UNIT- 3 : Electronic Payment System

Course outline:

- E-payment System, Online Credit Card Transaction,
- Digital and Mobile Wallet, Smart Cards, Social/Mobile Peer-to-Peer Payment Systems,
- Digital Cash/e-cash, E-Checks, Virtual Currency, Electronic Billing Presentment and Payment (EBPP) System,
- SET Protocol, Features of SET, Participants in SET, Card Holder Registration, Merchant Registration, Purchase Request, Dual Signature, Payment Authorization, Payment Capture,
- Status of E-Payment Systems in Nepal, Case Studies of Global and Local Payment Systems

Electronic Payment System

- Electronic Payment System allows people to make online payments for their purchases of goods and services without the physical transfer of cash and cheques, irrespective of time and location.
- The key components of this payment system are the payers and payees, financial institutions, electronic devices, communication networks, payment gateways, and mobile payment apps.
- As the global economy continues to evolve, the dependency on physical modes of payment is gradually giving way to digital alternatives that offer speed, convenience, and efficiency.
- These systems facilitate a diverse range of financial activities, from online purchases and bill payments to person-to-person transfers.
- Electronic Payment System allows customers to pay for goods and services electronically without the use of cheques or cash.
- Businesses need a strong and secure electronic payment system in online dealings.
- Electronic Payment System is regulated in India by the RBI.
- The system is safe, speedy, and cost-effective in comparison with paper-based payment systems.
- The **objectives** of electronic payment system technology are **to support the quick**, **efficient transfer of funds** and enable users to make paperless payments.

Stakeholders in Payment Systems

- **Consumers** are interested primarily in low-risk, low-cost, convenient, and reliable payment mechanism. Consumers have demonstrated that they will not use new payment mechanism unless they are equally or more
- **Merchants** are interested primarily in low-risk, low-cost, secure and reliable payment mechanism. Merchants currently carry much of the risk of credit card fraud and much of the hardware cost of verifying payments.
- **Financial intermediaries such** as banks and credit card networks are primarily interested in secure payment systems that transfer risks and cost to consumers and merchant, while maximizing transaction fees payable to them.
- **Government regulators** are interested in maintaining trust in the financial systems. Regulators seek to protect against fraud and abuse in the use of payment systems, ensure that the interests of consumers and merchants are balanced against the interest of the financial intermediaries whom they regulate; and enforce information reporting laws.

Characteristics of Electronic Payment System:

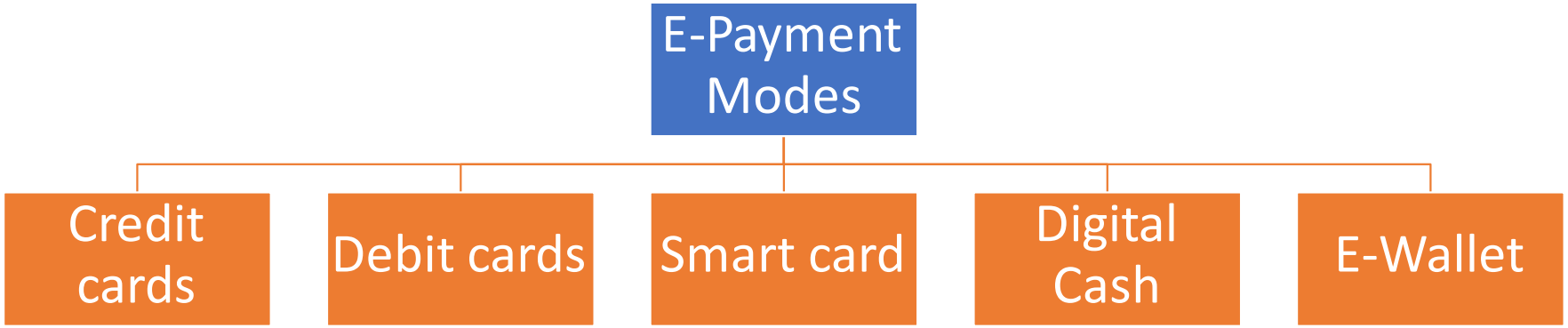
- **Applicability**: Applicability of payment system is the extent with which it is accepted as payment. Users should be able to pay for goods and services easily by using the system.
- **Easy to use**: The system should not be complex. A user from the remote area should be able to use the system.
- **Security:** It means e-payment systems should be able to resist attacks. Creation, modification and over spending of the value (money) should be protected.
- **Reliability:** It means system should run smoothly in all scenarios. It should be free from failures.
- **Trust**: It is the degree of the confidence that the money and the personal information are safe.
- **Scalability**: System should be scalable by timely changes in the underlying infrastructure.
- **Convertibility**: It means funds represented in one mechanism should be easily convertible to funds in another mechanism.
- **Interoperability:** System should be operable in between multiple service providers.
- **Efficiency:** It means cost of the handling payment should be reasonable.
- **Anonymity**: It is the feature related to privacy of user. System should be able to protect the identity of the user.
- **Traceability**: System should be able to link spending with the users even if the identity of the user is anonymous.
- **Authorization Type**: It is considered good if a payment system is useful in both online and offline environment.

Advantages of Electronic Payment System

- **24/7 Accessibility:** Electronic Payments can be made at any time, providing round-the-clock access to financial transactions.
- **Global Accessibility:** Users can make payments and transfer funds globally without being restricted by geographical boundaries.
- **Instant Transactions**: Electronic Payments are processed quickly, allowing for near-instantaneous transfer of funds between accounts.
- **Faster Settlement:** Compared to traditional payment methods, electronic transactions often result in faster settlement times.
- **Record-Keeping and Tracking:** Electronic Payment Systems facilitate easy record-keeping for both businesses and individuals.
- **Encryption and Authentication:** Electronic Payment Systems employ robust encryption and authentication protocols to secure transactions and protect sensitive information.

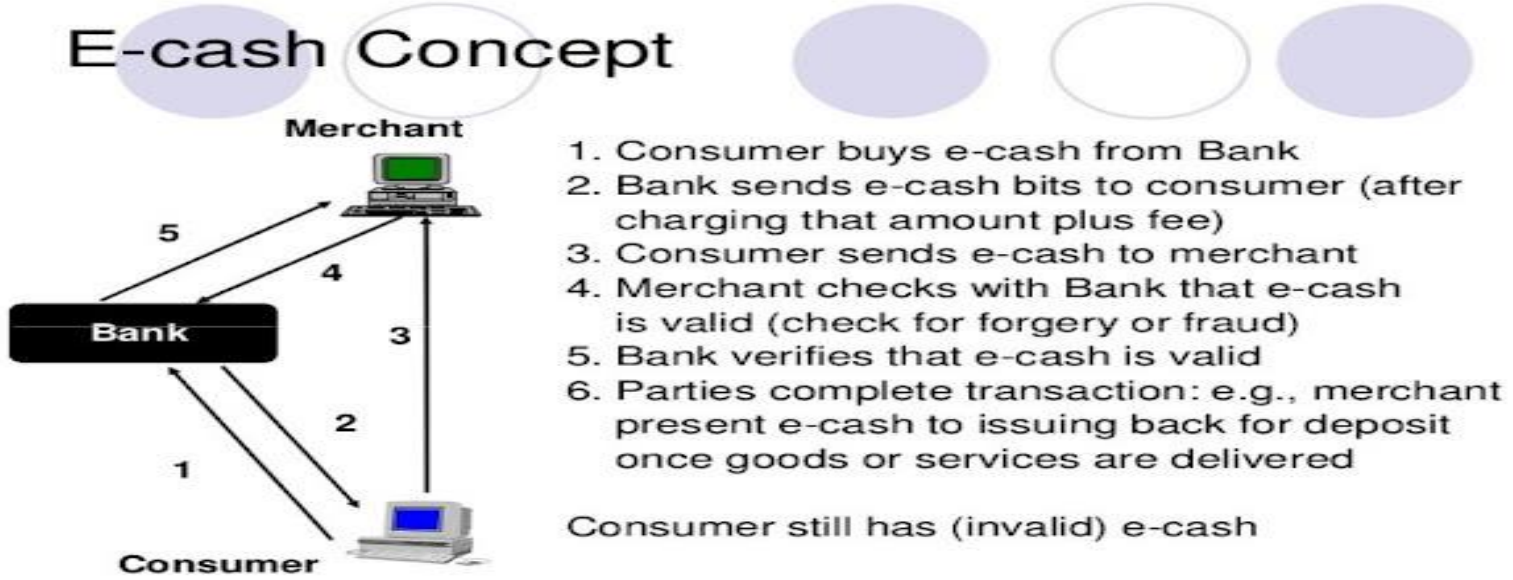
Disadvantages of Electronic Payment System

- **Security Concerns:** Electronic Payment Systems are susceptible to security breaches, including hacking, phishing, and identity theft.
- **Technical Issues**: Electronic Payment Systems rely on technology, and technical glitches or system failures can disrupt transactions.
- **Fraud Risk:** Despite security measures, Electronic Payment Systems are not immune to fraud. Unauthorized transactions, stolen credentials, or fraudulent activities can occur, leading to financial losses for individuals and businesses.
- **Privacy Concerns**: Users may be concerned about the collection and storage of personal information by electronic payment providers.
- **Transaction Fees**: Some electronic payment systems impose transaction fees, which can add up over time.


E-Payment Modes
Credit cards
Debit cards
Smart card
Digital Cash
E-Wallet

E-Cash (Digital Cash)

- Electronic cash is a new concept in online payment systems because it combines computerized convenience with security and privacy that improve on paper cash.
  - Its versatility opens up a host of new market and application.
  - E-cash is an electronic or digital form of value storage and value exchange that has limited convertibility into other forms of value. It requires intermediaries to convert.



Digital Cash

What is Digital Cash?

- Digital Cash acts much like real cash, except that it's not on paper.
- Money in your bank account is converted to a digital code.
- This digital code may then be stored on a microchip, a pocket card (like a smart card), or on the hard drive of your computer.

- The concept of privacy is the driving force behind digital cash. The user of digital cash is assured an anonymous transaction by any vendor who accepts it.
- Your special bank account code can be used over the internet or at any participating merchant to purchase an item.
- Everybody involved in the transaction, from the bank to the user to the vendor, agree to recognize the worth of the transaction, and thus create this new form or exchange.

How does Digital Cash work?

