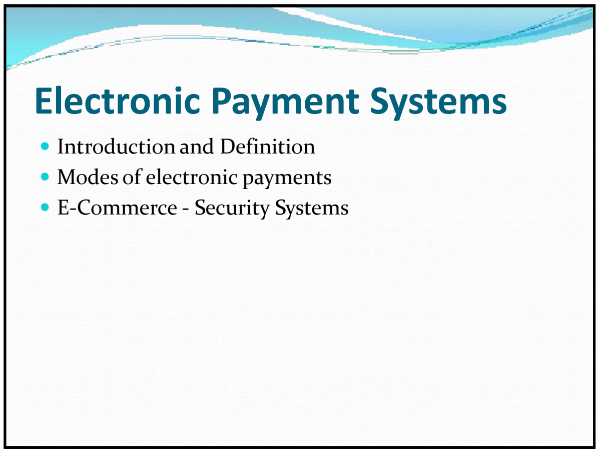
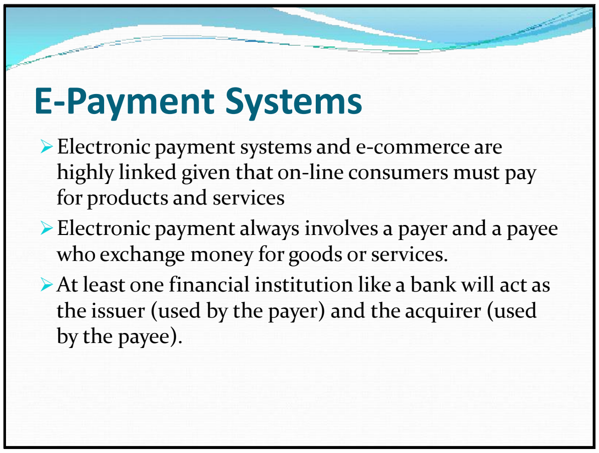


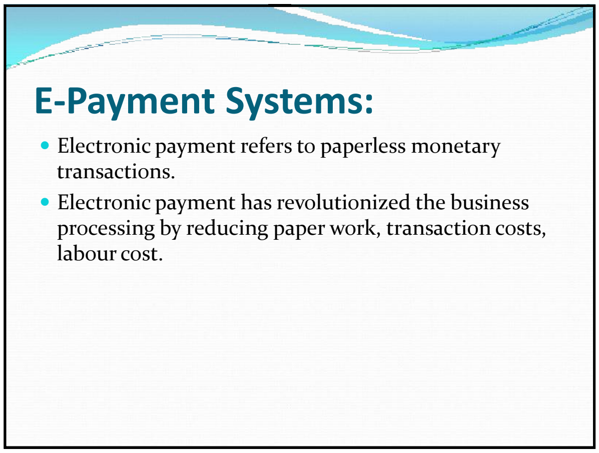
Electronic Payment Systems

- Introduction and Definition
- Modes of electronic payments
- E-Commerce - Security Systems



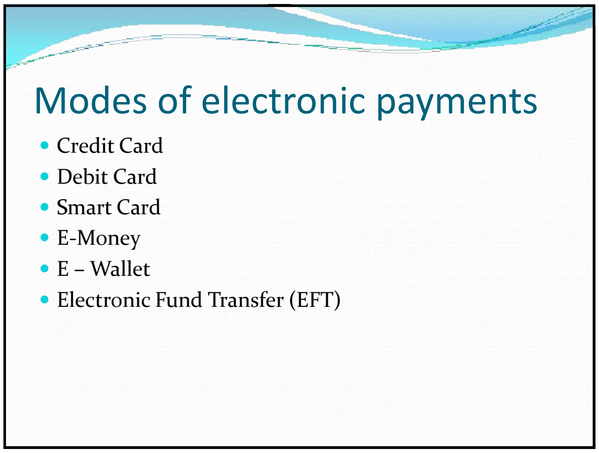
E-Payment Systems

- Electronic payment systems and e-commerce are highly linked given that on-line consumers must pay for products and services
- Electronic payment always involves a payer and a payee who exchange money for goods or services.
- At least one financial institution like a bank will act as the issuer (used by the payer) and the acquirer (used by the payee).



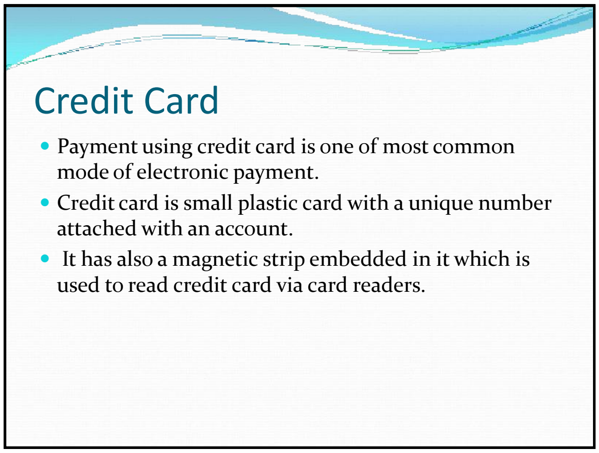
E-Payment Systems:

- Electronic payment refers to paperless monetary transactions.
- Electronic payment has revolutionized the business processing by reducing paper work, transaction costs, labour cost.



