E-Payment Mechanism

E-Payment System:

Electronic payment systems are central to on-line business process as companies look for ways to serve customers faster and at lower cost. Emerging innovations in the payment for goods and services in electronic commerce promise to offer a wide range of new business opportunities.

Electronic payment systems and e-commerce are highly linked given that on-line consumers must pay for products and services. Clearly, payment is an integral part of the mercantile process and prompt payment is crucial. If the claims and debits of the various participants (consumers, companies and banks) are not balanced because of payment delay, then the entire business chain is disrupted. Hence an important aspect of e-commerce is prompt and secure payment, clearing, and settlement of credit or debit claims.

Electronic payment systems are becoming central to on-line business transactions nowadays as companies look for various methods to serve customers faster and more cost effectively. Electronic commerce brings a wide range of new worldwide business opportunities. There is no doubt that electronic payment systems are becoming more and more common and will play an important role in the business world. 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).

Types of Electronic Payment Systems:

Electronic payment systems are proliferating in banking, retail, health care, on-line markets, and even government—in fact, anywhere money needs to change hands.

- Organizations are motivated by the need to deliver products and services more cost effectively and to provide a higher quality of service to customers.
- The emerging electronic payment technology labeled electronic funds transfer (EFT).

- EFT is defined as "any transfer of funds initiated through an electronic terminal telephonic instrument, or computer or magnetic tape so as to order, instruct, or authorize a financial institution.

EFT can be segmented into three broad categories:

- **Banking and financial payments**
  - Large-scale or wholesale payments (e.g., bank-to-bank transfer)
  - Small-scale or retail payments (e.g., automated teller machines
  - Home banking (e.g., bill payment)
- **Retailing payments**
  - Credit Cards (e.g., VISA or MasterCard)
  - Private label credit/debit cards (e.g., J.C. Penney Card)
  - Charge Cards (e.g., American Express)
- **On-line electronic commerce payments**
  - **Token-based payment systems**
    - Electronic cash (e.g., DigiCash)
    - Electronic checks (e.g., NetCheque)
    - Smart cards or debit cards (e.g., Mondex Electronic Currency Card)
  - **Credit card-based payments systems**
    - Encrypted Credit Cards (e.g., World Wide Web form-based encryption)
    - Third-party authorization numbers (e.g., First Virtual)

E-Cash:

- There are many ways that exist for implementing an e-cash system, all must incorporate a few common features.
- Electronic Cash is based on cryptographic systems called "digital signatures".
- This method involves a pair of numeric keys: one for locking (encoding) and the other for unlocking (decoding).

E-cash must have the following four properties.

- Monetary value
- Interoperability
- Retrievability
- Security

• Electronic cash is a general term that describes the attempts of several companies to create value storage and exchange system that operates online in much the same way that government-issued currency operates in the physical world.

• Concerns about electronic payment methods include:

– Privacy

– Security

– Independence

– Portability

Electronic Cash Storage:

• Two methods

– **On-line**

• Individual does not have possession personally of electronic cash

• Trusted third party, e.g. e-banking, bank holds customers' cash accounts

– **Off-line**

• Customer holds cash on smart card or electronic wallet

• Fraud and double spending require tamper-proof encryption

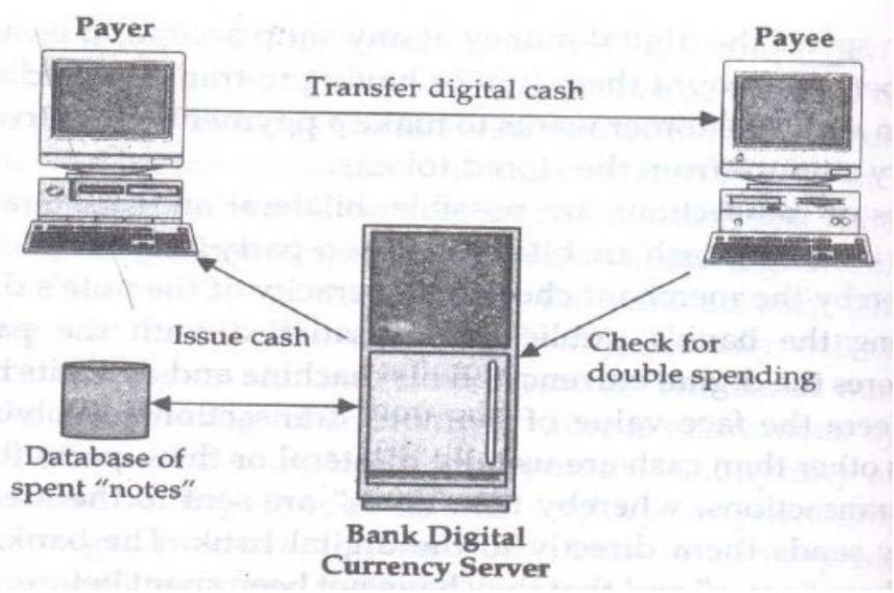
The purchase of e-cash from an on-line currency server (or bank) involves two steps:

- Establishment of an account
- Maintaining enough money in the account to bank the purchase.