- This example shows how digital cash might work through a banking institution. The bank creates a digital bank note by signing a message which specifies the serial number (with a primary or public key) and value of the note, and sends it to Person A. Person A, as he withdraws it, uses Chaum's technique (A Cryptography technique) to alter the serial number so that the bank will not recognize the note as being from this withdrawal. This note is now returned to the bank with the new serial number. The bank now has a note with a new serial number. Person A then pays Person B electronically by sending the bank note to him. Person B checks the note's validity by decrypting using the bank's public key to check its signature (new serial number validity). Person B then sends the note to the bank, which checks the serial number to confirm that this bank note hasn't been spent before. The serial number is now different from that in Person A's withdrawal, thereby pre- venting the bank from linking the two transactions. The enabling bank merely checks the new serialized key account for the amount of the transaction and transfers the money by sending out a depository notice. Person B using the same encrypting technique returns the depository notice with the new serialize account. The enabling bank does not know who the merchant is only that money is available for payment. In some respects, this is a debit card transaction with no information other than the amount of the transaction. All initial depositor information is in the primary key account not the password account.

Special software to enable these dual track procedures was developed by Digicash. However this venture was not successful, nor was it successful for its successor corporation, CyberCash, Inc.

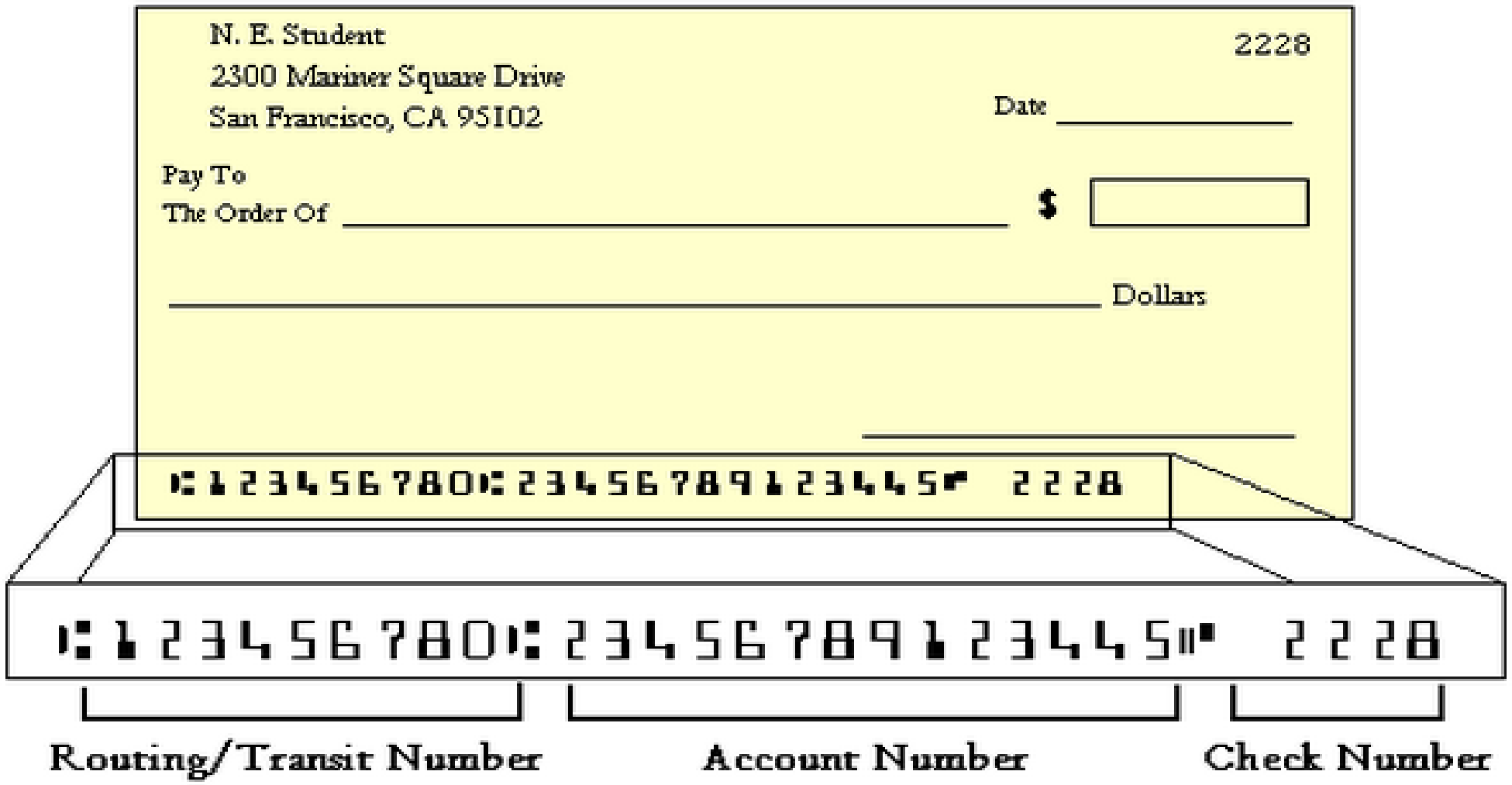
E-Cash (Digital Cash) Cont..

- ***Advantages of E-Cash***
- Lower Transaction Cost
- Convenient
- Authorization not required
- Suitable for small payments
- ***Limitations of E-Cash***
- High financial risk as e-cash may be stolen by hackers
- The vendors should have an account in the same bank which issued the e-cash
- ***Electronic Cash Issues***
- E-cash must allow spending only once
- - Must be anonymous, just like regular currency
- - Safeguards must be in place to prevent counterfeiting
- Must be independent and freely transferable regardless of nationality or storage mechanism
- Divisibility and Convenience Complex transaction (checking with Bank)

e-Cheque

- It's simply an electronic version of a paper check. An e-check uses the same legal and business protocols associated with traditional paper checks.
  - Electronic cheque fulfills the needs of many business organizations, which are previously exchanging paper-based cheque based on the vendors, consumers and government.
  - Working process of e-cheque is as same as that of the traditional cheque payment system.
  - An account holder will issue the electronic cheque document which contains the information such as name of the account holder payee name, name of the financial institution; payer account number and the amount of payment on the cheque.
  - Most of the information is in uncoded form. Like a paper cheque, e-cheques also bear the digital equivalent of signature, which is called digital signature.
  - It is a new payment instrument that combines high-security, speed, convenience, and processing efficiencies for online transactions.

e-Cheque Format



e-Cheque Cont..

Advantages

- Pay Quickly and Control Your Cash Flow
- Save Money
- Save Time
- Pay More Safely and Securely
- Compatible With Your Current Accounting Software
- Pay from Anywhere, Anytime.
- Faster Processing Fee and
- Labor Reduction Customer Payment Options.

Disadvantage

- Fraud Potential.
- Errors and Reduced Float.

Credit Cards

Credit is small plastic card with a unique number linked with an account.

It has magnetic strip or chip embedded init which is used to read by credit card reader.

Parties involved in credit card payment :

•**A cardholder** obtains a credit or debit card from an **issuing bank,** uses the account to pay for goods or services.

•**A merchant** is any type of business that accepts card payments in exchange for goods or services.

•**A merchant bank** establishes and maintains merchant accounts. Merchant banks allow merchants to accept deposits from credit and debit card payments.

•**Payment processors** are companies that process credit and debit card

transactions. Payment processors connect merchants, merchant banks, card networks and others to make card payments possible.

•**Issuing banks** are the banks, credit unions and other financial institutions that issue debit and credit cards to cardholders through the card

associations.

•**Card associations** include Visa, Mastercard, Discover and American Express. The card associations set interchange rates and qualification

guidelines, and act as the arbiter between **issuing banks** and **acquiring banks** among other vital functions.

Credit Card Cont..

- A credit card is termed as payment card, representing the majority of online payments because people are familiar with them, and merchants avoid the expense of a paper invoicing system.
- In this card payments are simple anywhere and, in any currency, thus it matches the global reach of the internet.
- To avoid the complexity associated with token-based payment methods, consumers and vendors are also looking at credit card payment on the internet as one possible time-tested alternative.
- There is nothing new in the basic process. Without doubt, the basic means of payment used and initiated via the internet for consumer transactions till date is the credit card.
- If consumers want to purchase a product or service, they simply send their credit card details to the service pro

Credit Card Cont..

- ***We can break credit cards payment on online networks into three basic categories:***
- **Payments using Plain Credit Card Details:**

  o The easiest method of payment is the exchange of unencrypted credit cards over a public network such as telephone line or the internet.

  o The low level of security inherent in the design of the internet makes this method problematic.

  o Authentication is also a significant problem, and the vendor usually responsible to ensure that the person using the credit card is its owner. Without encryption, there is no way to do it.

- **Payments using Encrypted Credit Card Details:**

  o It would make sense to encrypt your credit card details before sending them out, but even then, there are certain factors to consider.

  o One would be the cost of credit card transactions itself. Such cost would prohibit low value payments (micro-payments) by adding costs to the transactions.

- **Payments using Third Party Verification:**

  o One solution to security and verification problems is the introduction of a third party; a company that collects and approves payments from one client to another.

  o After a certain period of time, one credit card transaction for the total accumulated amount is completed.

Credit Card Cont..

- ***The participants involved in credit card payments include:***
  - **Customer/Cardholder**: The consumer doing the purchase, using a credit card that has been issued by its issuer.
  - **Issuer:** The financial institution (i.e., bank) that issues the card to the cardholder. The issuer guarantees payment for authorized transactions.
  - **Merchant:** The merchant offers the goods and services, and has a financial relationship with the acquirer.
  - **Acquirer:** The financial institution of the merchant. The acquirer processes credit card authorizations and payments.
  - **Clearing House:** The credit card processing centers (clearinghouse) are institution that handles verification of accounts and balances.