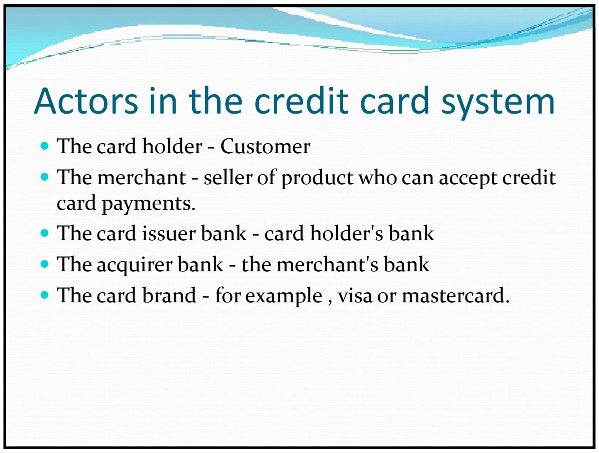
Modes of electronic payments

- Credit Card
- Debit Card
- Smart Card
- E-Money
- E – Wallet
- Electronic Fund Transfer (EFT)



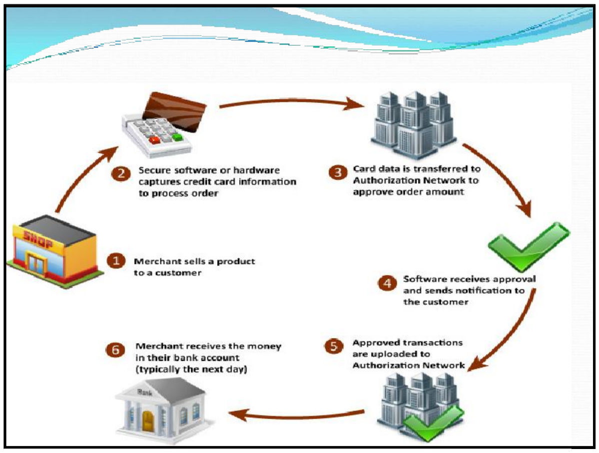
Credit Card

- Payment using credit card is one of most common mode of electronic payment.
- Credit card is small plastic card with a unique number attached with an account.
- It has also a magnetic strip embedded in it which is used to read credit card via card readers.



Actors in the credit card system

- The card holder - Customer
- The merchant - seller of product who can accept credit card payments.
- The card issuer bank - card holder's bank
- The acquirer bank - the merchant's bank
- The card brand - for example , visa or mastercard.



1 Merchant sells a product to a customer

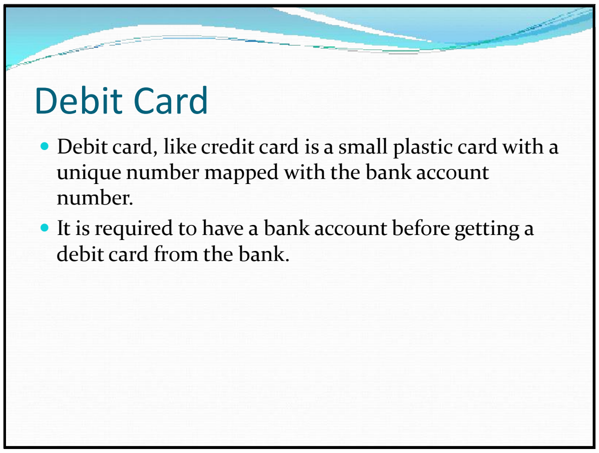
2 Secure software or hardware captures credit card information to process order

3 Card data is transferred to Authorization Network to approve order amount

4 Software receives approval and sends notification to the customer

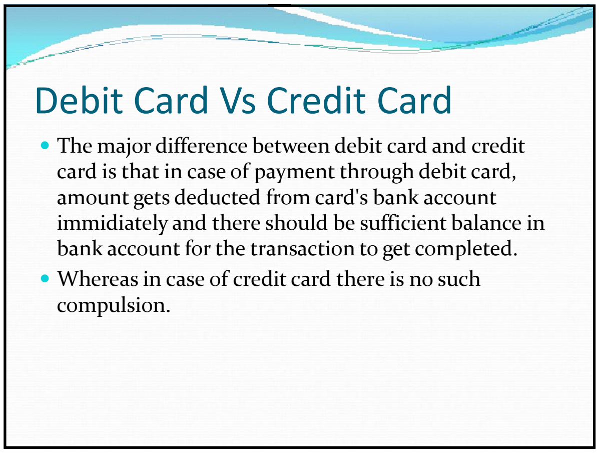
5 Approved transactions are uploaded to Authorization Network

6 Merchant receives the money in their bank account (typically the next day)



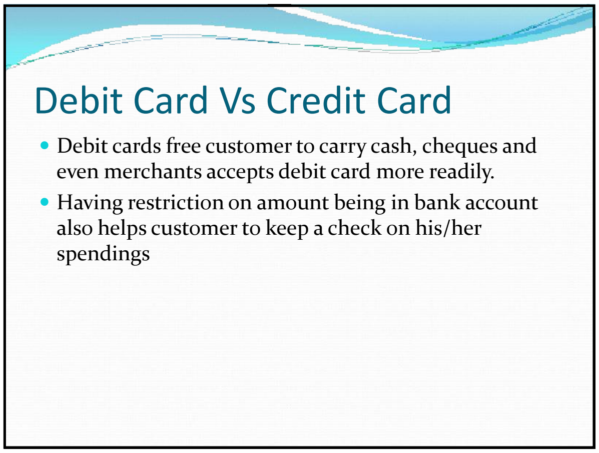
Debit Card

- Debit card, like credit card is a small plastic card with a unique number mapped with the bank account number.
- It is required to have a bank account before getting a debit card from the bank.