- Once the tokens are purchased, the e-cash software on the customer's PC stores digital money undersigned by a bank.
- The users can spend the digital money at any shop accepting e-cash, without having to

open an account there or having to transmit credit card numbers.

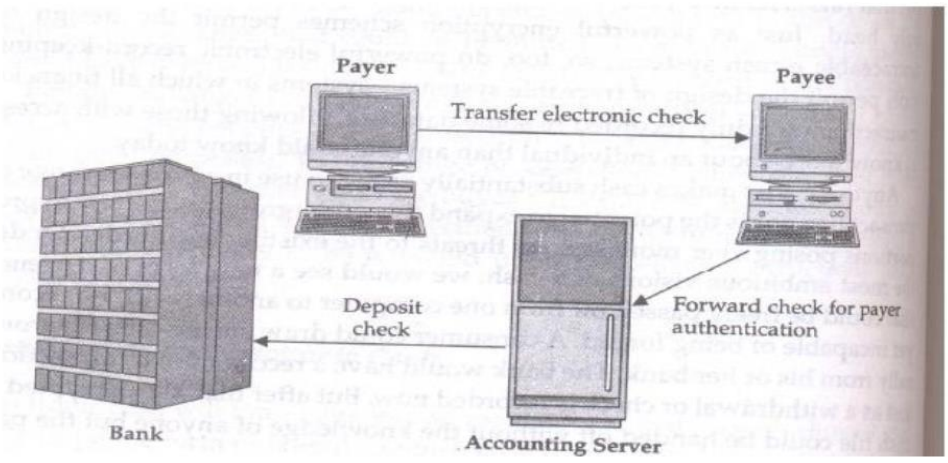
- As soon as the customer wants to make a payment, the software collects the necessary amount from the stored tokens



– Convenience

Electronic Checks:

- It is another form of electronic tokens.
- Buyers must register with third-party account server before they are able to write electronic checks.
- The account server acts as a billing service.



Advantages of Electronic Checks:

1. They work in the same way as traditional checks.
2. These are suited for clearing micropayments.
3. They create float & availability of float is an important for commerce.
4. Financial risk is assumed by the accounting server & may result in easier acceptance.

Smart Cards & Electronic Payment Systems:

- Smart cards have been in existence since the early 1980s and hold promise for secure transactions using existing infrastructure.
- Smart cards are credit and debit cards and other card products enhanced with microprocessors capable of holding more information than the traditional magnetic stripe.
- The smart card technology is widely used in countries such as France, Germany, Japan, and Singapore to pay for public phone calls, transportation, and shopper loyalty programs.

Types of Smart Cards:

- Relationship-Based Smart Credit Cards
- Electronic Purses also known as debit cards

➢ **Relationship-Based Smart Credit Cards:**

- It is an enhancement of existing cards services &/ or the addition of new services that a financial institution delivers to its customers via a chip-based card or other device.
- These services include access to multiple financial accounts, value-added marketing programs, or other information card holders may want to store on their card.
- It includes access to multiple accounts, such as debit, credit, cash access, bill payment & multiple access options at multiple locations.

➢ **Electronic Purses:**

To replace cash and place a financial instrument are racing to introduce electronic purses, wallet-sized smart cards embedded with programmable microchips that store sums of money for people to use instead of cash for everything.

The electronic purse works in the following manner:

- After purse is loaded with money at an ATM, it can be used to pay for candy in a vending machine with a card reader.
- It verifies card is authentic & it has enough money, the value is deducted from balance on the card & added to an e-cash & remaining balance is displayed by the vending machine.

Credit Card-Based Electronic Payment Systems:

Payment cards are all types of plastic cards that consumers use to make purchases:

– Credit cards

• Such as a Visa or a MasterCard, has a preset spending limit based on the user's credit limit.

– Debit cards

• Removes the amount of the charge from the cardholder's account and transfers it to the seller's bank.

– Charge cards

• Such as one from American Express, carries no preset spending limit.

Advantages:

– Payment cards provide fraud protection.

– They have worldwide acceptance.