Credit Card Payment Process

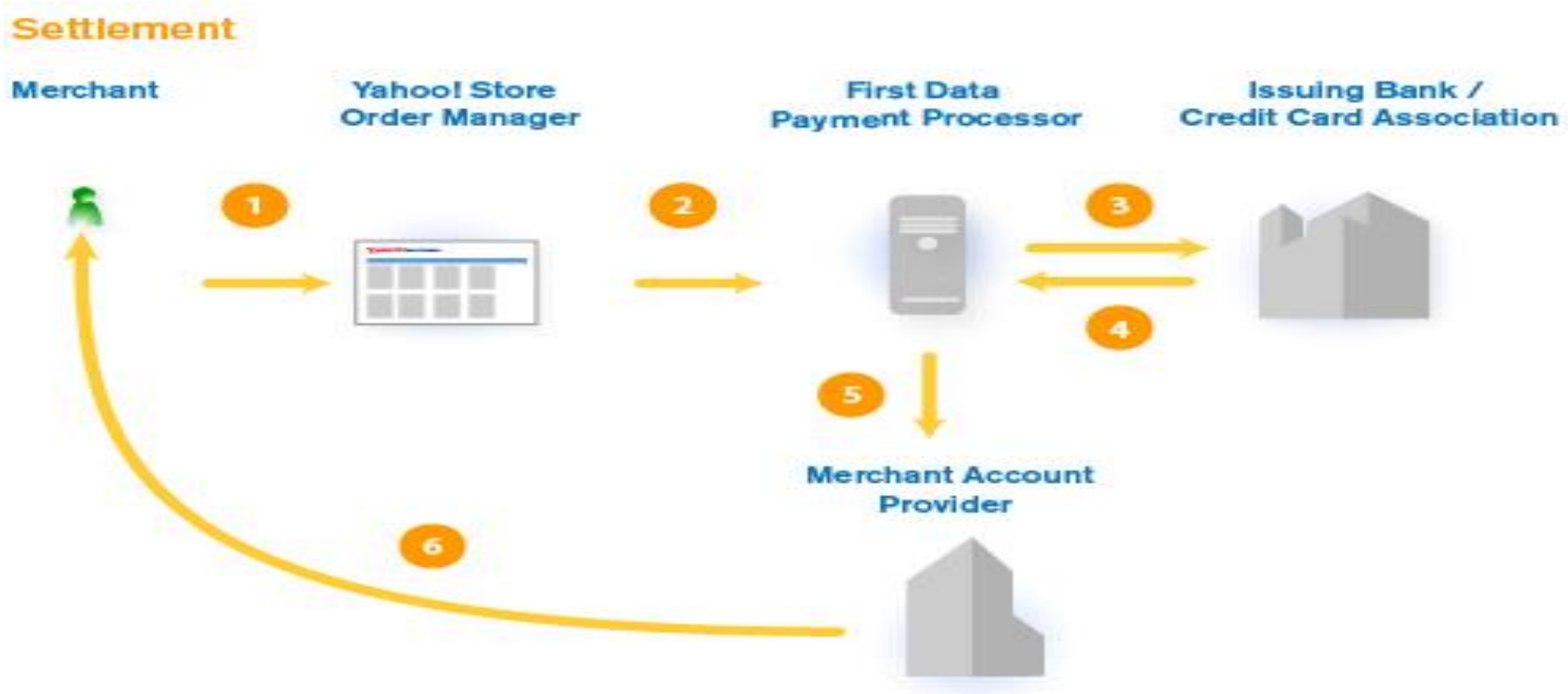
Step	Description
Step 1	Bank issues and activates a credit card to the customer on his/her request.
Step 2	The customer presents the credit card information to the merchant site or to the merchant from whom he/she wants to purchase a product/service.
Step 3	Merchant validates the customer's identity by asking for approval from the card brand company.
Step 4	Card brand company authenticates the credit card and pays the transaction by credit. Merchant keeps the sales slip.
Step 5	Merchant submits the sales slip to acquirer banks and gets the service charges paid to him/her.
Step 6	Acquirer bank requests the card brand company to clear the credit amount and gets the payment.
Step 7	Now the card brand company asks to clear the amount from the issuer bank and the amount gets transferred to the card brand company.

Working Techniques of Credit Cards

- Credit card payment processing for the e-commerce electronic payment system takes place in two phases:
- authorization (getting approval for the transaction that is stored with the order) and
- settlement (processing the sale which transfers the funds from the issuing bank to the merchant's account).
- The flow charts below represent the key steps in the process starting from what a customer sees when placing an order through completing the sale and finishing with the merchant processing the sale to collect funds.

Authorization Process of Credit Cards.

Settlement Process of Credit Cards



How Credit Card Works?

- When a consumer wants to make a purchase, he or she adds the item to the merchant's shopping cart.
- When the consumer wants to pay for item in the shopping cart, a secure tunnel through the Internet is created using SSL. Using encryption, SSL secures the session during which credit card information will be sent to the merchant and protects the information from the interlopers on the Internet.
- SSL does not authenticate either the merchant or the consumer. The transaction parties have to trust to one another. Once the consumer credit card information is received by the merchant, the merchant software contacts a clearinghouse.
- A clearing house verifies account balances. The clearing house contacts the issuing bank to verify the account information.
- Once verified the issuing bank credits the account of the merchant at the merchant's banks (usually occurs in a batch processes and it may happen in a few hours, or even in a few days).
- Once the merchant has received the payment gateway's digital signature; he will ship the goods to the cardholder knowing that the customer transaction has been approved.

Advantages of Credit Card

- The system is familiar to users and was widely used before the advent of e-commerce, thus maintaining the user's confidence.
- Transaction costs are hidden from users (i.e., basically met by sellers).
- Payment is simple anywhere and, in any currency, thus matching the global reach of the internet.
- The credit issuing company shares the transaction risk, helping overcome consumer's fear and reluctance to buy goods they have not actually seen, from sellers they do not know.
- **Cash back**: Many banks offer cash back opportunities if you use your card to pay monthly bills (electricity) or for grocery purchases. Besides, online shopping portals too have cash back offers on various products.
- **Reward points**: Credit card companies offer reward points for any purchases you make with your card.
- EMIs: If you are making a big purchase (TV, refrigerator, laptop), you can easily convert it to affordable monthly installments. Banks usually charge interest for conversion to EMIs.
- **Grace period**: You can defer your payments till your bill is due. Banks offer a maximum 50-day grace period for paying back your dues.
- **Safety:** Credit cards are safer than debit cards as in case of fraud you are not out of money immediately. Payment gateways like Visa, Mastercard also offer additional password protection while using the cards online.

Disadvantages of Credit Card Payment

- Relatively high transaction cost makes them impractical for small value payments.
- They cannot be used directly by individuals to make payments to other individuals.
- Protecting the security of transaction is vital, especially in the virtual world there is no payment guarantee to the merchant by a bank.
- All of the people do not have access to credit cards, so it can’t be treated as a default payment processing method for all electronic transactions.

What Is a Debit Card?

- A debit card is a payment card that deducts money directly from your checking account. Also called “check cards” or "bank cards," debit cards can be used to buy goods or services or to get cash from an ATM.
- Debit cards can help you reduce the need to carry cash, although using these cards can sometimes entail fees.1
- Debit cards are payment cards that reduce the need to carry cash or physical checks to make purchases.You can use debit cards at ATMs to withdraw cash.
- Debit card purchases may require a personal identification number (PIN), but some purchases can be made without one.
- You may be charged an ATM transaction fee if you use your debit card to withdraw cash from an ATM that's not affiliated with your bank. Some debit cards offer rewards, similar to credit card rewards, such as 1% back on purchases.

Debit Card

Debit card is also like credit card. It is required to have a bank account before having debit card.

How to Use a Debit Card Online?

If you're paying for something online, you can use your Debit Card. Here is a step-by-step guide to help you complete your payments online using Debit Cards-

•Once you are at the payment checkout, you need to choose “Pay Using Debit/ Credit Card. Once you select on the option, you need to specify the type of card, i.e., Debit Card and whether it is a Visa or Mastercard.

•Then, type the 16-digit Debit Card number which is on the front side of your Debit Card. You will also have to enter the expiration date of the card.

•Once you’ve entered the Debit Card details, you may be asked for a CCD, CVV, or similar security code. In most cases, it is a three or four- digit code that helps prove that you are authorised to use the card. This code is mostly found on the back of the cards.

•Once you are through the payment portal, you will be asked to enter a unique transaction code or an OTP (one-time password) that is sent to the mobile number linked to your Debit Cards. Once you enter the number, your transaction is verified, and you receive a notification.

•To use a Debit Card online, you will need to know the correct billing address which is linked to the card being used.

How a Debit Card Works

- A debit card is a card linked to your checking account. It looks like a credit card, but it works differently. The amount of money you can spend on a debit card is determined by the amount of funds in your account, not by a credit limit such as credit cards carry.
- Your debit card may be connected electronically to your account, or it can be an offline card. Offline cards take longer to process transactions.
- Unlike with a credit card, you don't go into debt when you use a debit card because you are using it to access funds you already have. You don't have to make monthly minimum payments on a debit card because there is no debt to repay.2
- You can use a debit card to get cash from an ATM, or you can make purchases with it like you make purchases with credit cards. With debit cards, you may need to enter your PIN (personal identification number), although many debit cards can be used to make purchases without a PIN.
- Debit cards usually have daily purchase limits, meaning you can't spend more than a certain amount in one 24-hour period.3
- Debit cards draw the funds immediately from the affiliated account. So, your spending is limited to what's available in your checking account, and the exact amount of money you have to spend will fluctuate along with your account balance.

Pros of Debit Cards

- Widely Accepted
- Manage Spending
- Can Be Replaced Easily
- Offer Secure Payment
- Give Access to Cash

Cons of Debit Cards

- Hold Funds
- Spending Limits
- Offer Few, If Any, Rewards

Electronic Fund Transfer (EFT)

- **An electronic funds transfer (EFT) is any transfer by two corresponding banks or financial institutions that is strictly handled by computerized systems.** In other words, this is a broad term for modern transaction methods. As long as it doesn't involve direct human contact and is facilitated through a computer, then it's considered an EFT.
- You can think of it as an umbrella term of sorts, so EFTs can be wire transfers, direct debits, *ACH payments*, and more. EFTs have exploded in popularity following the invention of the internet, eCommerce, and digital cash. Virtually all components of a traditional transaction are being digitized — invoices, receipts, payments, and EFT systems are an essential component of this. So why accept electronic checks, digital debit transactions, etc. if credit cards are so popular these days?
- ***Cost and convenience.***
- EFTs are significantly cheaper than credit cards — averaging at around 1% in fees as opposed to 3% or so for cards. For businesses of all types and sizes, this offers a significant incentive to support and encourage customers to use EFT methods.
- While features and specifics change payment type to payment type, there are some common characteristics across all EFT payment types.

- Funds are typically transferred with 24-48 hours. Fees typically hover around 1%
- EFTs are popular for recurring debits and credits.
- Customers enjoy having the payment flexibility EFTs offer.

Automated Clearing House (ACH)

- **What is ACH?**
- **ACH, or automated clearing house, is like a check without the paper.**
- ACH payments are a *type* of EFT. If EFT stood for electric cars, then ACH would be a Tesla or Nissan Leaf. So ACH can be a type of EFT but EFT can't be a type of ACH.
- It's a computer-based clearing and settlement facility that exchanges funds between two depository institutions. ACH is most commonly used in recurring invoicing (monthly auto-drafts) and direct deposit programs. ACH is cheap to send money with and relatively easy to set up, making it an attractive option for businesses that conduct large, recurring bills (think B2B or consulting fees).

Typical uses of ACH

- Direct deposits: This is the most popular use of ACH payments. By paying employees with ACH employers drastically reduce fees and increase employee satisfaction and convenience.
- Direct debits and credits: There's widespread use of ACH payments in subscription/repeat billing situations. Think automatic drafts via gyms, utilities, insurance, etc. If you work in any sort of SaaS or retainer-based business, you need to support ACH.
- Taxes: ACH is the most common form of tax payment.

