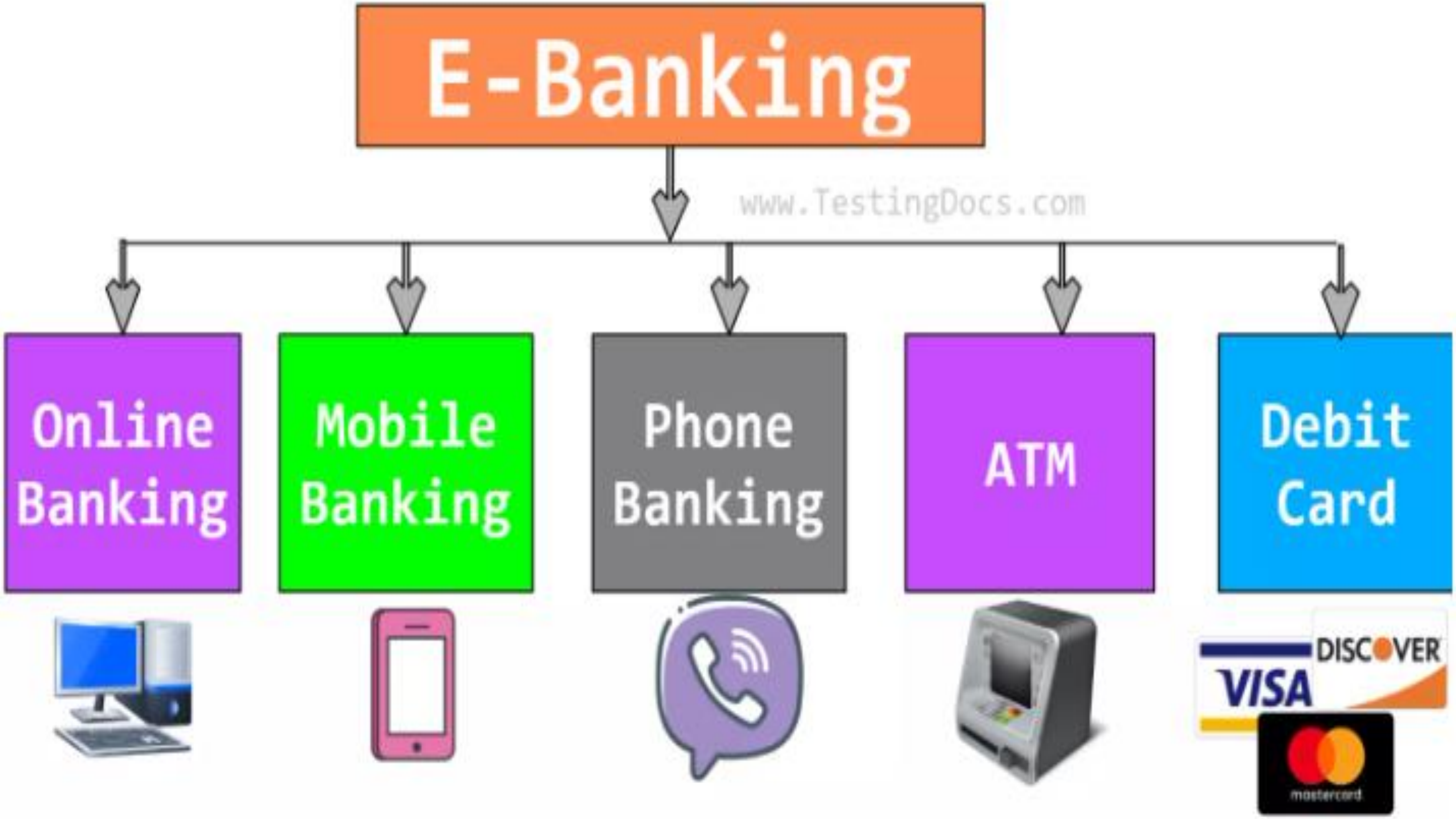


E-Banking

Online Banking

Mobile Banking

Phone Banking

ATM

Debit Card

Introduction to Bank Transfer

- Bank Transfer is the most favourite online payment methods.
- It is perceived as the most convenient and traditional way of doing payment. Around half of the online shopping uses Bank Transfer for payment over Cash on Delivery, Card Payment, or other payment methods.

Methods on doing Bank Transfer

- There are two categories of Bank Transfer based on the sender’s and receiver’s Bank account:

1. Intrabank transfer.

- Intrabank transfer is in-house transfer; means transfer is done within the same Bank network. To do an intrabank transfer, sender should have the same Bank network with the receiver. For example, a sender uses his/her BOI account to transfer to receiver’s BOI account.

2. Interbank transfer

- Interbank transfer is a money transfer to a different Bank; sender uses a different Bank network to transfer to the receiver.
- For example, a sender uses BOI account to transfer to receiver’s SBI account. In this case, there will be more parties involved; the sender’s Bank, Principal Network, and receiver’s Bank. Sender will be charged an additional bank transfer fees for interbank transfer.

Electronic Payment System

OBJECTIVES

- To understand the concept of Electronic Payment System and its security services.