– They are good for online transactions.

Disadvantages:

Payment card service companies charge merchants per-transaction fees and monthly processing fees.

Risks in Electronic Payment systems:

- Customer's risks
  - – Stolen credentials or password
  - – Dishonest merchant
  - – Disputes over transaction
  - – Inappropriate use of transaction details
- Merchant's risk
  - – Forged or copied instruments

– Disputed charges

– Insufficient funds in customer's account

– Unauthorized redistribution of purchased items

Electronic payments Issues:

- Secure transfer across internet
- High reliability: no single failure point
- Atomic transactions
- Anonymity of buyer
- Economic and computational efficiency: allow micropayments
- Flexibility: across different methods
- Scalability in number of servers and users

Security Requirements In Electronic Payment Systems:

- **Integrity and authorization**

  A payment system with integrity allows no money to be taken from a user without explicit authorization by that user. It may also disallow the receipt of payment without explicit consent, to prevent occurrences of things like unsolicited bribery. Authorization constitutes the most important relationship in a payment system. Payment can be authorized in three ways: via out-band authorization, passwords, and signature.

- **Out-band authorization**

  In this approach, the verifying party (typically a bank) notifies the authorizing party (the payer) of a transaction. The authorizing party is required to approve or deny the payment using a secure, out-band channel (such as via surface mail or the phone). This is the current approach for credit cards involving mail orders and telephone orders: Anyone who knows a user's credit card data can initiate transactions, and the legitimate user must check the statement and actively complain about unauthorized transactions. If the user does not complain within a certain time (usually 90 days), the transaction is considered "approved" by default.

- **Password authorization**

  A transaction protected by a password requires that every message from the authorizing party include a cryptographic check value. The check value is computed using a secret

known only to the authorizing and verifying parties. This secret can be a personal identification number, a password, or any form of shared secret. In addition, shared secrets that are short - like a six-digit PIN - are inherently susceptible to various kinds of attacks. They cannot by themselves provide a high degree of security. They should only be used to control access to a physical token like a smart card (or a wallet) that performs the actual authorization using secure cryptographic mechanisms, such as digital signatures.

- **Signature authorization**

  In this type of transaction, the verifying party requires a digital signature of the authorizing party. Digital signatures provide non repudiation of origin.

- **Confidentiality**

  Some parties involved may wish confidentiality of transactions. Confidentiality in this context means the restriction of the knowledge about various pieces of information related to a transaction: the identity of payer/payee, purchase content, amount, and so on. Typically, the confidentiality requirement dictates that this information be restricted only to the participants involved. Where anonymity or un-traceability are desired, the requirement may be to limit this knowledge to certain subsets of the participants only, as described later.

- **Availability and reliability**

  All parties require the ability to make or receive payments whenever necessary. Payment transactions must be atomic: They occur entirely or not at all, but they never hang in an unknown or inconsistent state. No payer would accept a loss of money (not a significant amount, in any case) due to a network or system crash. Availability and reliability presume that the underlying networking services and all software and hardware components are sufficiently dependable. Recovery from crash failures requires some sort of stable storage at all parties and specific resynchronization protocols. These fault tolerance issues are not discussed here, because most payment systems do not address them explicitly.

Electronic Data Interchange(EDI):

- Electronic Data Interchange (EDI) - interposes communication of business information in standardized electronic form.
- Prior to EDI, business depended on postal and phone systems that restricted communication to those few hours of the workday that overlap between time zones.

Why EDI?

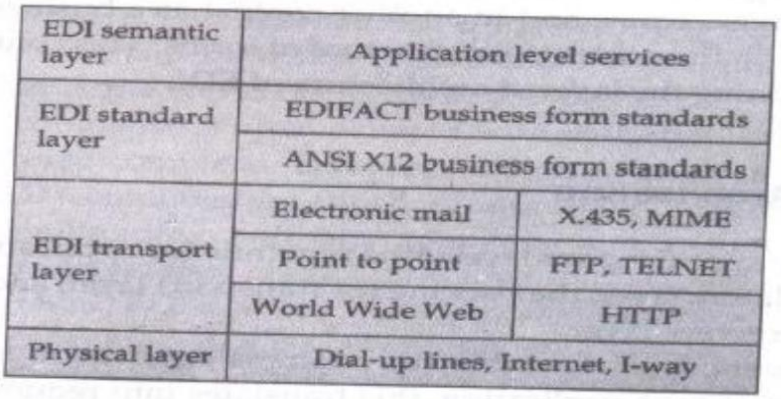
- Reduction in transaction costs
- Foster closer relationships between trading partners

EDI & Electronic Commerce

- Electronic commerce includes EDI & much more
- EDI forges boundary less relationships by improving interchange of information between trading partners, suppliers, & customers.