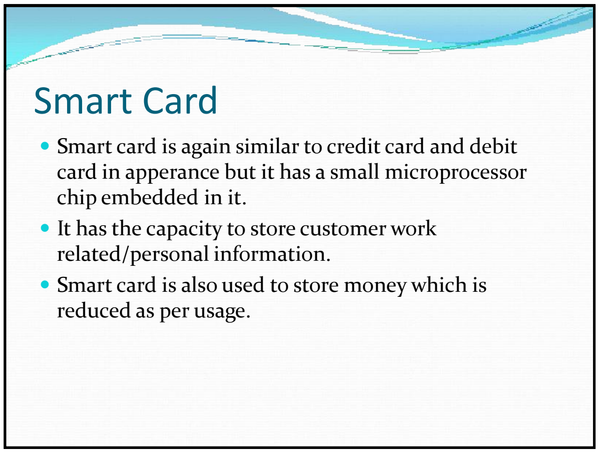
Debit Card Vs Credit Card

- The major difference between debit card and credit card is that in case of payment through debit card, amount gets deducted from card's bank account immidiately and there should be sufficient balance in bank account for the transaction to get completed.
- Whereas in case of credit card there is no such compulsion.



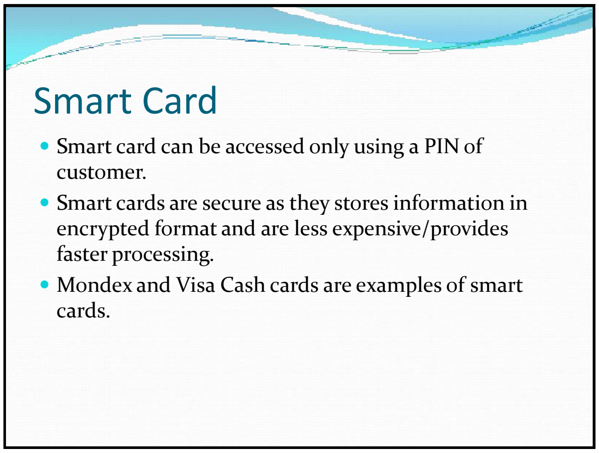
Debit Card Vs Credit Card

- Debit cards free customer to carry cash, cheques and even merchants accepts debit card more readily.
- Having restriction on amount being in bank account also helps customer to keep a check on his/her spendings



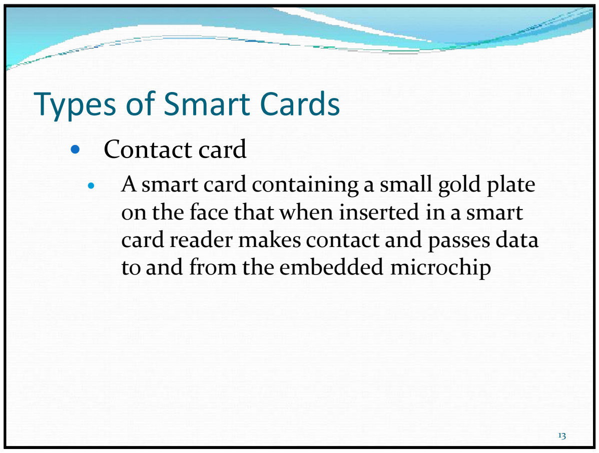
Smart Card

- Smart card is again similar to credit card and debit card in apperance but it has a small microprocessor chip embedded in it.
- It has the capacity to store customer work related/personal information.
- Smart card is also used to store money which is reduced as per usage.



Smart Card

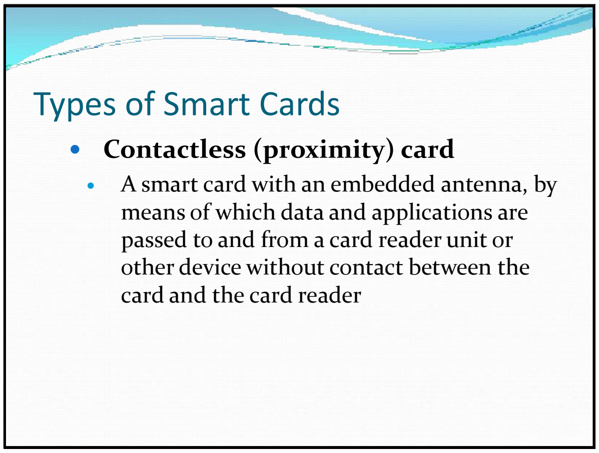
- Smart card can be accessed only using a PIN of customer.
- Smart cards are secure as they stores information in encrypted format and are less expensive/provides faster processing.
- Mondex and Visa Cash cards are examples of smart cards.



