Chapter 7

Electronic Payment Systems and Internet Banking

Electronic payment systems comprise payment services over the network for goods and services procured. They are integral to the completion of e-commerce transactions. Goods can include physical items such as books, CDs, garments and electronic content, while hotel booking, railway/airline reservations, stock trading, etc. are examples of services offered and procured over the Internet. Authentication, integrity, authorisation and confidentiality are the basic security requirements that must continue to be met when payments are made electronically for such procurement.

An electronic payment system consists of the following components:

- Buyer
- Seller (merchant)
- Payment gateway
- Buyer's bank (issuer of the payment instrument)
- Seller's bank (acquirer).

When a buyer procures goods or services electronically from a merchant, the method of payment could be chosen to be a credit card. Before the merchant agrees to supply the item to the buyer, the merchant looks for the assurance that the payment will be fulfilled. A request containing the transaction

details is sent to the payment gateway by the merchant. The payment gateway, in turn, interacts with the issuer bank on the financial network to carry out the verification. The result is sent back to the merchant to enable the merchant to decide on whether the goods/services should be supplied or not.

Other payment methods such as electronic cheque, funds transfer through Internet banking and innovative schemes like PayPal adopted by eBay are also widely used. When the buyer uses credit cards, the details of the transaction are posted to the buyer's account and processed in a cumulative manner. If, however, debit cards are used, then the buyer's account is debited automatically. These payment methods are discussed in the following sections.

18.1 Payment Gateway

Payment gateways handle all the payment operations that are needed for operating e-commerce sites. The servers on these sites have to be secured and duly certified by a Certifying Authority. Payment gateways can process multiple payment mechanisms including debit cards and smart cards. Normally, there are two functions within payment gateway software. Theses are:

- The ***authorisation*** function which performs certification and issuance of digital identification to the entities that would be interacting with the payment gateway.
- The ***settlement*** function which facilitates the carrying out of actual inter-bank transactions.

The entire system provides facilities like formatting, encrypting and digital signing of the orders for transferring to the financial network.

In India, payment gateway services are offered by ICICI, Citibank, Global Telesystems and HDFC Bank. These systems enable the seller to perform real-time credit card authorisation

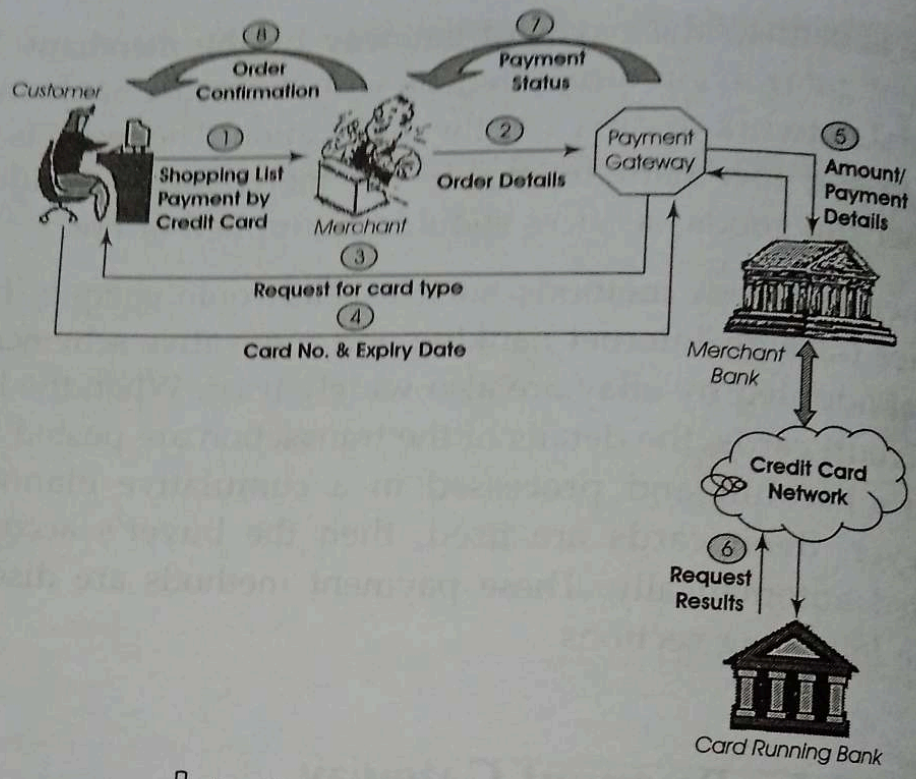

Fig. 18.1 *Payment gateway*

or debit card settlements from a website over the Internet. Payment can be made within seconds after the gateway obtains authorisation from the credit card institutions.