EDI layered architecture:

- Semantic (or application) layer
- Standards translation layer
- Packing (or transport) layer
- Physical network infrastructure layer



EDI semantic layer	Application level services	
EDI standard layer	EDIFACT business form standards	
	ANSI X12 business form standards	
EDI transport layer	Electronic mail	X.435, MIME
	Point to point	FTP, TELNET
	World Wide Web	HTTP
Physical layer	Dial-up lines, Internet, I-way	

EDI semantic layer:

- Describes the business application
- Procurement example
  - Requests for quotes
  - Price quotes
  - Purchase orders
  - Acknowledgments
  - Invoices
- Specific to company & software used

Standards translation:

- Specifies business form structure so that information can be exchanged
- Two competing standards
  - American National Standards Institute(ANSI)X12
  - EDIFACT developed by UN/ECE, Working Party for the Facilitation of International Trade Procedures

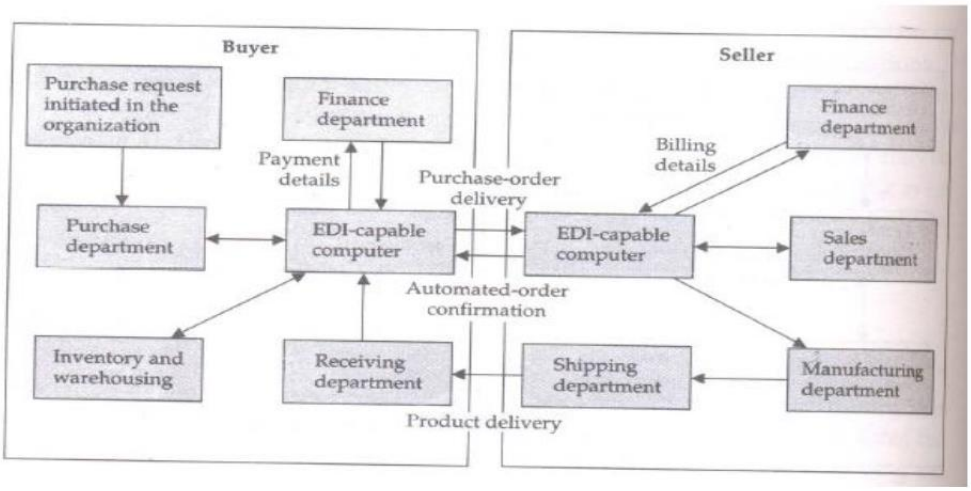
EDI transport layer

- How the business form is sent, e.g. post, UPS, fax
- Increasingly, e-mail is the carrier
- Differentiating EDI from e-mail
  - Emphasis on automation
  - EDI has certain legal status

Physical network infrastructure layer

- Dial-up lines, Internet, value-added network, etc.

Information flow with EDI:



1. Buyer sends purchase order to seller computer
2. Seller sends purchase order confirmation to buyer
3. Seller sends booking request to transport company
4. Transport company sends booking confirmation to seller
5. Seller sends advance ship notice to buyer
6. Transport company sends status to seller
7. Buyer sends Receipt advice to seller

8. Seller sends invoice to buyer
9. Buyer sends payment to seller

Applications of EDI:

1. Role of EDI in international trade:

- Reduced transaction expenditures
- Quicker movement of imported & exported goods
- Improved customer service through "track & trace" programs
- Faster customs clearance & reduced opportunities for corruption, a huge problem in trade

2. Interbank Electronic Funds Transfer (EFT)

• EFTS is credit transfers between banks where funds flow directly from the payer's bank to the payee's bank.

• The two biggest funds transfer services in the United States are the Federal Reserve's system, Fed wire, & the Clearing House Interbank Payments System (CHIPS) of the New York clearing house

3. Health care EDI for insurance EDI

• Providing good & affordable health care is a universal problem

• EDI is becoming a permanent fixture in both insurance & health care industries as medical provider, patients, & payers

• Electronic claim processing is quick & reduces the administrative costs of health care.

• Using EDI software, service providers prepare the forms & submit claims via communication lines to the value-added network service provider

• The company then edits sorts & distributes forms to the payer. If necessary, the insurance company can electronically route transactions to a third-party for price evaluation

• Claims submission also receives reports regarding claim status & request for additional Information

4. Manufacturing & retail procurement using EDI

• These are heavy users of EDI

• In manufacturing, EDI is used to support just-in-time.