Risks in E-Payment

- Disputed Transaction
- Lack of security or trust
- Lack of Account trail
- Lack of anonymity
- Impulse buying
- Payment conflicts
- Frauds - phishing , skimming , impersonating
- Costing
- Technological failure

What are the Benefits of Electronic Payment for the Merchant?

- It saves time
- It's more efficient
- It takes cash out of the equation
- It's more secure
- It generates more revenue
- It's easier to administer
- There's a certainty of payment.

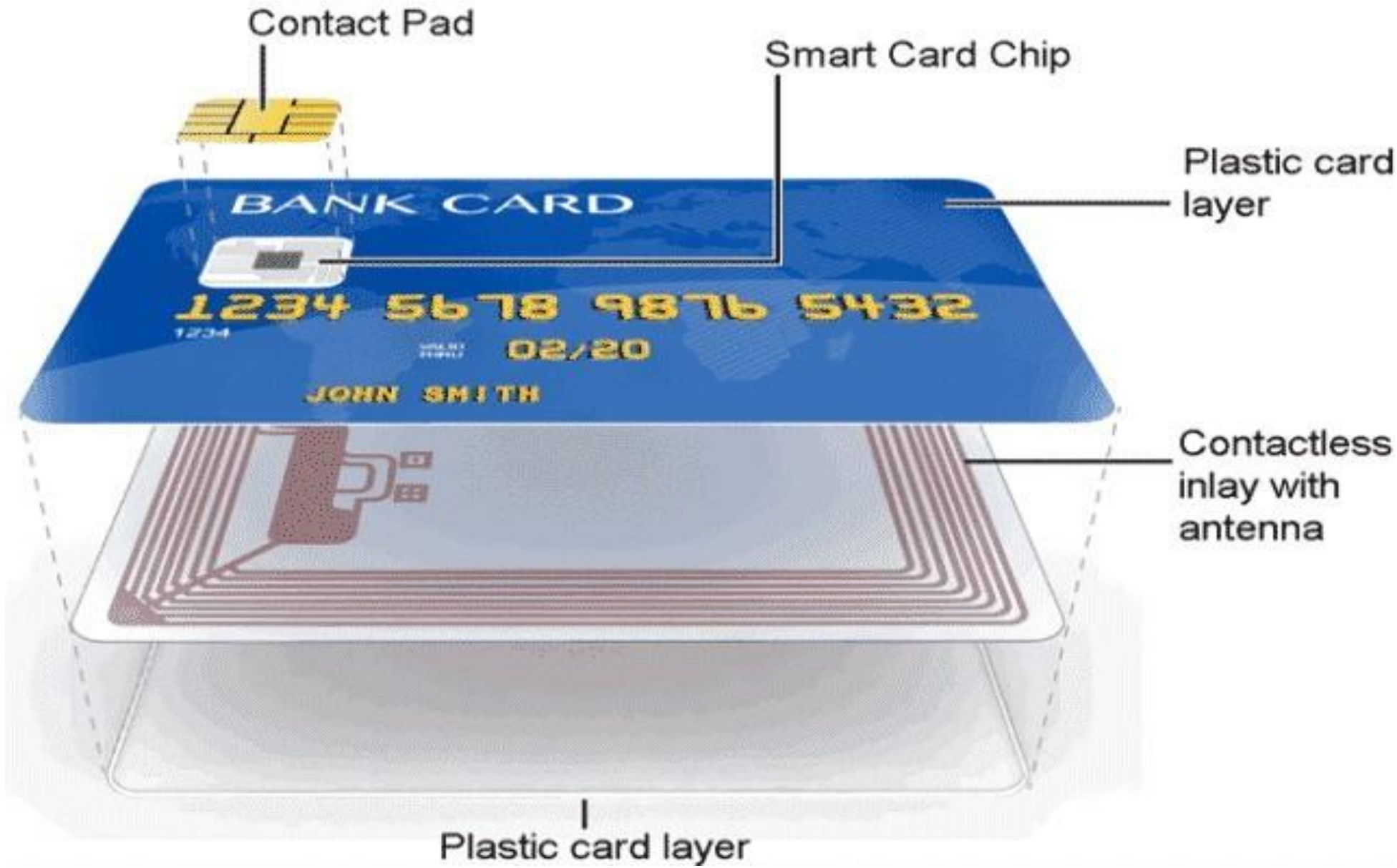
Smart Card

- A smart card is a physical card that has an embedded integrated chip that acts as a security token. Smart cards are typically the same size as a driver's license or credit card and can be made out of metal or plastic.

Secure and reliable Smart Card has played a key role in improving multifaceted digital security. A smart card is capable of storing and processing the data securely in a network of computers. The scope of smart cards is increasing day by day in diverse applications like banking, telephone services, and medical records systems etc. Smart-Card is a secure portable storage device which is used in various applications requiring controlled access to sensitive information. It is in the size of a credit/ debit card, incorporated with one or more integrated circuit chips.

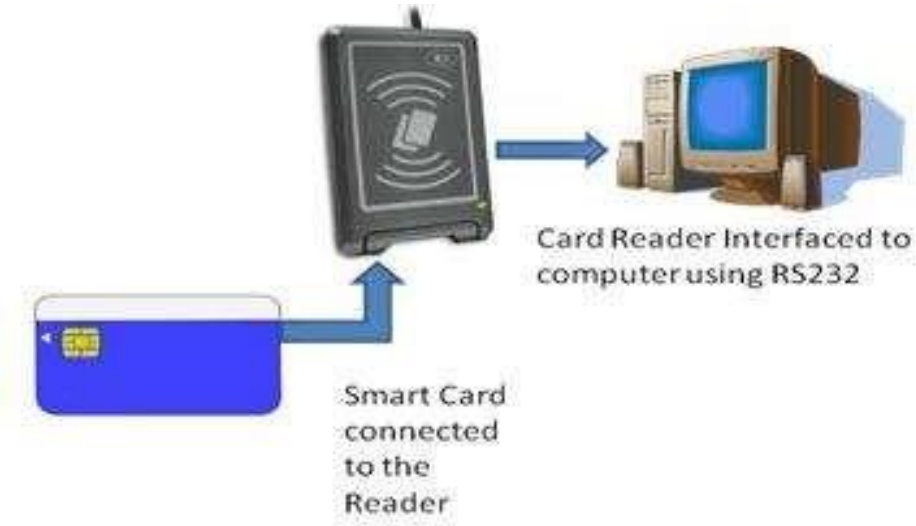
It functions as a microprocessor, memory and provides an input-output interface. The International

Organization for Standardization (ISO) specifies certain voluntary international standards in many scientific and technological fields. However, till to date, ISO has not defined any standards for the devices termed as “Smart Cards.”


Contact Pad
Smart Card Chip
Plastic card layer
BANK CARD
1234 5678 9876 5432
1234
02/20
JOHN SMITH
Contactless inlay with antenna
Plastic card layer

- **How does the Smart Card Works?**
- A smart card is connected to the host computer or controller via a card reader which gets information from the smart card and accordingly passes the information to the host computer or controller.

- **Advantages of Smart Card:**
- Might be promptly reconfigured
- Reusable
- Secure transactions
- Gives more security
- More tough and dependable
- Permit numerous provisions to be saved in one card



Smart Card Based Payment Systems

- Smart Cards are credit card sized plastic cards with the memory chips and in some cases, with microprocessors embedded in them so as to serve as storage devices for much greater information than credit cards with inbuilt transaction processing capability.
  - A single smart card can be used for many different purposes. It is more durable and is less expensive than credit cards.
  - The smart card technology is widely used in countries such as Japan, Germany, Singapore and France to pay for public phone calls, transportation and shopper loyalty programs.
  - Consumers can load money into an account on the card by using an automatic teller machine (ATM) or by placing the card in a slot in a specially equipped computer.
  - The embedded chip keeps track of how much money is added to and withdrawn from the account
  - Smart cards are already quite popular for online sales in some international markets.

Smart Card applications

- Smart cards are used in many applications worldwide, including:
- **Secure identity applications** - employee ID badges, citizen ID documents, electronic passports, driver's licenses, online authentication devices
- **Healthcare applications** - citizen health ID cards, physician ID cards, portable medical records cards
- **Payment applications** - contact and contactless **credit/debit cards**, transit payment cards
- **Telecommunications applications** - GSM Subscriber Identity Modules, pay telephone payment cards

Payment Gateway

- A payment gateway is the service that processes electronic transactions such as credit card transaction.
- When customers buy something from online store, they enter their credit card numbers during the checkout process. E-commerce site sends that credit card information to payment gateway to authorize the transaction and process the payment.
- If the credit card information submitted to the payment gateway matches the information on file with the credit card company and the charge is approved, the payment gateway will then transfer the money from customer's credit card into merchant’s account.

Payment Gateway working mechanism

- A customer places order on website by pressing the "Submit Order” or equivalent button.
- If the order is via a website, the customer's web browser encrypts the information to be sent between their browser and the merchant's web server. This is usually done via SSL (Secure Socket Layer) encryption.
- The merchant then forwards the transaction details through to their payment gateway.
- The payment gateway which receives the transaction information from the merchant forwards it to the merchant's acquiring bank.
- The acquiring bank then forwards the transaction information to the issuing bank for authorization.
- The card issuing bank receives the authorization request and sends a response back to the payment gateway with a response: approved or declined.

Payment Gateway Cont..

Digital Wallet

- Consumers are becoming more enthusiastic about online shopping and they can do shopping repeatedly.
- Entering detailed shipping and payment information each time they make online purchases may be boring for them.
- To address these concerns, many electronic commerce sites include a feature that allows a customer to store name, address, and credit card information.
- An electronic wallet (sometimes called an E-wallet/Digital Wallet), serving a function similar to a physical wallet, holds credit card numbers, electronic cash, owner identification, and owner contact information and provides that information at an electronic commerce site's checkout counter.
- Electronic wallets give consumers the benefit of entering their information just once, instead of having to enter their information at every site with which they want to do business.

Most important functions of a digital wallet

- Authenticate the consumer through the use of digital certificates or other encryption methods.
- Store and transfer value
- Secure the payment process from the consumer to the merchant. Digital wallets would support payments using a regular credit card, digital cash, digital credit card or digital check.

Digital Wallet Cont..

Electronic wallets fall into two categories based on where they are stored:

- **Server- side Electronic Wallet:**

  o A server-side electronic wallet stores a customer's information on a remote server belonging to a particular merchant or wallet publisher.

  o The main weakness of server-side electronic wallets is that a security breach could reveal thousands of users' personal information including credit card numbers.