Most credit cards such as MasterCard, Visa, American Express, etc. are acceptable to these payment gateways. Any credit card information submitted as a part of completing a transaction is encrypted before it is transmitted over the Internet to the acquiring bank. Most of these payment gateway servers are placed behind security firewalls and are integrated with risk management components so that the security is effectively managed.

For example, Payseal, the payment gateway operated by ICICI, ensures that the customer's credit card details are kept secure while transacting on the Net, thereby preventing unauthorised access to customer information. The card details would not be disclosed even to the merchant. Payseal which adopts the SSL (Secure Socket Layer) technology, is an integrated solution employing 128-bit encryption to secure online transactions. The

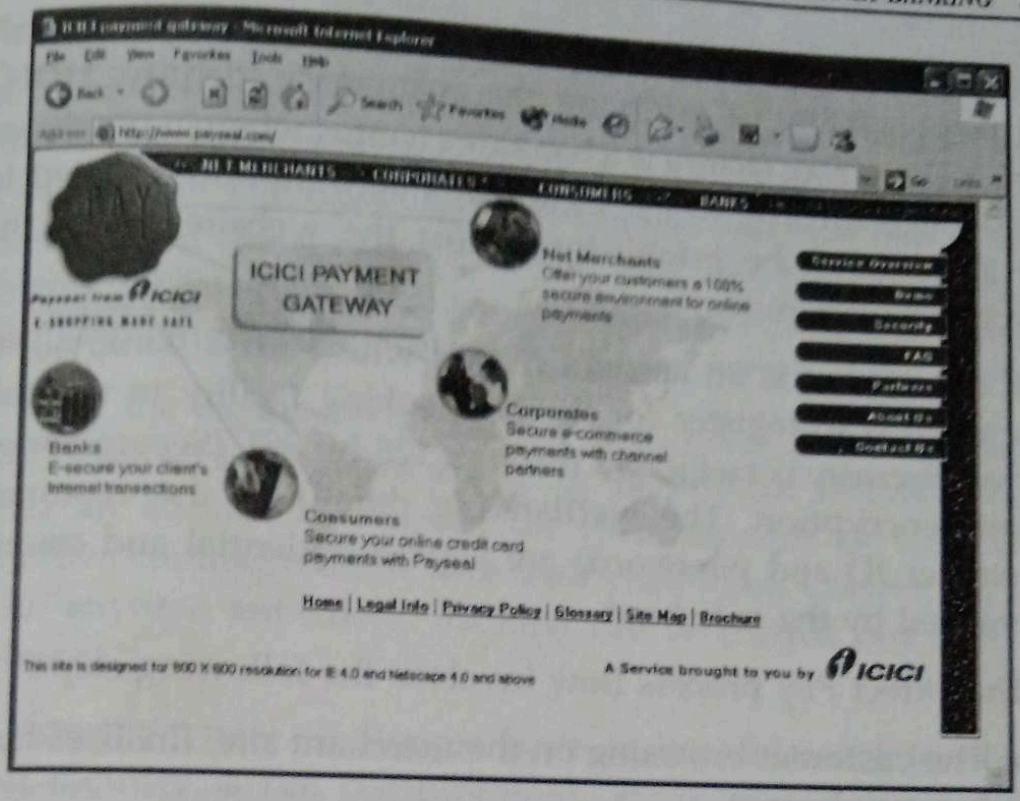

Fig. 18.2 *www.payseal.com*

client software, installed at the client's end, encrypts transaction information using 280-bit RSA before passing it through an SSL pipe using 128-bit encryption. The data is stored at ICICI's own data centre, which is secured by firewalls and other network security infrastructure. Physical access to the data centre is restricted by the use of biometrics. The gateway server has been assigned a server certificate by a certifying authority.

In the business-to-business sector, HDFC Bank's payment gateway, EPI, provides real-time transfer of funds transacted on the portal. EPI has been successfully implemented by fifteen B2B portals such as VSNL, Sifymall, Fabmart, etc. The entire operation takes place through a secure channel realised through Firewalls, 128-bit encryption and digital signatures.

In the 'Direct Pay' mode of payment, online payments are accepted from clients/customers who are HDFC Bank account holders. The account is automatically credited with the corresponding transaction amount instantaneously. Since the

customer is an HDFC Bank account holder, the bank takes all the responsibility of verifying the customer's identity. HDFC Bank's Direct Pay facility is a banking channel wherein purchases are debited directly to the customer's account and credited to the account of the establishment (or the website where the purchases were made).

