Secure Electronic Transactions (SET)

SET

- SET is an encryption and security specification designed to protect credit card transactions on the Internet.

- 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, such as Internet, in a secure fashion.

- The main participants in the SET system are : client, vendor and vendor bank

•The certification of all the three parts is required. The certificats of the client and vendor are provided by their banks (confirmation that they can pay or receive payments with a particular credit card).

•The certificats contain information about the financial institution that issued the certificate.

•An interesting and important feature of SET is that it prevents the vendor from learning the client credit card number; this is only provided to the issuing bank

Sequence of events required for a transaction

- Bob (the customer) comunicates to Alice(the vendor) that it is interested to buy some items with a credit card.
- Alice sends to Bob a transaction identifier.
- Alice sends to Bob its digital certificate and the certificate of its bank. The certificates contains the relative public key. They are encrypted with the private key of an certification authority.
- Bob utilizes the public key of the certification authority and obtains both the public keys of Alice and its bank.

• Bob sends to Alice two information blocks: Order information **(OI)** and purchase Information **(PI).**
OI contains the transaction identifier and the type of credit card used. It is encrypted wich the Alice's public key.
PI contains the purchase total price and the credit card number.

•Alice sends to its bank a message encrypted with the bank public key. The message contains PI, received from Bob and the Alice's certificate.

•The Alice's bank controls that the transaction identifier is the same of that contained in Bob's PI block.

•The Alice's bank sends a request to the bank that released the Bob's credit card looking for payment authorization.

•If the Bob's bank authorizes the payment, the Alice's bank sends to Alice a message encrypted with the Alice's public key containing the transaction identifier.

•If the transaction has been approoved Alice sends the response message to Bob with the indication that the payment has been accepted and that the required items will be delivered.