- **Client-Side Wallet:**

  o A client-side electronic wallet stores a consumer's information on his or her own computer.

  o Many of the early electronic wallets were client-side wallets that required users to download the wallet software.

Digital Wallet

An electronic device or online service that lets us make electronic transactions.

E-WALLET

SHOP ONLINE

Buy things using phone, tablet, or computer.

Stores money, ID, cards, etc.

Purchase history.

Payment options.

Encryption makes it safe.

Language options.

Paytm PayPal amazon payments Google wallet

BENEFITS OFFERED BY DIGITAL WALLETS

Benefits of a Digital Wallet

- Convenience. One of the biggest reasons people use their digital wallet is for the convenience!
- More Secure.
- Allows you to be More Organized
- Use Contactless Payment for a Faster Checkout.
- Get Rewarded for Purchases.

e-Sewa

- e-Sewa is the first online payment gateway of Nepal. It is an associate service of F1Soft International launched on 21 January 2010. Its headquarters is located at Hattisar, Kathmandu, Nepal.
- E-Sewa is a digital wallet. It facilitates its users to pay and get paid online.
- “e” means electronic, Sewa means "Service”: Electronic Service
- Registration and Merchant payment is free of cost, can be accessed using mobile application or web browser.

E-Sewa Cont..

- **Services like funds transfer to banks may incur charges depending on the policies adopted by eSewa.**
- **To register with eSewa, customer needs:**
  - o Citizenship card (scanned or photo copy) and
  - o Passport size photo (scanned copy or original)
- **eSewa is available in two modules: B2B and B2C.**
- **Currently, it provides following online services:**
  - o Sending and Receiving Money
  - o Online Shopping o Payment of Utility Bills
  - o Purchase of Air Tickets and Movie Tickets
  - o Purchase of Recharge Cards and Mobile Top Up
  - o Payment of School and College Bills
  - o Payment of Internet Service Bills
  - o Subscription of Newspapers and Magazines
  - o Payment of Credit Card Bills
  - o Facility of all eSewa services through mobile phone (mSewa)
  - o Withdraw funds from local bank account
  - o Upload funds to local bank

e-Sewa Cont..

- ***eSewa offers various ways to load/prefund your eSewa account:***

  o Internet Banking: You can transfer funds to your eSewa wallet using internet banking of bank that is partner with eSewa. For this, customer will need to have an Internet banking enabled account with one the partner banks.

  o Mobile Banking: If you have mobile banking enabled account with one of the banks then you can prefund your eSewa account using mobile banking.

- For the customers who don't have account in the above banks or the customers without mobile banking & internet banking can load their eSewa account the process of counter deposit

What is Cryptocurrency?

- Cryptocurrency, or Crypto, is a virtual form of currency that secures the financial assets through cryptography.
- It has become famous due to its decentralization feature.
- It doesn’t require a central bank or government for transactions. In a nutshell, cryptocurrency is a decentralized system of peer-to-peer transactions for more transparency and security.
- Cryptocurrencies are not physical; these are digital tokens stored on a blockchain or distributed ledger.
- One of the amazing things about cryptocurrency is that It’s exchangeable. Its value remains that same when you buy or trade them.
- Furthermore, this blockchain process allows the fast transfer of money without collapsing at any point.
- As the word Crypto refers to the encryption algorithm, so it offers various security functions, such as hashing, public-private key pairs, and elliptical curve encryption.

How Does Cryptocurrency Work?

- Blockchain technology is the secret sauce underlying cryptocurrency.
- It is a decentralized digital ledger for storing the public record of all transactions involving a specific cryptocurrency.
- Each transaction is linked to the previous one as a block, and in this way, it becomes a secure chain.
- Due to this well-organized distributed structure, cryptocurrencies are difficult to change or counterfeit.
- **Initiation:**
- The first step is the initiation of the cryptocurrency. Cryptocurrency transactions are initiated when a user sends or receives digital coins. Each transaction is encrypted and safe.
- **Broadcasting:**
- Once the transaction is initiated, it broadcast to a network of nodes. Nodes are computers that are part of the cryptocurrency network. The network ensures that the transaction is visible to all nodes in the network, maintaining the blockchain in this way.
- **Verification:**
- The nodes in the network ensure that the sender has sufficient funds to complete the transaction. This is done through complex cryptographic algorithms.
- **Validation:**
- After this, the transaction and other transactions are added in blockchain. This block is then added to the blockchain, a distributed ledger that records all transactions in a securely and transparently.
- **Update:**
- The blockchain is continuously updated as new blocks are added to it. This ensures that the transaction history is secure and cannot be changed. This initiation, broadcasting, verification, validation, and updating process makes cryptocurrency work effectively as a digital currency.

Types of Cryptocurrencies:

Various types of cryptocurrencies are available in the market, each with unique features.

- **Bitcoin**
- Bitcoin is the first and most popular cryptocurrency that is widely accepted by everyone. It is used as the medium of exchange for online transactions. It has limited supply and volatile price movement.
- **Ethereum**
- It has gained popularity due to its smart contract functionality and self-executing agreements. It facilitates decentralized applications.
- **Litecoin**
- This currency is called the silver to Bitcoin's gold. It is the lighter version of cryptocurrency. Litecoin allows faster transactions with lower fees. It is also widely accepted by merchants for payments.
- **Ripple**
- Ripple is a digital payment protocol in banks and financial institutions use for cross-border transactions. This quality makes it a popular choice for international money transfers. Investors should carefully research and understand the different options.

Cryptocurrency Cont..

Benefits of Cryptocurrency:

- **Decentralization:**
- Cryptocurrency offers users with a lot of benefits. It is decentralized in nature and doesn't have a controlling authority. The introduction of cryptocurrency has eliminated the need for intermediaries such as banks and government institutions.
- **Security:**
- Cryptocurrency transactions are secured by cryptography, making them highly secure and private. This reduces the risk of fraud, identity theft, and other forms of cyberattacks common with traditional payment methods.
- **Transparency:**
- All transactions made with cryptocurrency are recorded on a blockchain, which provides transparency and accountability. Anyone can trace and verify its transaction.
- **Fast and Low-Cost Transactions:**
- Cryptocurrency transactions are typically processed faster and at a lower cost, which is much better than traditional financial transactions. This is especially beneficial for cross-border payments, as transaction fees and processing times can be significantly reduced by using it.
- **Borderless:**
- Cryptocurrency can be transferred and used anywhere in the world. It doesn't need to be subjected to exchange rates or other restrictions. It allows for faster and more efficient cross-border payments.

Cryptocurrency Cont..

Drawbacks of Cryptocurrency:

- **Volatility:**
- One of the biggest drawbacks of cryptocurrency is its extreme volatility. The value of digital currencies can fluctuate wildly in a short period, making them a risky investment for many. This volatility can lead to significant losses for investors unprepared for sudden price changes.
- **Regulation:**
- There is lack of regulation in cryptocurrencies. Their decentralized nature of digital currencies makes it difficult for governments to control or monitor transactions. It may become a threat to illegal activities.
- **Security Threats:**
- Cryptocurrency transactions are not completely secure and are susceptible to hacking and fraud. Many exchanges and wallets have been targeted by cybercriminals, resulting in the loss of millions of dollars worth of digital assets.
- **Limited Adoption:**
- Although these currencies are getting popularity but still they are not widely accepted. Due to this, transaction of the currencies has become tough for the users.
- **Environmental Impact:**
- Mining cryptocurrency requires a great amount of energy that may rise question about environmental impacts. The massive amount of electricity needed to power mining operations. It impacts the sustainability of the cryptocurrency.

Electronic Billing Presentment and Payment (EBPP) System

- **What Is Electronic Bill Payment and Presentment?**
- Electronic bill payment and presentment (EBPP) is a process that companies use to collect payments electronically through systems like the Internet, direct-dial access, and Automated Teller Machines (ATMs).
- It has become a core component of online banking at many financial institutions today. Other industries—including insurance providers, telecommunications companies, and utilities—depend on EBPP services as well.
- **Understanding EBPP**
- EBPPs come in two types: biller-direct and bank-aggregator. Biller-direct is electronic billing, which is offered by the company providing the good or service.
- The company gives customers the option to pay bills directly on their web site and might alert them when a payment is due via email.
- The customer then logs into the site via a secure connection, reviews the billing information, and enters payment amount.

Electronic Billing Presentment and Payment (EBPP) System Cont..

- The bank-aggregator or bill-consolidator model allows customers to pay bills to many different companies through one portal.
- That is, the service collects different payments from customers and distributes each payment to the appropriate company.
- A bank, for instance, might offer online users the option to make many different payments like credit cards, utility bills, and insurance premiums. Standalone sites also exist that allow people to view and pay all of their bills.
- These are called consumer consolidator models.
- Some newer EBPP products include features like secure email delivery, stored payment data, and autopay.
- For example, a healthcare insurance company looking to streamline its customer billing system may decide to switch to EBPP and allow customers to pay directly on their website or to have premiums automatically deducted each month.
- Doing so saves customers the hassle of filing paperwork and can save the organization on document delivery and processing costs.

Online Banking facilities in Banks of Nepal:

- What is Internet Banking/e-Banking/Online Banking/Virtual Banking?
- Internet banking/e-banking is an electronic payment system that enables customers of a bank or financial institution to conduct a range of financial transactions through the financial institution's website.
- Using internet banking, we can obtain our account balances, a list of recent transactions, various utility bill payments, and funds transfers between accounts.
- We can access all these facilities from anywhere and anytime using mobile or computer.
- It's less time consuming, and very safe and secure.
- Nowadays, mobile banking is also gaining popularity but it shouldn't be mistaken with internet banking.
- In mobile banking, we use our smartphone's application or internet but the two have significant differences. Both are the modes of e-Banking.

Online Banking facilities in Banks of Nepal:

- **E-banking services includes: -**
- ATMs o Cash Withdrawal

o Balance Inquiry o Fund Transfer is not available.

- **PoS Terminals o Financial transactions are made via Cards.**

o Cash is debited from the client's account(s).

o Cash cannot be deposited.

- **Tele-Banking**

o Account Status check

o Balance Inquiry

o No fund transfer facility.

- **SMS-Banking (Mobile Banking)**

o Similar to Tele-Banking except telephone

o Cell phone is required instead of telephone.