If a customer is an account holder with HDFC Bank, all he has to do is to register for the Netbanking facility to use this option. Security is facilitated through 128-bit SSL (Secure Socket Layer) encryption. The NetBanking details of the customer (customer ID and password) are kept confidential and cannot be viewed by the merchant.

The Direct Pay process flow involves the following steps:

- The customer browsing on the merchant site, finalises his/her purchase.
- The customer decides to make payments for the transaction that he/she has finalised.
- The customer selects 'Debit my HDFC Bank A/C'.
- The customer clicks on the pay button and he/she is traversed to page to make payments.
- The customer enters his/her Netbanking *ID* and password.
- The customer then selects the account, from which he/she wants to make the purchase.
- The customer account with HDFC Bank is debited online and the transaction is over for the customer.
- The merchant account is credited for the transaction amount, less the transaction fee.
- The customer is honoured with the purchase made as per the terms of the merchant agreed upon by the customer.

18.2 Internet Banking

Internet banking allows any user with a PC and a browser to get connected to his bank's website to perform any of the virtual banking functions and avail himself of any of the bank's

services. There is no human operator present in a remote location to respond to his needs such as in telephone banking, or in a call centre. The bank has a centralised database that is web-enabled. All the services that the bank has permitted on the Internet are displayed in a menu. Any service can be selected and further interaction is dictated by the nature of the service.

With the expansion of the Internet, more and more banks and financial institutions are using the Internet and the Web to offer an additional channel for their services as well as to improve communication with their customers. Convenient and safe 'anytime anywhere' banking can be carried out over the Internet.

However, new challenges have to be addressed to ensure that security is not compromised. When one is using online banking systems, it is extremely important for the customer to assure himself that the online bank is a legitimate site, preferably certified by a certifying authority. Customers will be exchanging personal information in addition to giving out the account number and the corresponding password in any such online session. Some websites deliberately use names, which are very similar to those of reputed organisations and use this tactic to trick customers into revealing information, which would not otherwise be divulged.

In India, a number of banks have introduced Internet banking. While most of them are restricted to information about the customer's own account and transactions between different accounts belonging to the same customer, some banks have enhanced their services by including funds transfer between different customers.

The Reserve Bank of India has issued guidelines for Internet banking, covering:

1. Technology and security standards
2. Legal issues
3. Regulatory and supervisory issues

Technology and Security Standards

The need for banks to define security policies has been emphasised. Although the use of Public Key Infrastructure (PKI) has been suggested, the use of at least 128-bit SSL for server authentication and for securing browser-to-web server communication has been mandated.

Legal Issues

The asymmetric cryptosystem as advocated in the IT Act, 2000 has been recommended as the security procedure for digital signatures for authenticating electronic records. Other methods of authentication have been highlighted as a source of legal risk. The RBI has also warned against the enhanced risk of liability to customers on account of breach of secrecy, denial of service, etc. caused by hacking or other attacks.

Regulatory and Supervisory Issues

The following guidelines apply for these issues:

- Internet banking service can only be offered to the account holder of the bank and only for Indian local currency products.
- All banks that offer transactional services on the Internet will do so after obtaining approval from the RBI.
- Any breach or failure of security systems is to be reported to the RBI.
- Interbank payment gateways can only be set up by those institutions that are members of the cheque clearing systems in the country.

The detailed guidelines issued by the Reserve Bank of India in respect of Internet Banking are available at *www.rbi.org.in*.

18.3 PayPal

PayPal, an eBay company, has a unique payment model wherein

money can be sent to anyone who has an e-mail address. Founded in 1998, PayPal was acquired by eBay Inc. in October, 2002. PayPal enables any individual or business with an e-mail address to send and receive payments online. PayPal's service builds on the existing financial infrastructure of bank accounts and credit cards. With 56 million account members worldwide, PayPal is available in 45 countries around the world. Buyers and sellers on eBay, online retailers, online businesses, as well as traditional offline businesses are transacting payments on PayPal.

PayPal is not a payment gateway. Customers of PayPal are allowed to move money electronically from their bank account to other PayPal account holders, unlike traditional banks wherein such transfers require cheques. Account holders can send money to non-account holders by creating a virtual account attached to an e-mail address. In PayPal's model, when the recipient gets a 'you've got cash' e-mail and is directed to go to PayPal's website, he has to open an account by filling out a one-screen form providing his name, phone number and e-mail address. PayPal then sends e-mail for confirmation following which an account is created for that customer.

