Ans-2) Secure Electronic Transaction (SET) is a system for ensuring the security of financial transactions on the Internet. It was supported initially by Mastercard, Visa, Microsoft, Netscape, and others. With SET, a user is given an electronic wallet (digital certificate) and a transaction is conducted and verified using a combination of digital certificate and digital signatures among the purchaser, a merchant and the purchaser's bank in a way that ensures privacy and confidentiality. SET makes use of Netscape's Secure Sockets Layer (SSL), Microsoft's Secure transaction Technology (STT) and Terisa System's Secure Hypertext Transfer Protocol (SHTTP). SET uses some but all aspects of a Public key infrastructure (PKI).

Assume that a Customer has a SET-enable browser such as Netscape or Microsoft's Internet Explorer and that the transaction Provider (bank, Store, etc.) has a SET-enabled Server.

Advantages

1. The Customer open a Mastercard or Visa bank account. Any issuer of a Credit Card is some kind of bank.
2. The Customer receives a digital Certificate. This electronic file functions as a Credit card for online Purchases or other transaction. It includes a public key with an expiration date. It has been through a digital switch to the bank to ensure its validity.
3. Third party merchants also receive Certificates from the bank. These Certificates include the merchant's public key and the bank's public key.
4. The Customer Places an order on a web page,

DATE
PAGE NO.

by phone, or some other means.

5. The customer's browser receives and confirms from the merchant's certificate that the merchant is valid.

6. The browser sends the order information. This message is encrypted with the merchant's public key, the payment information, which is encrypted with the bank's public key (which can't be read by the merchant), and information that ensures the payment can only be used with this particular order.

7. The merchant sends the order message along to the bank. This includes the bank's public key, the customer's payment information (which the merchant can't decode), and the merchant's certificate).

8. The merchant verifies the customer by checking the digital signature on the customer's certificate. This may be done by sending the certificate to the bank or to a third-party verifier.

9. The bank verifies the merchant and the message. The bank uses the digital signature on the certificate with the message and verifies the payment part of the message.

10. The bank digitally signs and sends authorization to the merchant, who can then fill the order.