- **Online Banking / Internet Banking**

o Viewing account balances, recent transactions

o Bank statements o Funds transfers between the customer's linked accounts

o Paying third parties, including bill payments and third-party fund transfers

o Many more including non-transactional tasks and transact banking tasks

History of Online Banking in Nepal:

- Establishment of first Joint Venture Bank, Nepal Arab Bank Limited (now NABIL Bank), in 1984 was the first step towards e-banking in Nepal. It introduced Credit Cards in Nepal in early 1990.
- Automated Teller Machine (ATM) was first introduced by another Joint Venture Bank, Himalayan Bank Ltd. in 1995. Himalayan Bank Limited was also the first bank to introduce Tele-Banking (Telephone Banking) in Nepal.
- Internet-Banking was first introduced by Kumari Bank Limited in 2002.
- Laxmi Bank Limited was the first bank to introduce SMS-Banking (or Mobile Banking) in Nepal in the year 2004.
- The channels in e-Banking available in Nepal are Automated Teller Machines (ATM), Point of Sales (PoS), Telephone Banking (Tele Banking), Internet Banking, Mobile Banking (SMS Banking).

Services of Online Banking in Nepal

- ***Some of the services accessible through Internet banking in Nepal are:***
- Online tax payment
- Access the account to check balance,
- Online trading of shares,
- Online remittance of money,
- Electronic bill payment system,
- Check the account statement online.
- Open a fixed deposit account.
- Pay utility bills such as water bill and electricity bill.
- Make merchant payments.
- Transfer funds.
- Order for a cheque book.
- Buy general insurance.
- Recharge prepaid mobile
- Transfer of funds from one customer's account to other, etc.

Important Security Tips to Use Online Banking Safely:

- Access your bank's website/web portal/application only by typing the URL in the address bar of your browser
- Clicking on any links from email or SMS to access the bank's site may lead to a breach of your personal information.
- No banks will send you an SMS/email or call you over the phone to provide your personal information or OTP. So, make sure to avoid such scams.
- To improve your security, update your operating system, mobile application, and use the latest version of your browser.
- Also, make sure to scan your computer regularly with antivirus and ensure that the firewall is enabled.
- If possible, change your Internet Banking password at a regular interval.
- Monitor your transactions and activity log.
- Avoid accessing your online banking services from shared PCs, cyber cafes, or untrusted devices.

What is HTTPS?

- Hypertext transfer protocol secure (HTTPS) is the secure version of HTTP, which is the primary protocol used to send data between a web browser and a website.
- HTTPS is encrypted in order to increase security of data transfer.
- This is particularly important when users transmit sensitive data, such as by logging into a bank account, email service, or health insurance provider.
- Any website, especially those that require login credentials, should use HTTPS.
- In modern web browsers such as Chrome, websites that do not use HTTPS are marked differently than those that are.
- Look for a padlock in the URL bar to signify the webpage is secure.
- Web browsers take HTTPS seriously; Google Chrome and other browsers flag all non-HTTPS websites as not secure.

How does HTTPS work?

- HTTPS uses an encryption protocol to encrypt communications. The protocol is called Transport Layer Security (TLS), although formerly it was known as Secure Sockets Layer (SSL). This protocol secures communications by using what's known as an asymmetric public key infrastructure.
- This type of security system uses two different keys to encrypt communications between two parties:
- **The private key** - this key is controlled by the owner of a website and it's kept, as the reader may have speculated, private. This key lives on a web server and is used to decrypt information encrypted by the public key.
- **The public key** - this key is available to everyone who wants to interact with the server in a way that's secure. Information that's encrypted by the public key can only be decrypted by the private key.

Secure Socket Layer (SSL)

- **Secure Socket Layer (SSL)** provides security to the data that is transferred between web browser and server.
- SSL encrypts the link between a web server and a browser which ensures that all data passed between them remain private and free from attack.
- Secure sockets layer (SSL) is a networking protocol designed for securing connections between web clients and web servers over an insecure network, such as the internet.

Why is SSL Important?

- Originally, data on the web was transmitted in plaintext, making it easy for anyone who intercepted the message to read it.
- For example, if someone logged into their email account, their username and password would travel across the Internet unprotected.
- SSL was created to solve this problem and protect user privacy.
- By encrypting data between a user and a web server, SSL ensures that anyone who intercepts the data sees only a scrambled mess of characters.
- This keeps the user's login credentials safe, visible only to the email service.
- Additionally, SSL helps prevent cyber attacks by:
- **Authenticating Web Servers**: Ensuring that users are connecting to the legitimate website, not a fake one set up by attackers.
- **Preventing Data Tampering**: Acting like a tamper-proof seal, SSL ensures that the data sent and received hasn't been altered during transit

How does SSL work?

- **Encryption**: SSL encrypts data transmitted over the web, ensuring privacy. If someone intercepts the data, they will see only a jumble of characters that is nearly impossible to decode.
- **Authentication**: SSL starts an authentication process called a handshake between two devices to confirm their identities, making sure both parties are who they claim to be.
- **Data Integrity**: SSL digitally signs data to ensure it hasn't been tampered with, verifying that the data received is exactly what was sent by the sender.

What Is SSL and How Does It Work?

- **Secure Sockets Layer** (SSL) is a security protocol that creates an encrypted connection between a web server and a browser.
- It provides a secure connection and prevents third parties from accessing or modifying information transferred.
- To get an SSL certificate, website owners must buy it from a **Certificate Authority** (CA).
- The CA will use the CSR or **Certificate Signing Request** to create the certificate.
- The CSR is an encrypted text generated on the server where the certificate will be installed. It includes information such as the website's domain name, contact details, and the public key to encrypt the data sent.
- When the visitor's browser tries to access the website, the web server will send a copy of the certificate for verification.
- If the process is successful, an SSL-secured connection will be established. The website will use an URL that starts with HTTPS and, depending on the browser, a padlock icon will be displayed in the address bar.

HOSTINGER

Three. Two. Online

How Do SSL Certificates Work?

1. A webmaster purchases an SSL certificate from a Certificate Authority

2. The browser will request the web server to send its SSL certificate and public key for verification.*

3. The browser will generate two symmetric keys to encrypt the connection (one for itself and the other for the web server).**

4. After receiving the encrypted symmetric key, the server will use its private key to decrypt it.

5. The padlock and https:// will appear on the address bar and all content between web server and browser will be encrypted then decrypted with the symmetric key.

*Most web browsers come with built-in public keys from various Certificate Authorities, so they're able to check their validity.

**The browser delivers the symmetric key to the server using its public key to keep it secured.

Why Do I Need an SSL Certificate?

Improve Security

- There are many ways to **make your site secure**. Adding an SSL certificate provides an extra and crucial layer of protection against malicious attacks.
- Even if the website doesn't accept transactions, you still need to protect users' login details, addresses, and other personal information.
- Websites without SSL certificates use HTTP, a text-based protocol, meaning it's easier to intercept and read its traffic. HTTPS uses cryptographic keys to encrypt data, providing more complex security and making it difficult for potential attackers to intercept the data exchange.
- Thus, the HTTPS protocol protects your website against digital threats such as man-in-the-middle (MITM) attacks. These attacks take place when someone intercepts the traffic between the website's server or the client's browser.
- Attackers may either steal information exchanged or redirect traffic to a phishing website, where they ask for login credentials or other sensitive data.
- Even if an attacker intercepts your connection, having an SSL certificate ensures that they cannot decrypt the information passed.

Establish Trust

- Establishing trust with your customers is essential. Particularly in the case of online businesses, your customers need concrete proof that it's safe to provide their data. Research shows that **17% of shoppers abandon their carts** because they don't trust the website enough to enter their credit card details.
- An SSL certificate communicates to visitors that they can safely exchange information with the website, encouraging them to use your service and keeping you ahead of competitors who don't have one.
- Furthermore, it helps visitors verify ownership of the website before signing in or providing other sensitive information.

Strengthen SEO

- Another advantage of **installing an SSL certificate** is boosting your **SEO** strategy. **Google** and other search engines have made website security an important factor when determining page rankings.
- Since they aim to provide users with a safe web browsing experience, **Google Chrome** and other web browsers display a **"Not Secure" warning message** on all non-SSL websites to alert visitors.
- Having an SSL certificate gives you an advantage over competitors who do not have one, improving your site's position on search engine results pages (SERPs).

Salient Features of Secure Socket Layer

- The advantage of this approach is that the service can be tailored to the specific needs of the given application.
- Secure Socket Layer was originated by Netscape.
- SSL is designed to make use of TCP to provide reliable end-to-end secure service.
- This is a two-layered protocol.

SSL Certificate

- SSL (Secure Sockets Layer) certificate is a digital certificate used to secure and verify the identity of a website or an online service.
- The certificate is issued by a trusted third-party called a Certificate Authority (CA), who verifies the identity of the website or service before issuing the certificate.
- The SSL certificate has several important characteristics that make it a reliable solution for securing online transactions:
- **Encryption**: The SSL certificate uses encryption algorithms to secure the communication between the website or service and its users. This ensures that the sensitive information, such as login credentials and credit card information, is protected from being intercepted and read by unauthorized parties.
- **Authentication**: The SSL certificate verifies the identity of the website or service, ensuring that users are communicating with the intended party and not with an impostor. This provides assurance to users that their information is being transmitted to a trusted entity.
- **Integrity**: The SSL certificate uses message authentication codes (MACs) to detect any tampering with the data during transmission. This ensures that the data being transmitted is not modified in any way, preserving its integrity.
- **Non-repudiation**: SSL certificates provide non-repudiation of data, meaning that the recipient of the data cannot deny having received it. This is important in situations where the authenticity of the information needs to be established, such as in e-commerce transactions.
- **Public-key cryptography:** SSL certificates use public-key cryptography for secure key exchange between the client and server. This allows the client and server to securely exchange encryption keys, ensuring that the encrypted information can only be decrypted by the intended recipient.
- **Session management**: SSL certificates allow for the management of secure sessions, allowing for the resumption of secure sessions after interruption. This helps to reduce the overhead of establishing a new secure connection each time a user accesses a website or service.
- **Certificates issued by trusted CAs**: SSL certificates are issued by trusted CAs, who are responsible for verifying the identity of the website or service before issuing the certificate. This provides a high level of trust and assurance to users that the website or service they are communicating with is authentic and trustworthy.

Advantages of SSL

- Security
- Authentication
- Reliability
- Prevent Phishing
- Online Payments
- Software Requirements
- SEO

Transport Layer Securities (TLS)

- Transport Layer Securities (TLS) are designed to provide security at the transport layer. TLS was derived from a security protocol called Secure Socket Layer (SSL).
- TLS ensures that **no third party may eavesdrop or tampers with any message**.
- **There are several benefits of TLS:**
  Encryption:
  TLS/SSL can help to secure transmitted data using encryption.
- **Interoperability:**
  TLS/SSL works with most web browsers, including Microsoft Internet Explorer and on most operating systems and web servers.
- **Algorithm flexibility:**
  TLS/SSL provides operations for authentication mechanism, encryption algorithms and hashing algorithm that are used during the secure session.
- **Ease of Deployment:**
  Many applications TLS/SSL temporarily on a windows server 2003 operating systems.
- **Ease of Use:**
  Because we implement TLS/SSL beneath the application layer, most of its operations are completely invisible to client.

