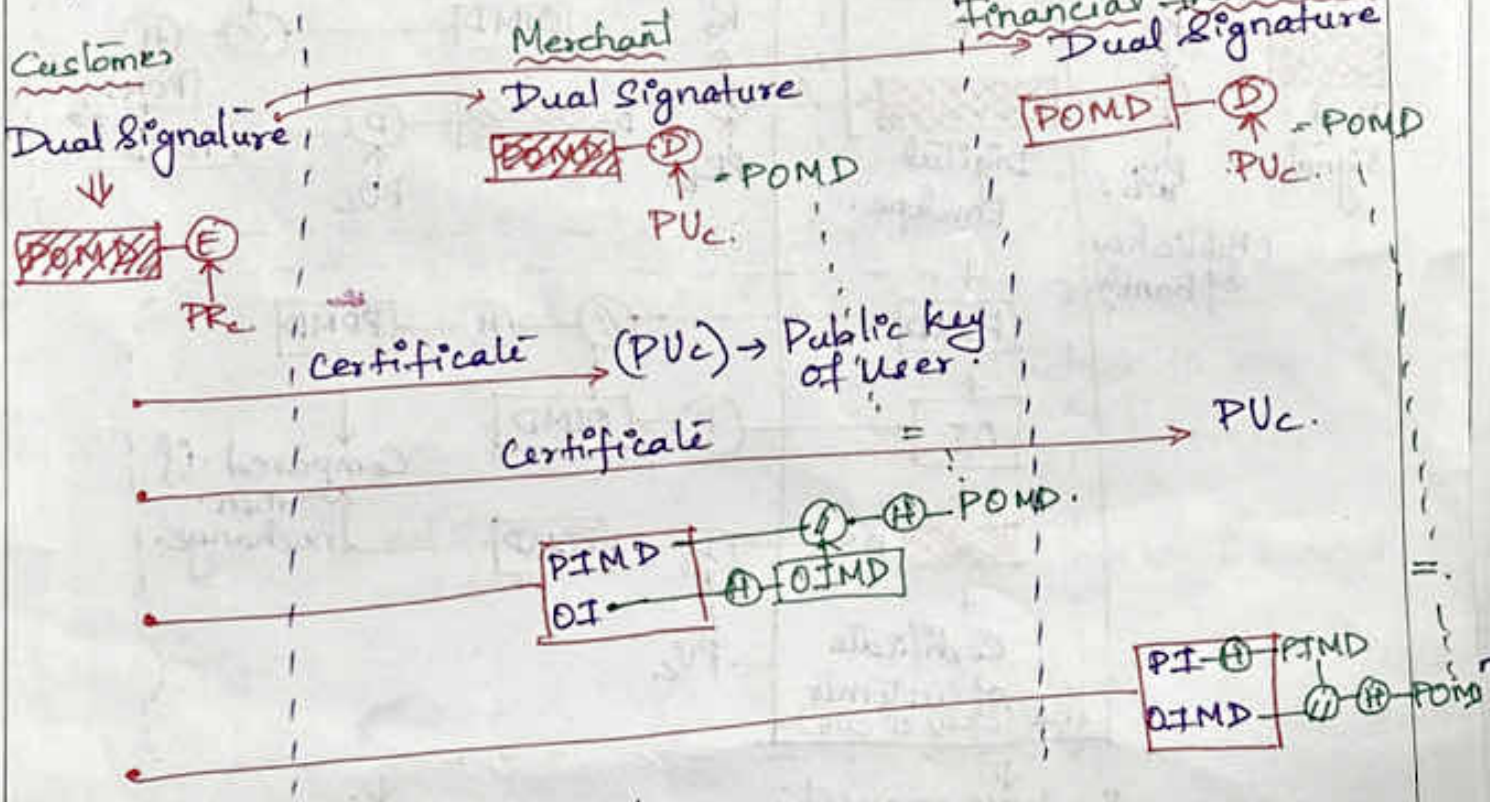
* Apply hash algorithm on PIMD and OIMD to generate POMD [Payment Order Message Digest].

* Encrypt the generated POMD using the Private key of the customer.

* The encrypted POMD is the dual signature

The customer generates the dual signature and sends along with the purchase details to the merchant & also. with the payment details to the ~~cust~~ bank.

The merchant and the bank decrypts the dual signature using the public key of the user and verifies the POMD. If both POMD are same then the integrity is achieved.



