4. SECURE ELECTRONIC TRANSACTION

- **List out the participants of SET system and explain in detail. (16) (IT2352 / May/June'12)**
- **Explain in detail about SET (16 Marks – Nov/Dec'12)**

Secure Electronic Transaction:

Secure Electronic Transaction (SET) is an open encryption and security specification designed to protect credit card transactions on the Internet.

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

SET is an open encryption and security specification designed to protect credit card transactions on the Internet. The current version, SETv1, emerged from a call for security standards by MasterCard and Visa in February 1996.

SET is not itself a payment system. Rather it is a set of security protocols and formats that enables users to employ the existing credit card payment infrastructure on an open network (Internet) in a secure fashion.

SET services:

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

SET Overview:

Requirements:

Business requirements for secure payment processing with credit cards over the Internet and other networks:

- Provide confidentiality of payment and ordering information: It is necessary to assure cardholders that this information is safe and accessible only to the intended recipient.

- Ensure the integrity of all transmitted data: That is, ensure that no changes in content occur during transmission of SET messages. Digital signatures are used to provide integrity.

- Provide authentication that a cardholder is a legitimate user of a credit card account. Digital signatures and certificates are used to verify that a cardholder is a legitimate user of a valid account.

- Provide authentication that a merchant can accept credit card transactions through its relationship with a financial institution.

- Ensure the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction.

- Create a protocol that neither depends on transport security mechanisms nor prevents their use.

- Facilitate and encourage interoperability among software and network providers.

Key Features of SET

SET incorporates the following features:

- Confidentiality of information.
- Integrity of data.
- Cardholder account authentication
- Merchant authentication

SET Participants:

Cardholder:

In the electronic environment, consumers and corporate purchasers interact with merchants from personal computers over the Internet. A cardholder is an authorized holder of a payment card (e.g., MasterCard, Visa) that has been issued by an issuer.

Merchant:

A merchant is a person or organization that has goods or services to sell to the cardholder.

Issuer:

This is a financial institution, such as a bank, that provides the cardholder with the payment card.

Acquirer:

This is a financial institution that establishes an account with a merchant and processes payment card authorizations and payments. The acquirer also provides electronic transfer of payments to the merchant's account.

Payment gateway:

This is a function operated by the acquirer or a designated third party that processes merchant payment messages. The payment gateway interfaces between SET and the existing bankcard payment networks for authorization and payment functions.

Certification authority (CA):

This is an entity that is trusted to issue X.509v3 public-keycertificates for cardholders, merchants, and payment gateways. The success of SET will depend on the existence of a CA infrastructure available for this purpose.

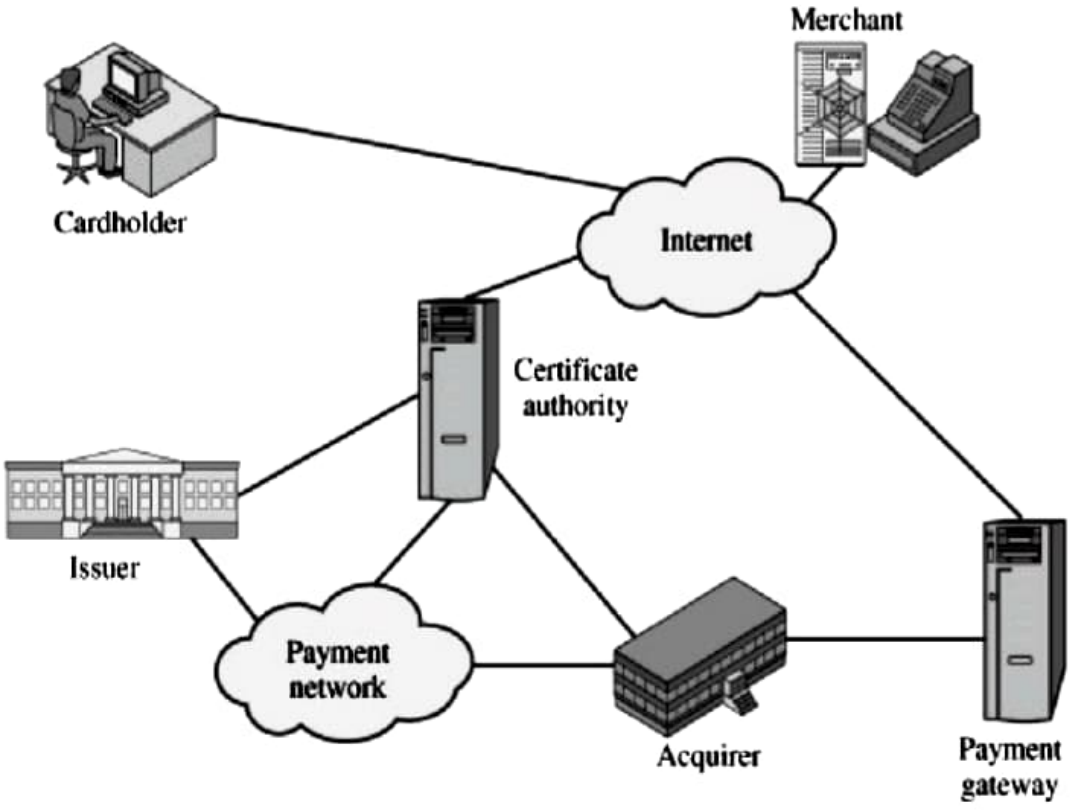

Figure: Secure Electronic Commerce Components

Sequence of events for a transaction:

