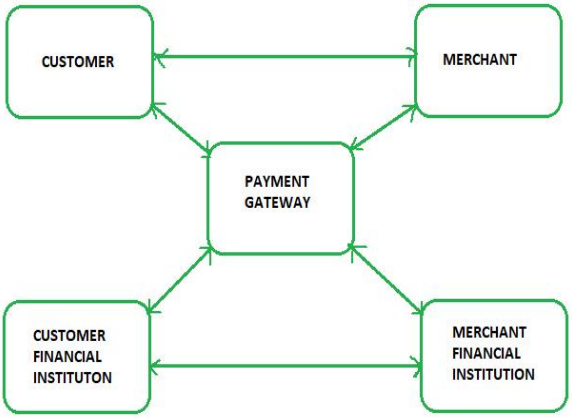
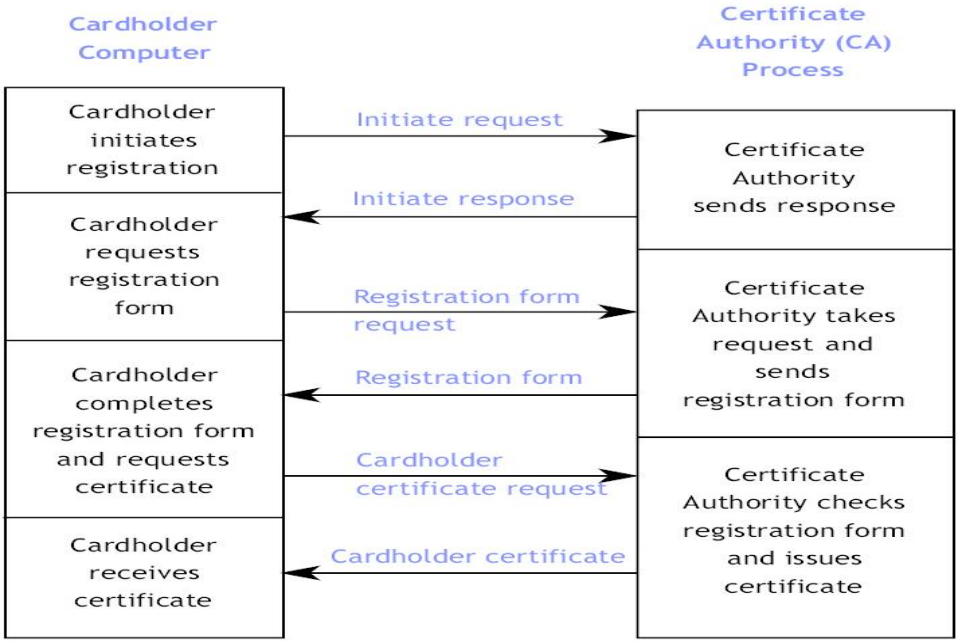
CARD HOLDER REGISTRATION, MERCHANT REGISTRATION AND PURCHASE REQUEST

Secure Electronic Transaction or SET is a system that ensures the security and integrity of electronic transactions done using credit cards in a scenario. SET is a security protocol applied to the transactions.
It used 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) , and Netscape which provided the technology of Secure Socket Layer(SSL).



Cardholder Registration

This is the initial step for cardholders. The agent C sends to a certification authority CA the information on the credit card he wants to use. The CA replies with a registration form, which C completes and returns, together with the signing key that C wants to register. Then, CA checks that the credit card is valid and releases the signature certificate for C who stores it for future use. All this information myst be protected and this makes the protocol steps complicated.



Merchant Registration: This phase performs the analogous function for merchants. In contrast with Cardholder Registration, the merchant M can not only register a public key for signature but also a public key for encryption. The process is shorter because there is no confidential information to be protected.

Purchase Request: We reach this phase if C has decided to buy something. C sends to M the order information and the payment instructions. M processes the order and starts the Payment Authorization phase by forwarding the payment instructions to the PG. This last step is needed because SET aims to keep the cardholder's PAN confidential.
The purchase request exchange consists of four messages:

- Initiate Request
- Initiate Response
- Purchase Request
- Purchase Response

To send SET messages to the merchant, the cardholder must have a copy of the certificates of the merchant and the payment gateway. The customer requests the certificates in the Initiate Request message, sent to the merchant. This message includes the brand of the credit card that the customer is using. The message also includes an ID assigned to this request/response pair by the customer.

The merchant generates a response and signs it with its private key. The response includes a transaction ID for this purchase transaction. In addition to the signed response, the Initiate Response message includes the merchant's certificate and the payment gateway's certificate.

The cardholder verifies the merchant and gateway certificates by means of their respective CA signatures and then creates the order information (OI) and payment information (PI). The transaction ID assigned by the merchant is placed in both the OI and PI. The OI doesn't contain explicit order data such as the number and price of items. Rather, it contains an order reference generated in the exchange between merchant and customer during the shopping phase before the first SET message.