Working of TLS

- The client connect to server (using TCP), the client will be something. The client sends number of specification:
- Version of SSL/TLS.
- which cipher suites, compression method it wants to use.

- The server checks what the highest SSL/TLS version is that is supported by them both, picks a cipher suite from one of the clients option (if it supports one) and optionally picks a compression method.
- After this the basic setup is done, the server provides its certificate.
- This certificate must be trusted either by the client itself or a party that the client trusts.
- Having verified the certificate and being certain this server really is who he claims to be (and not a man in the middle), a key is exchanged.
- This can be a public key, “PreMasterSecret” or simply nothing depending upon cipher suite.
- Both the server and client can now compute the key for symmetric encryption.
- The handshake is finished and the two hosts can communicate securely.
- To close a connection by finishing. TCP connection both sides will know the connection was improperly terminated. The connection cannot be compromised by this through, merely interrupted.

TLS Cont..

- Transport Layer Security (TLS) continues to play a critical role in securing data transmission over networks, especially on the internet. Let's delve deeper into its workings and significance:
- **Enhanced Security Features:**
- TLS employs a variety of cryptographic algorithms to provide a secure communication channel. This includes symmetric encryption algorithms like AES (Advanced Encryption Standard) and asymmetric algorithms like RSA and Diffie-Hellman key exchange. Additionally, TLS supports various hash functions for message integrity, such as SHA-256, ensuring that data remains confidential and unaltered during transit.
- **Certificate-Based Authentication:**
- One of the key components of TLS is its certificate-based authentication mechanism. When a client connects to a server, the server presents its digital certificate, which includes its public key and other identifying information. The client verifies the authenticity of the certificate using trusted root certificates stored locally or provided by a trusted authority, thereby establishing the server's identity.
- **Forward Secrecy:**
- TLS supports forward secrecy, a crucial security feature that ensures that even if an attacker compromises the server's private key in the future, they cannot decrypt past communications. This is achieved by generating ephemeral session keys for each session, which are not stored and thus cannot be compromised retroactively.
- **TLS Handshake Protocol**:
- The TLS handshake protocol is a crucial phase in establishing a secure connection between the client and the server. It involves multiple steps, including negotiating the TLS version, cipher suite, and exchanging cryptographic parameters. The handshake concludes with the exchange of key material used to derive session keys for encrypting and decrypting data.

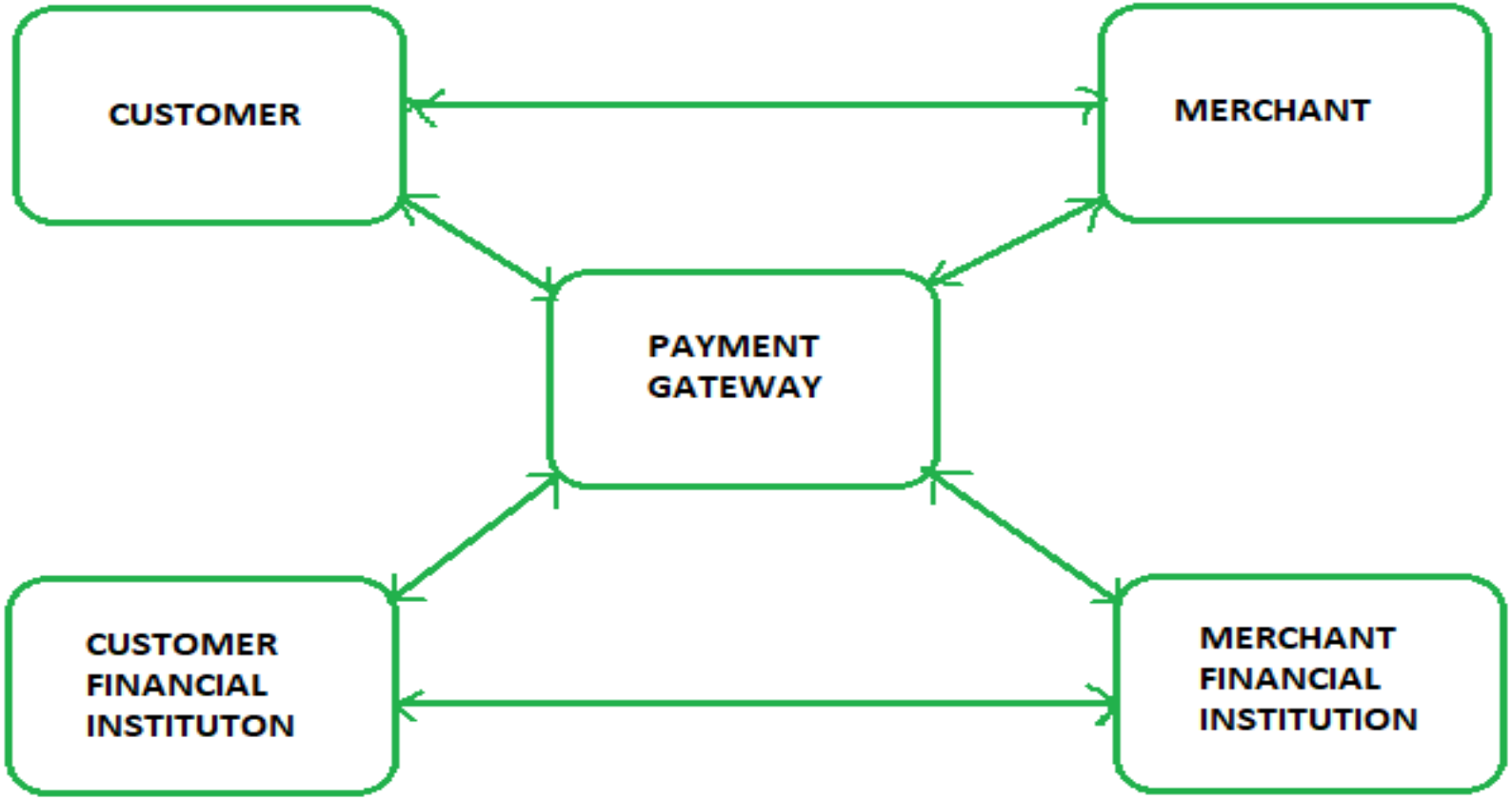
TLS Cont..

- **Perfect Forward Secrecy (PFS):**
- Perfect Forward Secrecy is an advanced feature supported by TLS that ensures the confidentiality of past sessions even if the long-term secret keys are compromised. With PFS, each session key is derived independently, providing an additional layer of security against potential key compromise.
- **TLS Deployment Best Practices**:
- To ensure the effectiveness of TLS, it's essential to follow best practices in its deployment. This includes regularly updating TLS configurations to support the latest cryptographic standards and protocols, disabling deprecated algorithms and cipher suites, and keeping certificates up-to-date with strong key lengths.
- **Continual Evolution:**
- TLS standards continue to evolve to address emerging security threats and vulnerabilities. Ongoing efforts by standards bodies, such as the Internet Engineering Task Force (IETF), ensure that TLS remains robust and resilient against evolving attack vectors.
- Conclusion:
- In an increasingly interconnected world where data privacy and security are paramount, Transport Layer Security (TLS) serves as a foundational technology for securing communication over networks. By providing encryption, authentication, and integrity protection, TLS enables secure data transmission, safeguarding sensitive information from unauthorized access and tampering. As cyber threats evolve, TLS will continue to evolve, adapting to new challenges and reinforcing the security posture of digital communications.

Secure Electronic Transaction (SET)

- Secure Electronic Transaction (SET) is a system and electronic protocol to ensure the integrity and security of transactions conducted over the internet.
- E-commerce websites implemented this early protocol to secure electronic payments made via debit and credit cards.
- **Secure Electronic Transaction** or SET is a security protocol designed to ensure the security and integrity of electronic transactions conducted using credit cards. Unlike a payment system, SET operates as a security protocol applied to those payments.
- It uses 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).
- SET protocol restricts the revealing of credit card details to merchants thus keeping hackers and thieves at bay.
- The SET protocol includes Certification Authorities for making use of standard Digital Certificates like X.509 Certificate.
- Before discussing SET further, let's see a general scenario of electronic transactions, which includes client, payment gateway, client financial institution, merchant, and merchant financial institution.

Secure Electronic Transaction (SET) Cont..



Secure Electronic Transaction (SET) Cont..

- **Requirements in SET:** The SET protocol has some requirements to meet, some of the important requirements are:
- It has to provide mutual authentication i.e., customer (or cardholder) authentication by confirming if the customer is an intended user or not, and merchant authentication.
- It has to keep the PI (Payment Information) and OI (Order Information) confidential by appropriate encryptions.
- It has to be resistive against message modifications i.e., no changes should be allowed in the content being transmitted.
- SET also needs to provide interoperability and make use of the best security mechanisms.

Secure Electronic Transaction (SET) Cont..

- **Participants in SET:** In the general scenario of online transactions, SET includes similar participants:
- **Cardholder –** customer
- **Issuer –** customer financial institution
- **Merchant**
- **Acquirer –** Merchant financial
- **Certificate authority –** Authority that follows certain standards and issues certificates(like X.509V3) to all other participants.

Secure Electronic Transaction (SET) Cont..

- **SET functionalities:**
- **Provide Authentication**
  - **Merchant Authentication** – To prevent theft, SET allows customers to check previous relationships between merchants and financial institutions. Standard X.509V3 certificates are used for this verification.
  - **Customer / Cardholder Authentication** – SET checks if the use of a credit card is done by an authorized user or not using X.509V3 certificates.
- **Provide Message Confidentiality**: Confidentiality refers to preventing unintended people from reading the message being transferred. SET implements confidentiality by using encryption techniques. Traditionally DES is used for encryption purposes.
- **Provide Message Integrity**: SET doesn't allow message modification with the help of signatures. Messages are protected against unauthorized modification using RSA digital signatures with SHA-1 and some using HMAC with SHA-1,

Secure Electronic Transmission (SET) Cont..