Types of Smart Cards

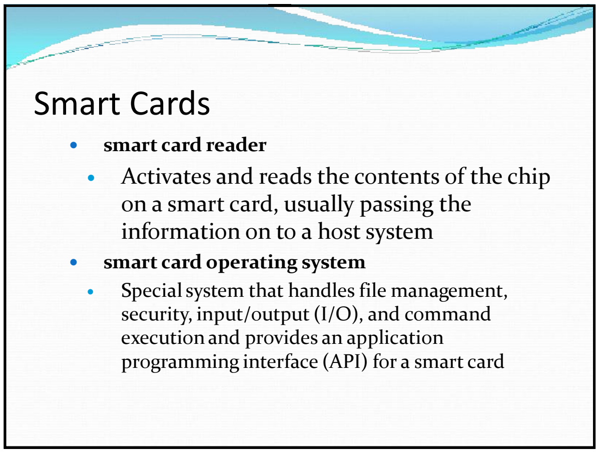
- Contact card
  - A smart card containing a small gold plate on the face that when inserted in a smart card reader makes contact and passes data to and from the embedded microchip

13



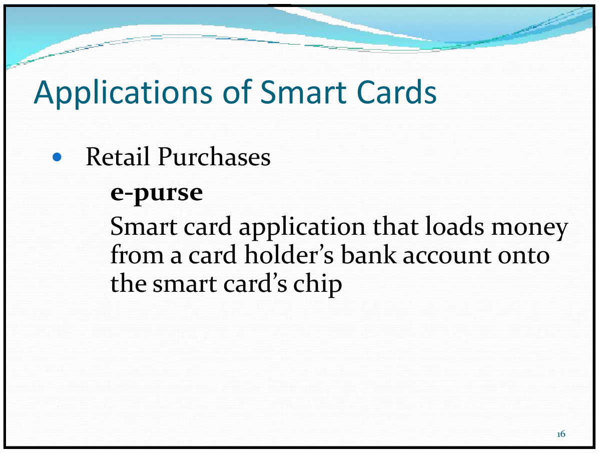
Types of Smart Cards

- **Contactless (proximity) card**
  - A smart card with an embedded antenna, by means of which data and applications are passed to and from a card reader unit or other device without contact between the card and the card reader



Smart Cards

- **smart card reader**
  - Activates and reads the contents of the chip on a smart card, usually passing the information on to a host system
- **smart card operating system**
  - Special system that handles file management, security, input/output (I/O), and command execution and provides an application programming interface (API) for a smart card



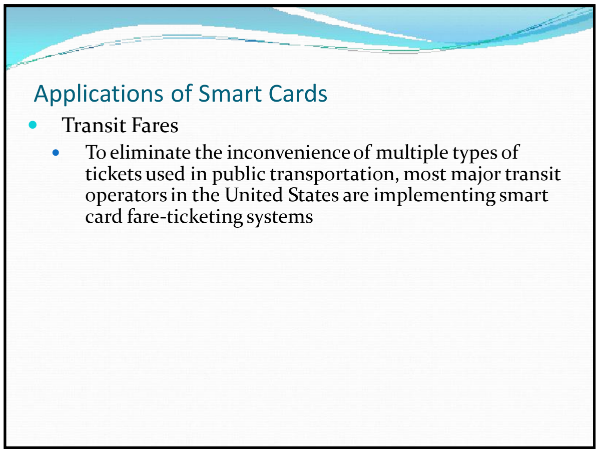
Applications of Smart Cards

- Retail Purchases

  e-purse

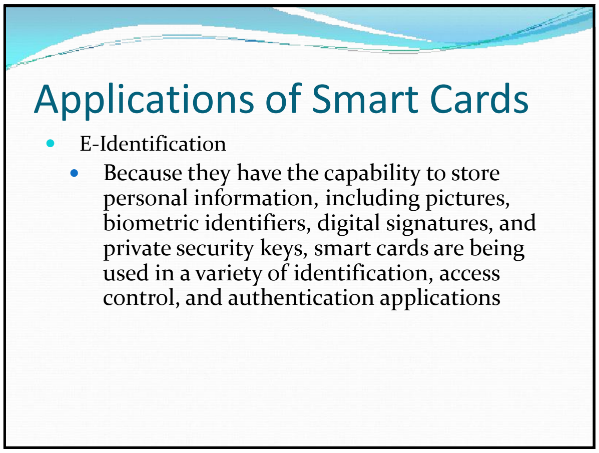
  Smart card application that loads money from a card holder's bank account onto the smart card's chip

16



Applications of Smart Cards

- Transit Fares
  - To eliminate the inconvenience of multiple types of tickets used in public transportation, most major transit operators in the United States are implementing smart card fare-ticketing systems



Applications of Smart Cards

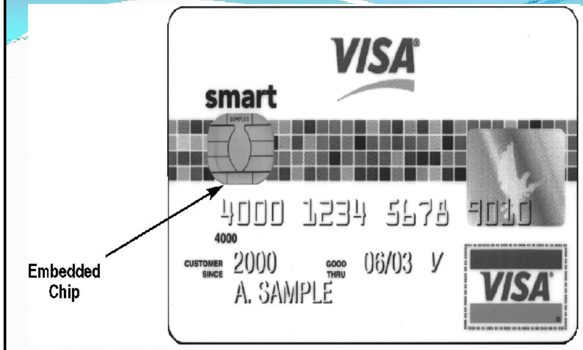
- E-Identification
  - Because they have the capability to store personal information, including pictures, biometric identifiers, digital signatures, and private security keys, smart cards are being used in a variety of identification, access control, and authentication applications