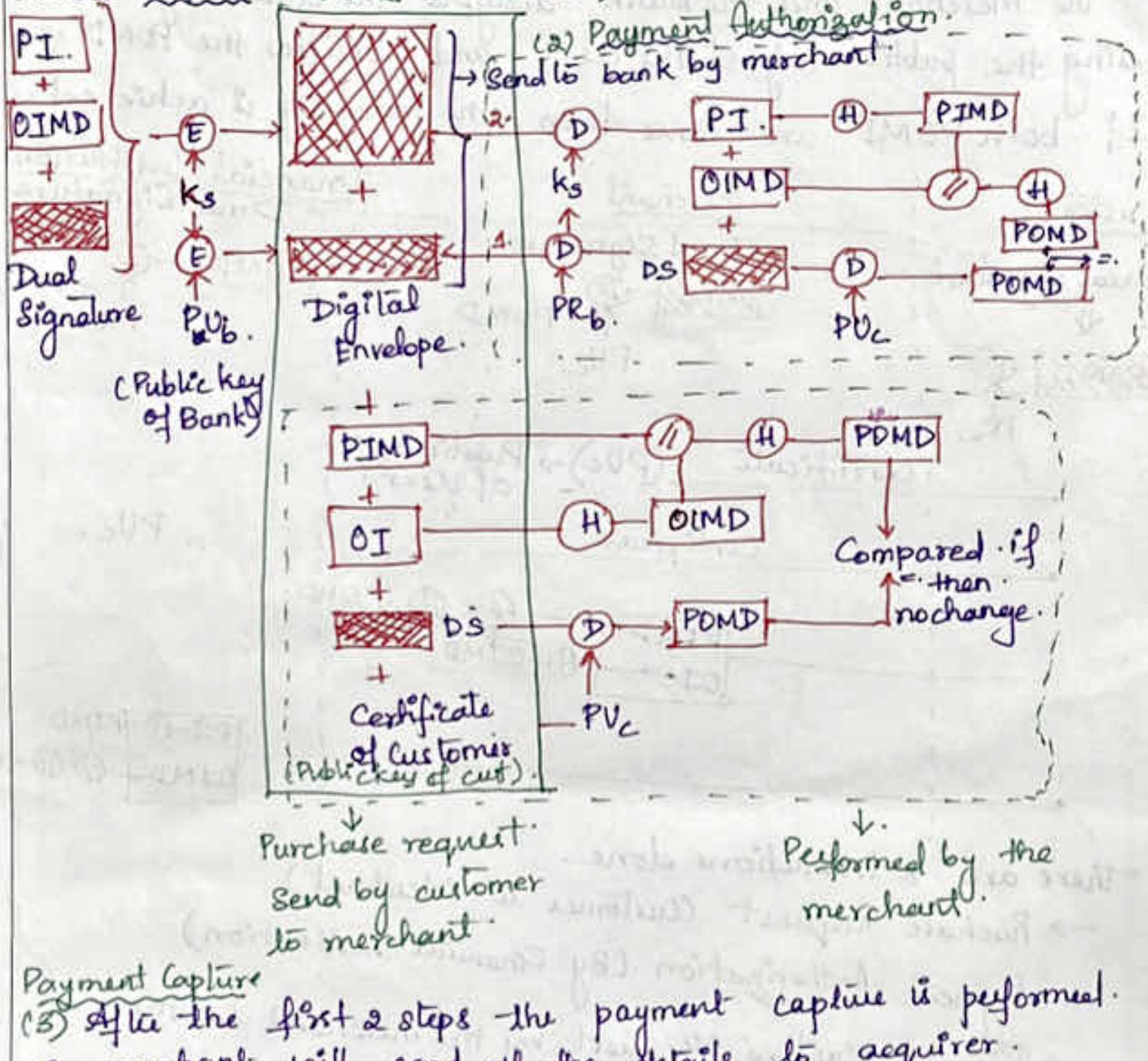
- There are 3 trasactions done.

→ Purchase Request (Customer to Merchant)

→ Payment Authorization (By Financial Institution)

→ Payment Capture (Request by the merchant to the Acquirer).

(1). Purchase Request (Customer to Merchant).



Purchase request send by customer to merchant.

Performed by the merchant.

Payment Capture
(3) After the first 2 steps the payment capture is performed. The merchant will send all the details to acquirer. The acquirer will debit the amount from any bank of customer bank and credit it to customers account.

Semester: VI Subject: CSS Academic Year: 2023-2024

(1) Purchase Request → Customer to Merchant)

→ The customer sends the purchase request to the merchant.

→ The purchase request consists of the following:

* PI + OIMD + Dual signature which is encypted using K_s → Symmetric key.

* The symmetric key is again encypted using Public key of bank (PU_b). and digital envelope is generated.

* PIMD + OI + Dual Signature + Certificate of Customer

This entire packet is send by the customer to merchant.

* The merchant cannot decrypt the digital envelope and the encypted text.

* The merchand will aply hash algorithm on OI and genuate OIMD.

* The OIMD and PIMD is appended and hash algorithm is applied to generate POMD.

* The Dual Signature is decypted using Public key of customer and POMD is generated.

* If both POMD is same then the integrity of order information is achieved and the sender is also verified.

(2) Payment Authorization:

* The merchant will send encypted text and digital envelope to the bank.

* The bank will decypt the digital envelope using Public key of bank. and receive k_s.

* Using k_s decrypt the encypted text and receive → PI + OIMD + Dual signature.

* The payment information is verified.

(3) Payment Capture:

After the first 2 steps the payment capture is performed.

* The merchant will send all the details to acquirer

* The acquirer will debit the amount from any bank of customer bank and credit it to the customer's account.