- The Secure Electronic Transmission (SET) protocol imitates the current structure of the credit card processing system.
- Secure Electronic Transaction is a communications protocol standard for securing credit card transactions over networks, specifically, the Internet.
- The most important property of SET is that the credit card number is not open to the seller.
- On the other hand, the SET protocol, despite strong support from Visa and MasterCard, has not appeared as a leading standard.
- The two major reasons for lack of widespread acceptance are followings:

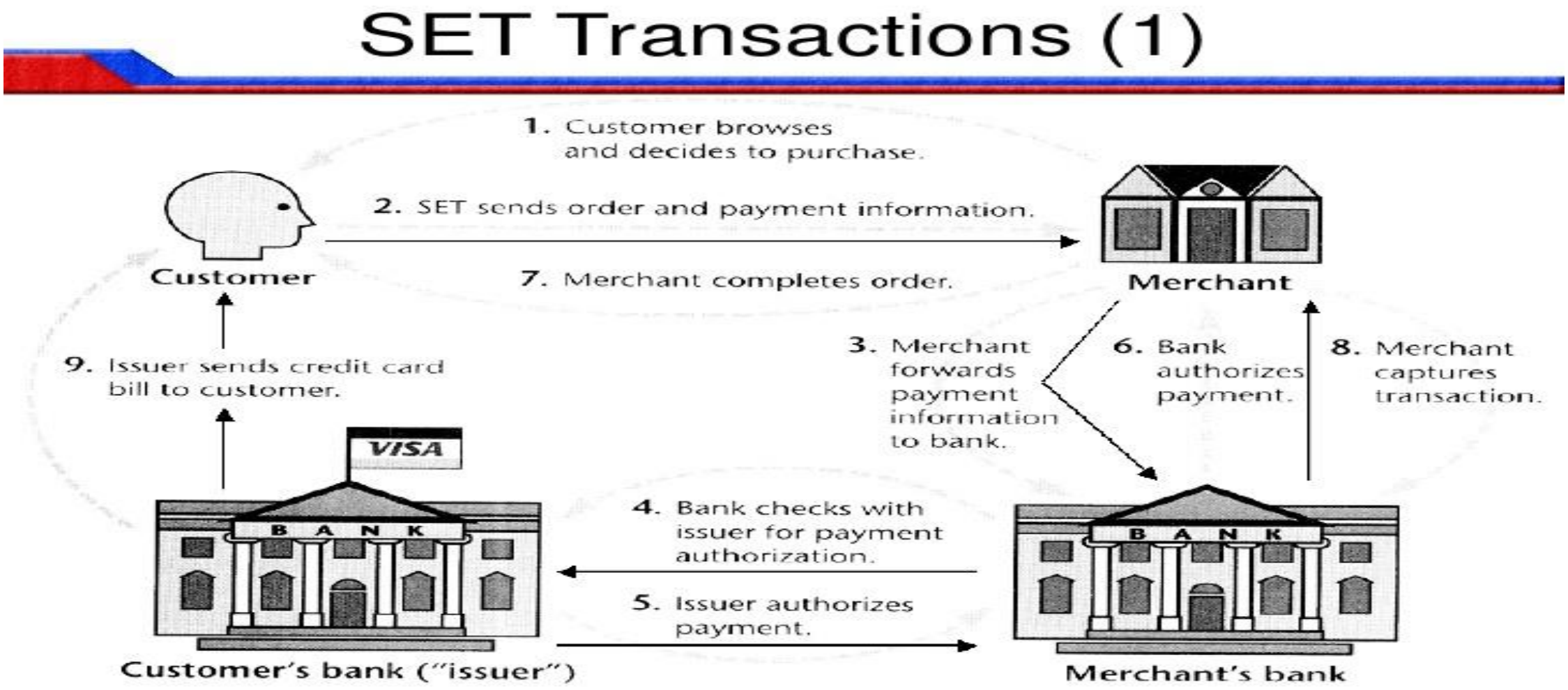
  (1) **The complexity of SET**

  (2) The need for the added security that SET provides.
- *Though, this might change in the future as encryption technology becomes more commonly utilized in the e-business world.*

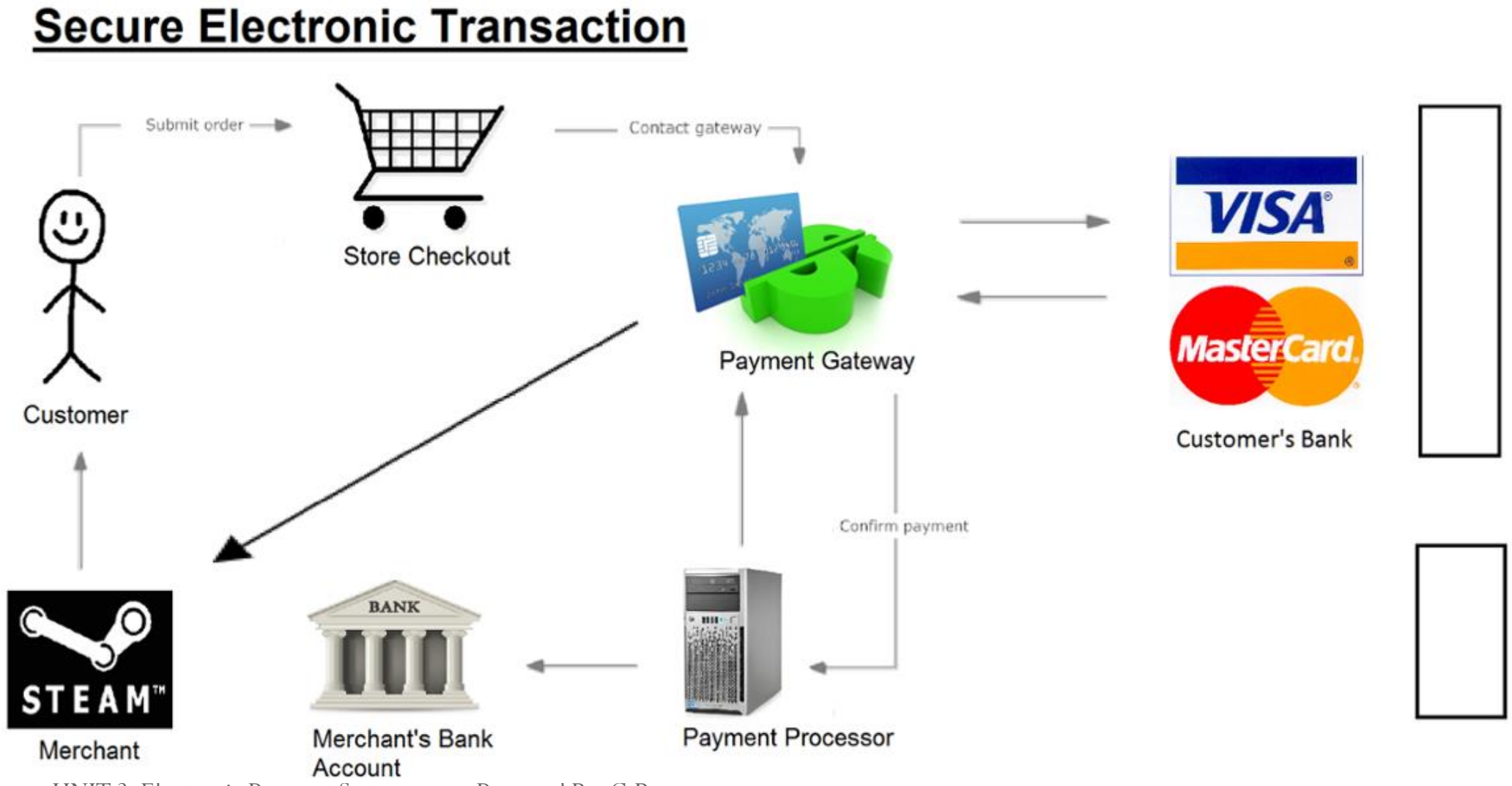
Security architecture of Secure Electronic Transaction

- ***The SET architecture (designed to support PKI) comprises***:
- **Digital certificates**
- Digital signatures authenticate the merchant's and customer's identities to mitigate the risk of a malicious third party manipulating transaction information. The Certificate Authority (CA) issues digital certificates to the issuing bank. The card issuer and acquirer, which may be a bank or other financial institution, both play an important role in issuing digital certificates.
- **Dual signatures**
- In the SET scheme, the customer's order information and payment information are encrypted with separate public keys. The order information is encrypted with the merchant's public keys, and the payment information is encrypted with the acquiring bank's public keys.
- This system ensures that the encrypted PI can only be decrypted by the acquiring bank, and the encrypted OI can only be decrypted by the merchant.

Secure Electronic Transmission (SET) Cont..



Secure Electronic Transmission (SET) Cont..



Secure Electronic Transaction participants

- ***A number of participants are involved in the SET process***:
- **Cardholder/customer**: The authorized holder of the payment card (Visa or Mastercard)
- **E-commerce merchant**: The seller
- **Card issuer**: A financial organization (e.g., bank) that issues the payment card
- **Acquirer**: A financial organization that processes payment authorization and facilitates electronic funds transfer to the merchant's account
- **Payment gateway**: Interface between card payment networks and secure electronic transactions
- **Certificate Authority**: Trusted organization that provides public key digital certificates

SET Cont..

- **Advantages of SET:**
- Information security
- Credit card security
- Flexibility in shopping
- **Disadvantages of SET:** *Some of the disadvantages of SET include its* ***complexity and high cost for implementation.***

Status of E-Payment Systems in Nepal,

- **What are the challenges of e-payment system in Nepal?**
- Nepal's payment service providers are grappling with a shortage of adequate policies, insufficient physical infrastructure, subpar corporate governance, and a lack of proper strategy for sustained business operations during times of crisis, a report by the central bank says
- **What are the different electronic payment systems in Nepal?**
- There are several digital payment providers in Nepal like Fone Pay, eSewa, Khalti, Prabhu Pay, and IME Pay, SmartQR, which enabled a wide range of services like mobile banking, digital wallet, and UPI-based transactions. Also, Banks and Financial Institution have their own digital payment platform.

Advantages of Online Payments

- 1. Speed of transactions
- 2. Convenience
- 3. Reaching global audience
- 4. Low transaction costs
- 5. Quick and easy setup
- 6. Variety of payment choices
- 7. Availability of more distribution channels
- 8. Easy management
- 9. Better customer experience
- 10. Recurring payment capabilities

Disadvantages of Online Payments

- 1. Technical problems
- 2. Password threats
- 3. Cost of fraud
- 4. Security Concerns
- 5. Technological illiteracy
- 6. Limitations on amount and time
- 7.Service fees and other additional costs
- 8. Disputed transactions
- 9. Loss of smart cards
- 10. False identity

Why is digital payment system important in Nepal?

- The use of mobile wallets and digital payment systems for remittance transactions is having a positive impact on the economy of Nepal.
- This is because remittances can help to boost economic growth, reduce poverty, and improve financial inclusion.

Case Studies of Global and Local Payment Systems

- Global Payments is staying competitive in the rapidly changing technology solutions industry by driving innovation and collaboration with Google Workspace apps and tools such as Google App Maker.


Thank you!