Applications of Smart Cards

- Applications of Smart Cards in Health Care
  - Storing vital medical information in case of emergencies
  - Preventing patients from obtaining multiple prescriptions from different physicians
  - Verifying a patient's identity and insurance coverage
  - Speeding up the hospital or emergency room admissions process

Applications of Smart Cards

- Applications of Smart Cards in Health Care
  - Storing vital medical information in case of emergencies
  - Providing medical practitioners with secure access to a patient's complete medical history
  - Speeding up the payment and claims process
  - Enabling patients to access their medical records over the Internet



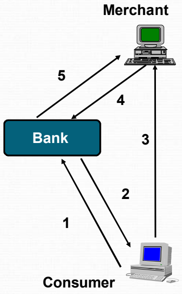
E-Money

- E-Money transactions refers to situation where payment is done over the network and amount gets transferred from one financial body to another financial body without any involvement of a middleman.
- E-money transactions are faster, convenient and saves a lot of time.

E-Money

- Online payments done via credit card, debit card or smart card are examples of e-money transactions.
- Another popular example is e-cash.
- In case of e-cash, both customer and merchant both have to sign up with the bank or company issuing e-cash.

E-cash Concept



1. Consumer buys e-cash from Bank
2. Bank sends e-cash bits to consumer (after charging that amount plus fee)
3. Consumer sends e-cash to merchant
4. Merchant checks with Bank that e-cash is valid (check for forgery or fraud)
5. Bank verifies that e-cash is valid
6. Parties complete transaction: e.g., merchant present e-cash to issuing back for deposit once goods or services are delivered

Consumer still has (invalid) e-cash

Electronic Wallets

- Stores credit card, electronic cash, owner identification and address
  - Makes shopping easier and more efficient
    - Eliminates need to repeatedly enter identifying information into forms to purchase
    - Works in many different stores to speed checkout
  - Amazon.com one of the first online merchants to eliminate repeat form-filling for purchases

Electronic Wallets

- Agile Wallet
  - Developed by CyberCash
  - Allows customers to enter credit card and identifying information once, stored on a central server
  - Information pops up in supported merchants' payment pages, allowing one-click payment

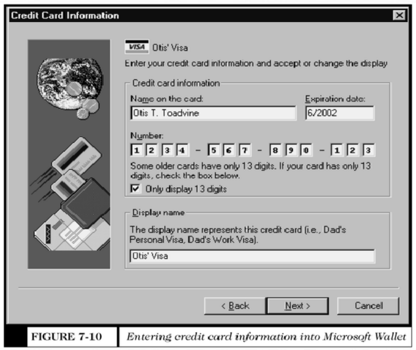
Electronic Wallets

- eWallet
  - Developed by Launchpad Technologies
  - Free wallet software that stores credit card and personal information on users' computer, not on a central server; info is dragged into payment form from eWallet
  - Information is encrypted and password protected
  - Works with Netscape and Internet Explorer

Electronic Wallets

- Microsoft Wallet
  - Comes pre-installed in Internet Explorer 4.0, but not in Netscape
  - All information is encrypted and password protected
  - Microsoft Wallet Merchant directory shows merchants setup to accept Microsoft Wallet

Entering Information Into Microsoft Wallet



Credit Card Information

VISA Otis' Visa

Enter your credit card information and accept or change the display

Credit card information

Name on the card: Otis T. Toadvine

Expiration date: 6/2002

Number: 1 2 3 4 - 5 6 7 - 8 9 0 - 1 2 3

Some older cards have only 13 digits. If your card has only 13 digits, check the box below.

☑ Only display 13 digits

Display name

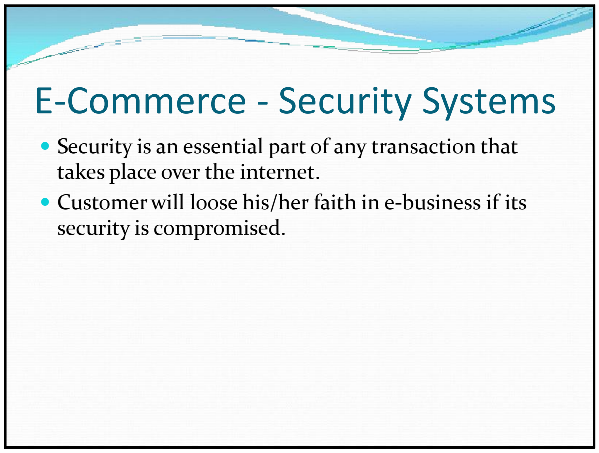
The display name represents this credit card (i.e., Dad's Personal Visa, Dad's Work Visa).