- The customer opens an account
- The customer receives a certificate
- Merchants have their own certificates
- The customer places an order
- The merchant is verified.
- The order and payment are sent.
- The merchant requests payment authorization
- The merchant confirms the order.
- The merchant provides the goods or service.
- The merchant requests payment.

Dual Signature:

SET dual signature : The purpose of the dual signature is to link two messages that are intended for two different recipients. In this case, the customer wants to send the order information (OI) to the merchant and the payment information (PI) to the bank. The merchant does not need to know the customer's credit card number, and the bank does not need to know the details of the customer's order. The customer is afforded extra protection in terms of privacy by keeping these two items separate.

The customer takes the hash (using SHA-1) of the PI and the hash of the OI. These two hashes are then concatenated and the hash of the result is taken. Finally, the customer encrypts the final hash with his or her private signature key, creating the dual signature. The operation can be summarized as

$$DS = E(PRc, [H(H(PI)||H(OI)])$$

where PRc is the customer's private signature key.

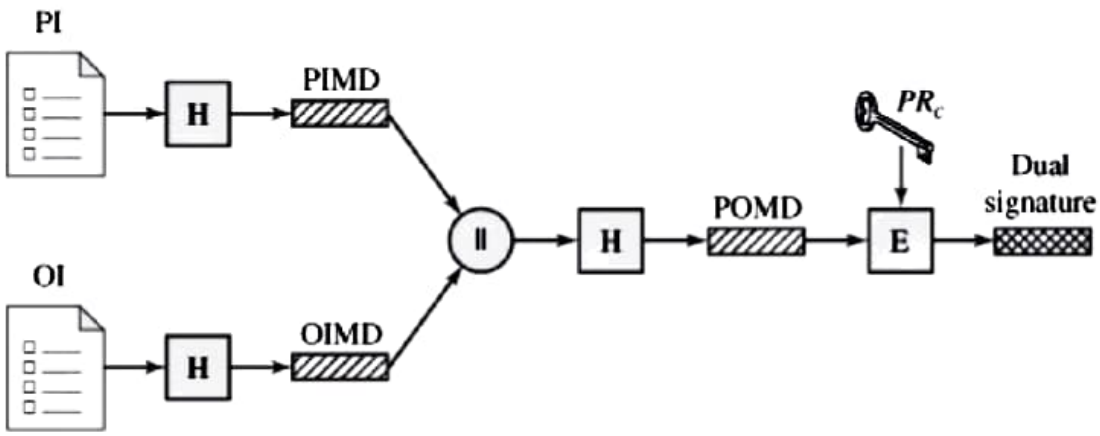

Figure: Construction of Dual Signature

if these two quantities are equal, then the bank has verified the signature.

1.The merchant has received OI and verified the signature.

2.The bank has received PI and verified the signature.

3.The customer has linked the OI and PI and can prove the linkage.

Payment Processing:

- Purchase request
- Payment authorization
- Payment capture

SET Transaction Types:

Cardholder registration:

Cardholders must register with a CA before they can send SET messages to merchants.

Merchant registration:

Merchants must register with a CA before they can exchange SET messages with customers and payment gateways.

Purchase request:

Message from customer to merchant containing OI for merchant and PI for bank.

Payment authorization:

Exchange between merchant and payment gateway to authorize a given amount for a purchase on a given credit card account.

Payment capture:

Allows the merchant to request payment from the payment gateway.

Certificate inquiry and status:

The cardholder or merchant sends the Certificate Inquiry message to determine the status of the certificate request and to receive the certificate if the request has been approved.

Purchase inquiry:

Allows the cardholder to check the status of the processing of an order after the purchase response has been received.

Authorization reversal:

Allows a merchant to correct previous authorization requests. If the order will not be completed, the merchant reverses the entire authorization.

Capture reversal :

Allows a merchant to correct errors in capture requests such as transaction amounts that were entered incorrectly by a clerk.

Credit:

Allows a merchant to issue a credit to a cardholder's account such as when goods are returned or were damaged during shipping.

Credit reversal:

Allows a merchant to correct a previously request credit. **Payment Gateway certificate request**:

Allows a merchant to query the payment gateway and receive a copy of the gateway's current key-exchange and signature certificates.

Batch administration:

Allows a merchant to communicate information to the payment gateway regarding merchant batches.

Error message:

Indicates that a responder rejects a message because it fails format or content verification tests.