• In retailing, EDI is used to support quick response

EDI Protocols:

- ANSI X12
- EDIFACT

Comparison of EDIFACT & X.12 Standards:

- These are comprised of strings of data elements called segments.
- A transaction set is a set of segments ordered as specified by the standard.
- ANSI standards require each element to have a very specific name, such as order date or invoice date.
- EDIFACT segments, allow for multiuse elements, such as date.
- EDIFACT has fewer data elements & segments & only one beginning segment (header),but it has more composites.
- It is an ever-evolving platform.

E-Marketing:

- E-marketing is directly marketing a commercial message to a group of people using email. In its broadest sense, every email sent to a potential or current customer could be considered email marketing.
- It usually involves using email to send ads, request business, or solicit sales or donations, and is meant to build loyalty, trust, or brand awareness.
- Email marketing can be done to either sold lists or a current customer database. Broadly, the term is usually used to refer to sending email messages with the purpose of enhancing the relationship of a merchant with its current or previous customers, to encourage customer loyalty and repeat business, acquiring new customers or convincing current customers to purchase something immediately, and adding advertisements to email messages sent by other companies to their customers.

Advantages:

- An exact return on investment can be tracked and has proven to be high when done properly. Email marketing is often reported as second only to search marketing as the most effective online marketing tactic.
- Email marketing is significantly cheaper and faster than traditional mail, mainly because of high cost and time required in a traditional mail campaign for producing the artwork, printing, addressing and mailing.
- Advertisers can reach substantial numbers of email subscribers who have opted in (i.e., consented) to receive email communications on subjects of interest to them.
- Almost half of American Internet users check or send email on a typical day with email blasts that are delivered between 1 am and 5 am local time outperforming those sent at other times in open and click rates.
- Email is popular with digital marketers, rising an estimated 15% in 2009 to £292 m in the UK.
- If compared to standard email, direct email marketing produces higher response rate and higher average order value for e-commerce businesses.

Disadvantages:

- A report issued by the email services company Return Path, as of mid-2008 email deliverability is still an issue for legitimate marketers. According to the report, legitimate email servers averaged a delivery rate of 56%; twenty percent of the messages were rejected, and eight percent were filtered.
- Companies considering the use of an email marketing program must make sure that their program does not violate spam laws such as the United States' Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM),the European Privacy and Electronic Communications Regulations 2003, or their Internet service provider's acceptable use policy.

Tele Marketing:

- Telemarketing is a method of direct marketing in which a salesperson solicits prospective customers to buy products or services, either over the phone or through a subsequent face to face or Web conferencing appointment scheduled during the call.
- Telemarketing can also include recorded sales pitches programmed to be played over the phone via automatic dialing.
- Telemarketing may be done from a company office, from a call center, or from home. It may involve a live operator voice broadcasting which is most frequently associated with political messages.
- An effective telemarketing process often involves two or more calls. The first call (or series of calls) determines the customer's needs. The final call (or series of calls) motivates the customer to make a purchase. Prospective customers are identified by various means, including past purchase history, previous requests for information, credit limit, competition entry forms, and application forms. Names may also be purchased from another company's consumer database or obtained from a telephone directory or another public list. The qualification process is intended to determine which customers are most likely to purchase the product or service.
- Charitable organizations, alumni associations, and political parties often use telemarketing to solicit donations. Marketing research companies use telemarketing techniques to survey the prospective or past customers of a client's business in order to assess market acceptance of or satisfaction with a particular product, service, brand, or company. Public opinion polls are conducted in a similar manner.
- Telemarketing techniques are also applied to other forms of electronic marketing using e-mail or fax messages, in which case they are frequently considered spam by receivers.

Disadvantages:

- Telemarketing has been negatively associated with various scams and frauds, such as pyramid schemes, and with deceptively overpriced products and services
- Telemarketing is often criticized as an unethical business practice due to the perception of high-pressure sales techniques during unsolicited calls.

- Telemarketers marketing telephone companies may participate in telephone slamming, the practice of switching a customer's telephone service without their knowledge or authorization.
- Telemarketing calls are often considered an annoyance, especially when they occur during the dinner hour, early in the morning, or late in the evening.

REFERENCE

Cyber Law: Intellectual Property and E-Commerce Security Hardcover – January 1, 2011 by Kumar & Sharma (Author)

Cyberlaw and E-Commerce 1st Edition by David Lee Baumer (Author), J. C. Poindexter (Author)

CYBER LAW AND E COMMERCE IN 60 MINUTES Jun 3, 2014 by sukhdarshan sehgal

Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace Jul 10, 2014 by Scott J. Shackelford