Otis' Visa

FIGURE 7-10 *Entering credit card information into Microsoft Wallet*

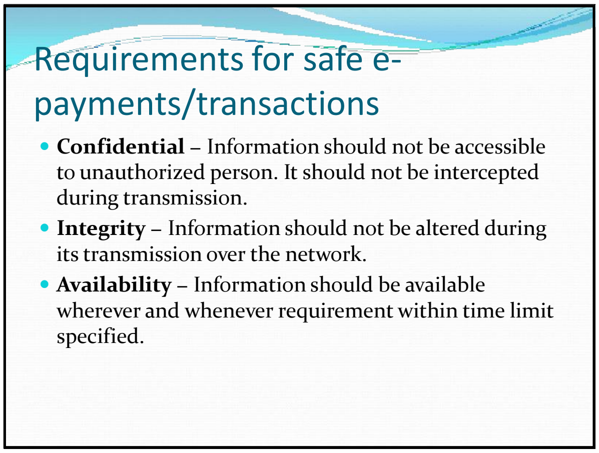
Electronic Fund Transfer

- It is a very popular electronic payment method to transfer money from one bank account to another bank account.
- Accounts can be in same bank or different bank.
- Fund transfer can be done using ATM (Automated Teller Machine) or using computer.
- Once amount is transferred to other account, customer is notified of the fund transfer by the bank.



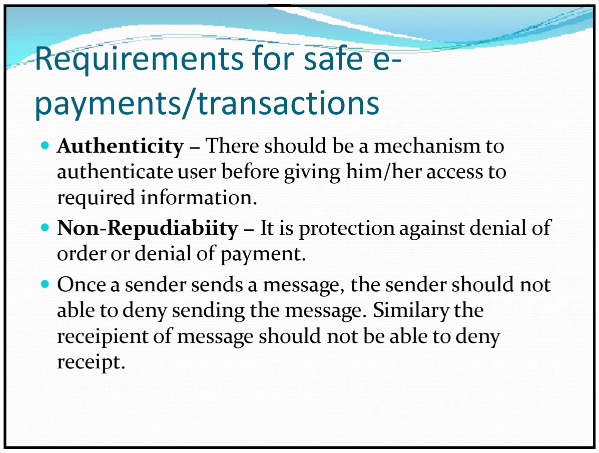
E-Commerce - Security Systems

- Security is an essential part of any transaction that takes place over the internet.
- Customer will loose his/her faith in e-business if its security is compromised.



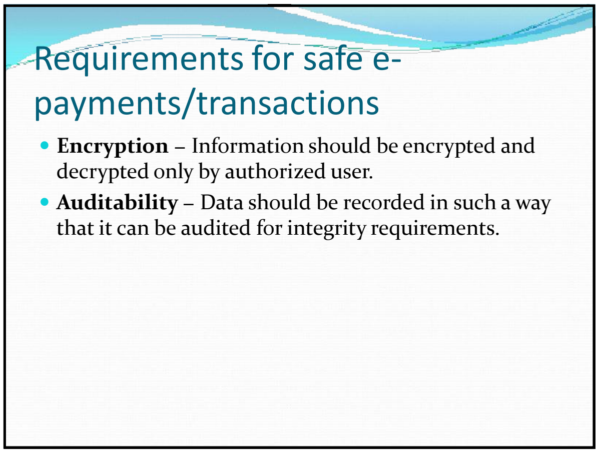
Requirements for safe e-payments/transactions

- **Confidential** – Information should not be accessible to unauthorized person. It should not be intercepted during transmission.
- **Integrity** – Information should not be altered during its transmission over the network.
- **Availability** – Information should be available wherever and whenever requirement within time limit specified.



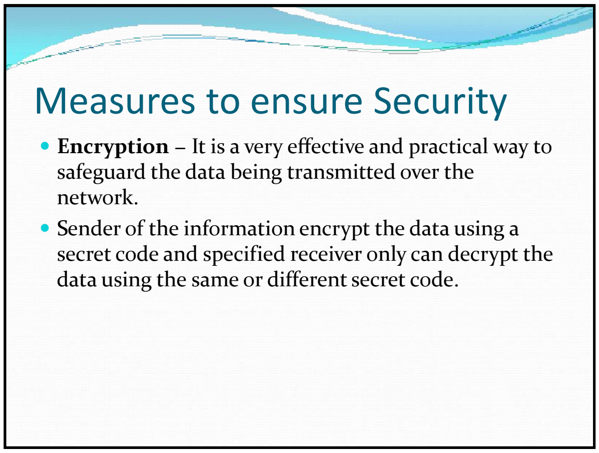
Requirements for safe e-payments/transactions

- **Authenticity** – There should be a mechanism to authenticate user before giving him/her access to required information.
- **Non-Repudiabiity** – It is protection against denial of order or denial of payment.
- Once a sender sends a message, the sender should not able to deny sending the message. Similary the receipient of message should not be able to deny receipt.