Once the account is opened, the recipient claims the payment. The payment appears in the recipient's PayPal account balance. The recipient can choose to transfer the funds to a bank account, request a cheque, or send the funds to someone else.

Payments are made digitally and instantly, and can be sent in US dollars, Canadian dollars, euros, pounds sterling, and yen. Person-to-person payments were introduced in thirty-six countries in the European Union (EU) and Asia in the year 2001. The widespread acceptance and convertibility of these payments were the key to PayPal's strategy. Customer service agents of PayPal, reachable by e-mail or telephone, deal with customer problems ranging from lost passwords to disputes over payments.

Customers are offered money market returns on their account balances as well as instant access to their money. From December

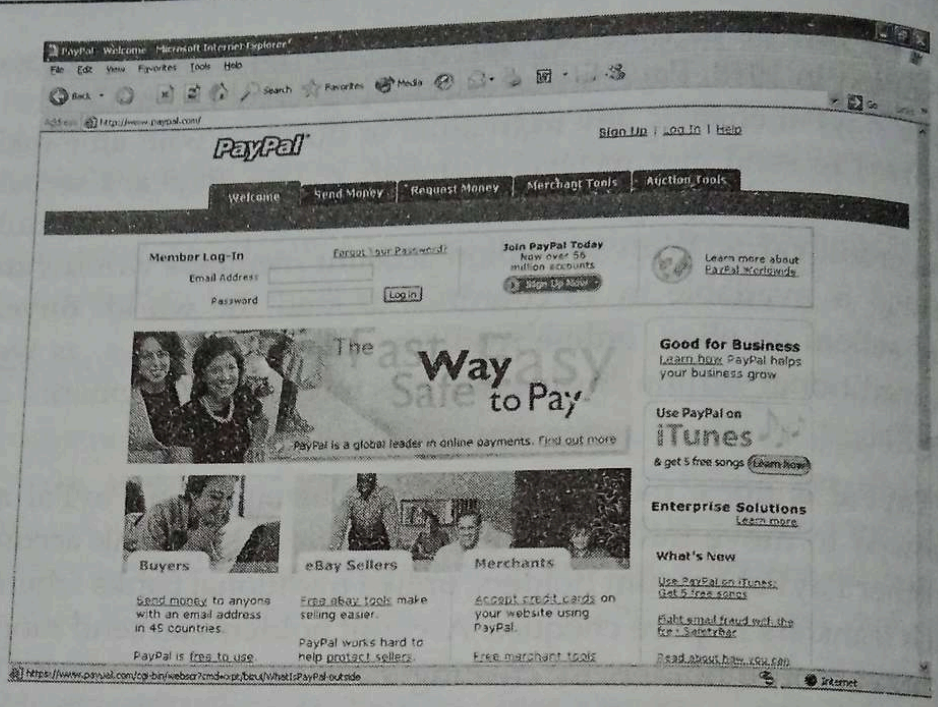

Fig 18.3 *www.paypal.com*

2000, PayPal began to offer an ATM/debit card co-branded by MasterCard. Cardholders could convert their PayPal account balances to cash at an ATM or use the debit card to pay for products and services.

In order to make sure that accounts were opened by a human being, and not by an automated entity, a security measure called the Turing Test was devised. Characters are presented on a changing chequered background so that automated character recognition programs are unable to correctly identify the characters. The re-entry of these characters is therefore only possible by humans.

Customers were encouraged by PayPal to register their bank accounts so that the PayPal account could be funded from a bank account through the ACH. A customer who opened an account and provided a verified bank account number was rewarded with a bonus of US$ 5. The account was then verified by a process for which PayPal had applied for a patent: PayPal would randomly deposit two small amounts (less than a dollar)

in the customer's bank account. If the customer could tell PayPal what the amounts were, PayPal knew that the customer could control the account, and that the customer had opened the account and had been screened by the bank. Once the customer's bank account was verified, there was no limit to how much could be spent from that bank account.

In September 2000, PayPal introduced a payment capability for wireless devices and cell phones. In this case, the notification was sent to a wireless device instead of PC-based e-mail. If one person wanted to send money to another and they both had web-enabled cell phones, the sender would access the PayPal server via the cell phone to carry out the transaction. The recipient could indicate whether the payment notification should be sent to the web-enabled cell phone or to the e-mail inbox.

18.4 The Secure Electronic Transaction (SET) Protocol

The SET protocol was developed by Visa and MasterCard to provide security for credit card-based payment transactions on the Internet. Figure 18.4 exhibits the SET protocol.