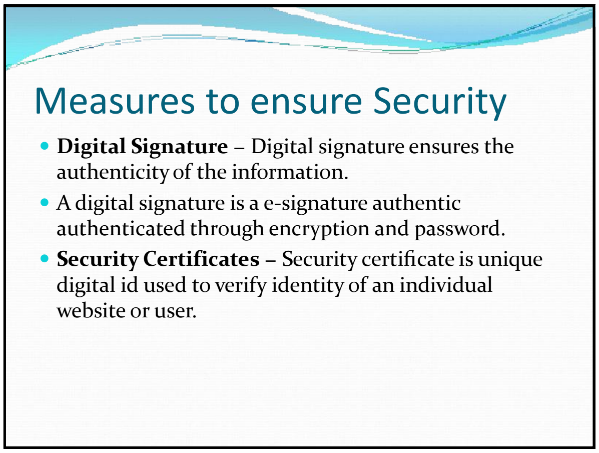
Requirements for safe e-payments/transactions

- **Encryption** – Information should be encrypted and decrypted only by authorized user.
- **Auditability** – Data should be recorded in such a way that it can be audited for integrity requirements.



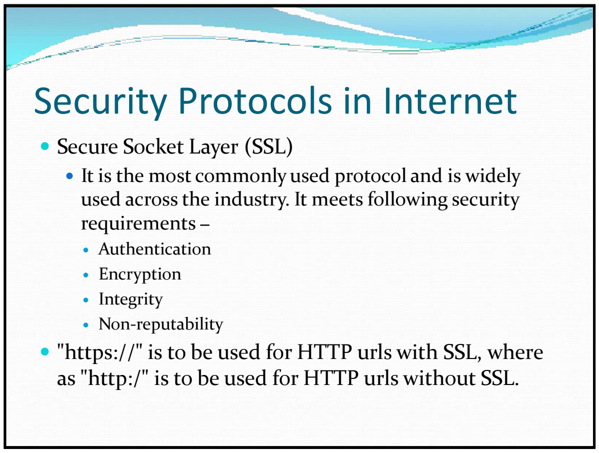
Measures to ensure Security

- **Encryption** – It is a very effective and practical way to safeguard the data being transmitted over the network.
- Sender of the information encrypt the data using a secret code and specified receiver only can decrypt the data using the same or different secret code.



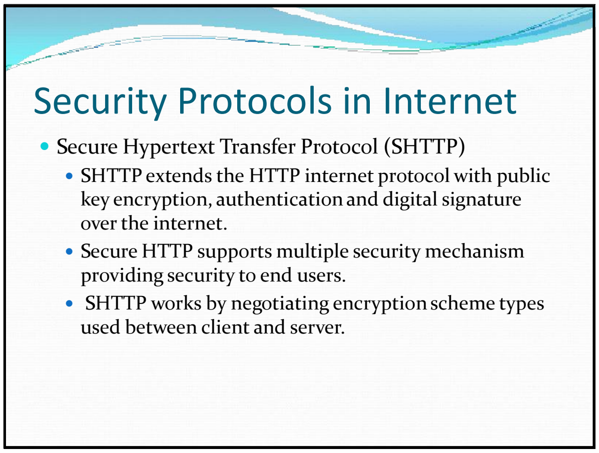
Measures to ensure Security

- **Digital Signature** – Digital signature ensures the authenticity of the information.
- A digital signature is a e-signature authentic authenticated through encryption and password.
- **Security Certificates** – Security certificate is unique digital id used to verify identity of an individual website or user.



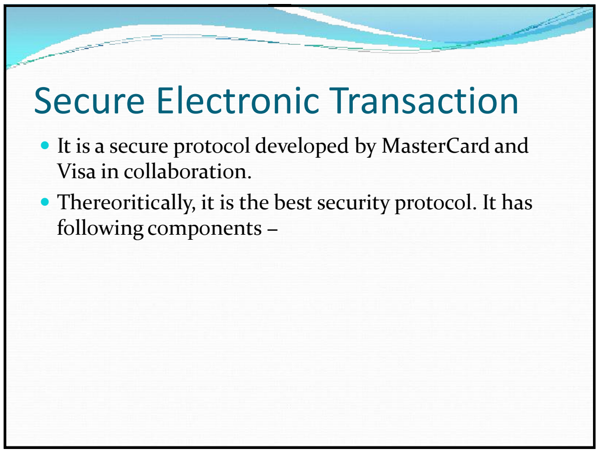
Security Protocols in Internet

- Secure Socket Layer (SSL)
  - It is the most commonly used protocol and is widely used across the industry. It meets following security requirements –
    - Authentication
    - Encryption
    - Integrity
    - Non-reputability
- "https://" is to be used for HTTP urls with SSL, where as "http:/" is to be used for HTTP urls without SSL.



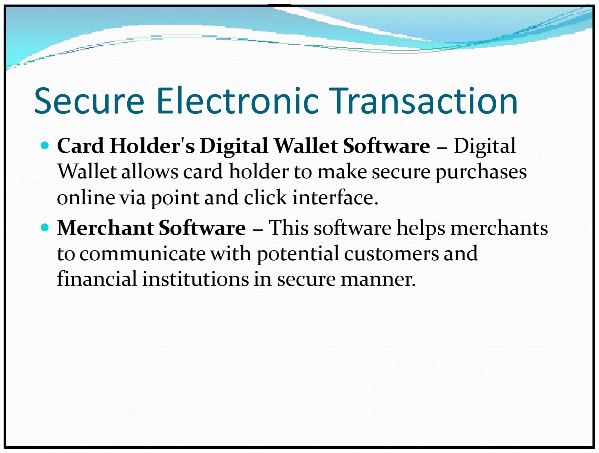
Security Protocols in Internet

- Secure Hypertext Transfer Protocol (SHTTP)
  - SHTTP extends the HTTP internet protocol with public key encryption, authentication and digital signature over the internet.
  - Secure HTTP supports multiple security mechanism providing security to end users.
  - SHTTP works by negotiating encryption scheme types used between client and server.



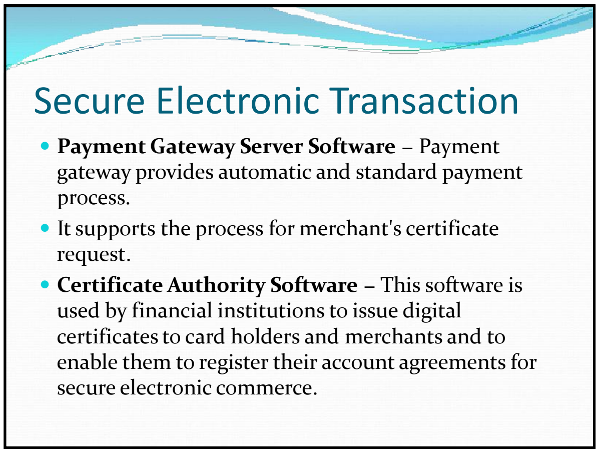
Secure Electronic Transaction

- It is a secure protocol developed by MasterCard and Visa in collaboration.
- Thereoritically, it is the best security protocol. It has following components –



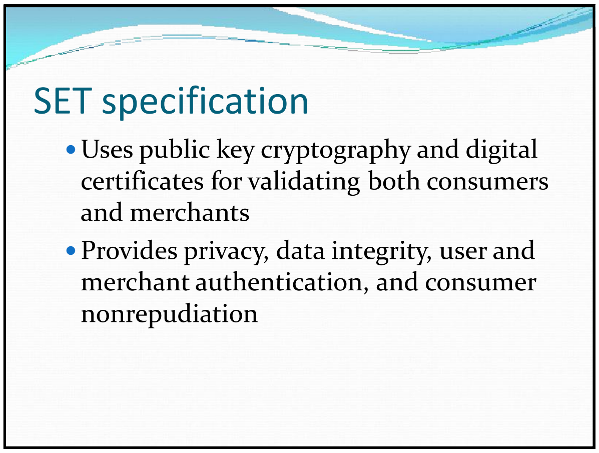
Secure Electronic Transaction

- **Card Holder's Digital Wallet Software** – Digital Wallet allows card holder to make secure purchases online via point and click interface.
- **Merchant Software** – This software helps merchants to communicate with potential customers and financial institutions in secure manner.



Secure Electronic Transaction

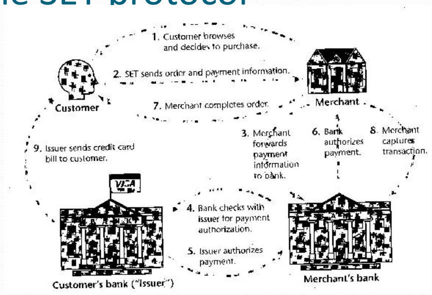
- **Payment Gateway Server Software** – Payment gateway provides automatic and standard payment process.
- It supports the process for merchant's certificate request.
- **Certificate Authority Software** – This software is used by financial institutions to issue digital certificates to card holders and merchants and to enable them to register their account agreements for secure electronic commerce.



SET specification

- Uses public key cryptography and digital certificates for validating both consumers and merchants
- Provides privacy, data integrity, user and merchant authentication, and consumer nonrepudiation

The SET protocol


1. Customer browses and decides to purchase.
2. SET sends order and payment information.
Customer
Merchant
7. Merchant completes order.
9. Issuer sends credit card bill to customer.
3. Merchant forwards payment information to bank.
6. Bank authorizes payment.
8. Merchant captures transaction.
VISA
4. Bank checks with issuer for payment authorization.
5. Issuer authorizes payment.
Customer's bank ("Issuer")
Merchant's bank

The SET protocol coordinates the activities of the customer,
merchant, merchant's bank, and card issuer. [Source:

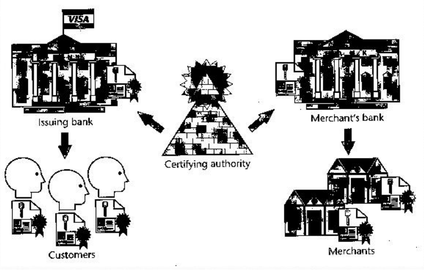
SET Payment Transactions

- SET-protected payments work like this:
  - Consumer makes purchase by sending encrypted financial information along with digital certificate
  - Merchant's website transfers the information to a payment card processing center while a Certification Authority certifies digital certificate belongs to sender

SET Payment Transactions

- Payment card-processing center routes transaction to credit card issuer for approval
- Merchant receives approval and credit card is charged
- Merchant ships merchandise and adds transaction amount for deposit into merchant's account

SET uses a hierarchy of trust



All parties hold certificates signed directly or indirectly by a certifying authority. [Source: Stein]

Problems with SET

- Not easy to implement
- Not as inexpensive as expected
- Expensive to integrated with legacy applications
- Not tried and tested, and often not needed
- Scalability is still in question