SET addresses the following business requirements of confidentiality, integrity, authentication and interoperability:

- Confidentiality of payment information and order information that is transmitted along with the payment information
- Integrity of all data that is transmitted
- Authentication that a cardholder is a legitimate user of a branded payment card account
- Authentication that a merchant can accept branded payment card transactions through his relationship with an acquiring financial institution
- Use of the best practices for security and system design so as to protect all legitimate parties in an electronic commerce/payment transaction

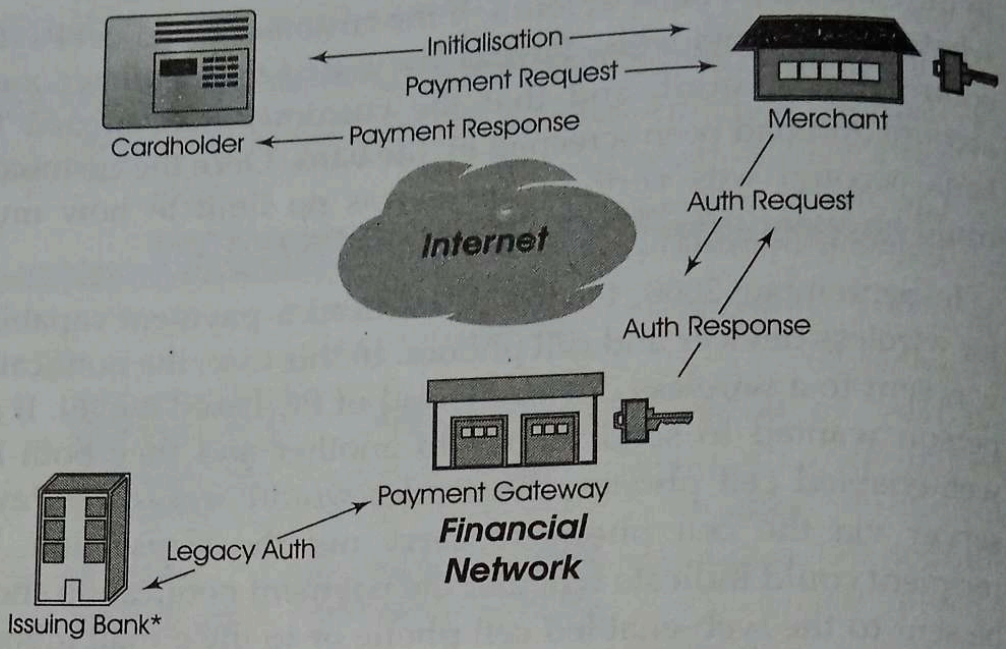

Fig. 18.4 *SET protocol*

- Independence from transport layer security mechanisms
- Interoperability among software and network providers.

When SET is used for completing an e-commerce transaction, the entire process can be broken up into the following activities:

- The cardholder selects items for procurement.
- The cardholder is presented with an order form containing the list of items, their prices, and a total price including shipping, handling and taxes. This order form can be obtained from the website of the merchant or can be created on the cardholder's computer by special purpose electronic shopping software.
- The cardholder selects the means of payment—in this case, a payment card is selected.
- The cardholder sends the merchant a completed order form along with the payment instructions. The order and the payment instructions are digitally signed by the cardholder who is already in possession of digital signature certificates.
- The merchant requests payment authorisation from the cardholder's financial institution.

- On receiving authorisation, the merchant sends confirmation of the order.
- The merchant ships the goods or performs the requested services from the order.
- The merchant requests payment from the cardholder's financial institution.

In a SET transaction, the electronic processing begins with the cardholder. A cardholder uses a payment card that has been issued by an Issuer. SET ensures that in the cardholder's interactions with the merchant, the payment card account information remains confidential. An issuer is a financial institution that establishes an account for a cardholder and issues the payment card. The issuer guarantees payment for authorised transactions using the payment card in accordance with payment card brand regulations and local legislation. Merchants offer goods for sale or provide services in exchange for payment. With SET, a merchant can offer his cardholders secure electronic interactions. A merchant who accepts payment cards must have a relationship with an acquirer—the financial institution that establishes an account with a merchant and processes payment card authorisations and payments. The payment gateway is operated by an acquirer or a designated third party which processes merchant payment messages, including payment instructions from cardholders.

Within SET, public key cryptography is extensively used. Payment instructions are encrypted so that credit card numbers are not intelligible to anyone. Cardholders, merchants and acquirers are authenticated to each other and the integrity of the data contained in the payment instruction is maintained.