- To bring out solution in the form of applications to uproot Electronic Payment.

- To understand working of various Electronic Payment System based applications.

What Electronic Payment system is?

Electronic payment system is a system which helps the customer or user to make online payment for their shopping.

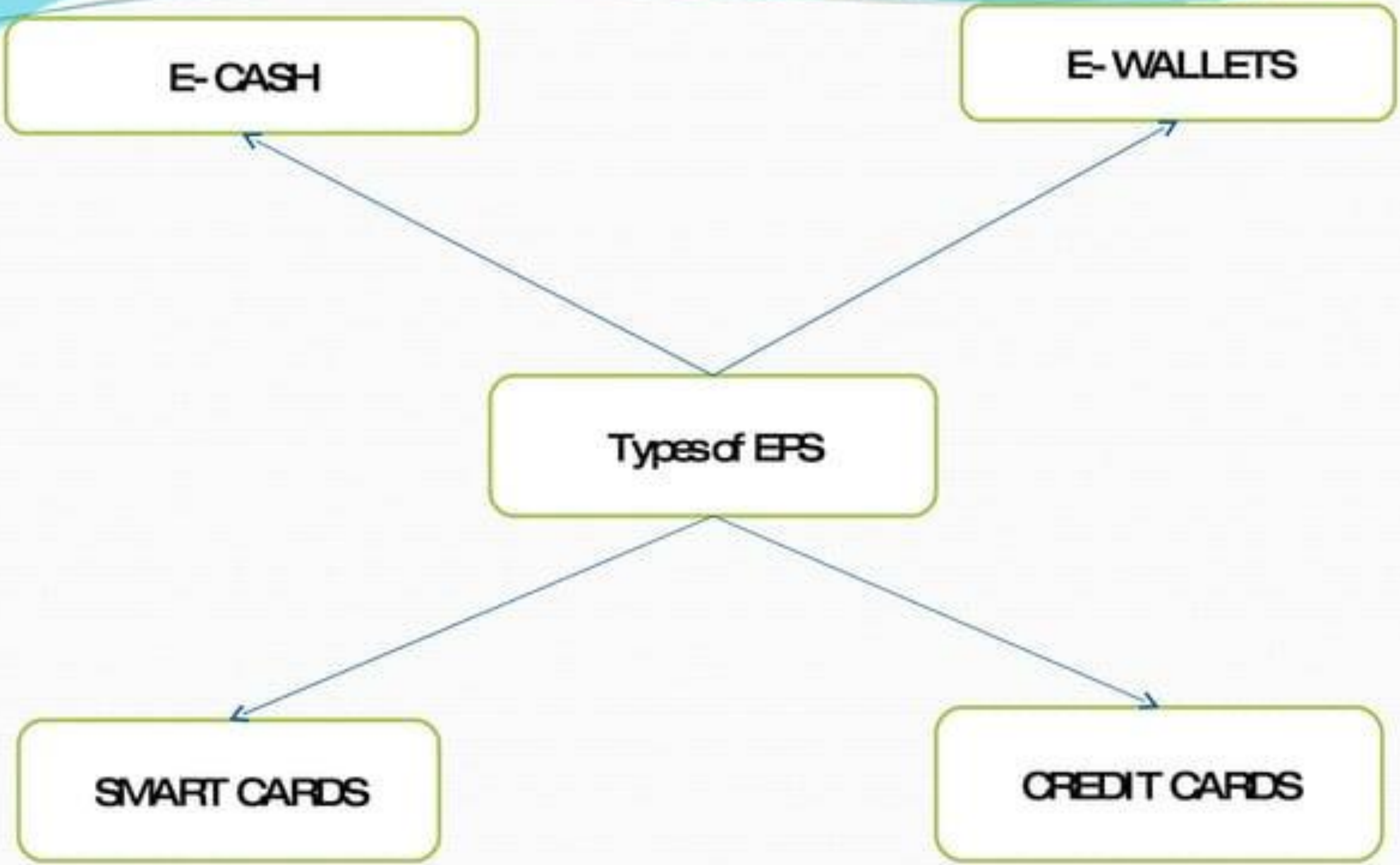
- To transfer money over the Internet.
- Methods of traditional payment.
  - Check, credit card, or cash.
- Methods of electronic payment.
  - Electronic cash, software wallets, smart cards, and credit/debit cards.

Some Examples Of EPS:-

- ❑Online reservation
- ❑Online bill payment
- ❑Online order placing (nirulas)
- ❑Online ticket booking (Movie)

Two storage methods

- On-line
  - Individual does not have possession personally of electronic cash
  - Trusted third party, e.g. online bank, holds customers' cash accounts
- Off-line
  - Customer holds cash on smart card or software wallet
  - Fraud and double spending require tamper-proof encryption



E- CASH

E- WALLETS

Types of EPS

SMART CARDS

CREDIT CARDS

E-Cash

- A system that allows a person to pay for goods or services by transmitting a number from one computer to another.

- Like the serial numbers on real currency notes, the E-cash numbers are unique.

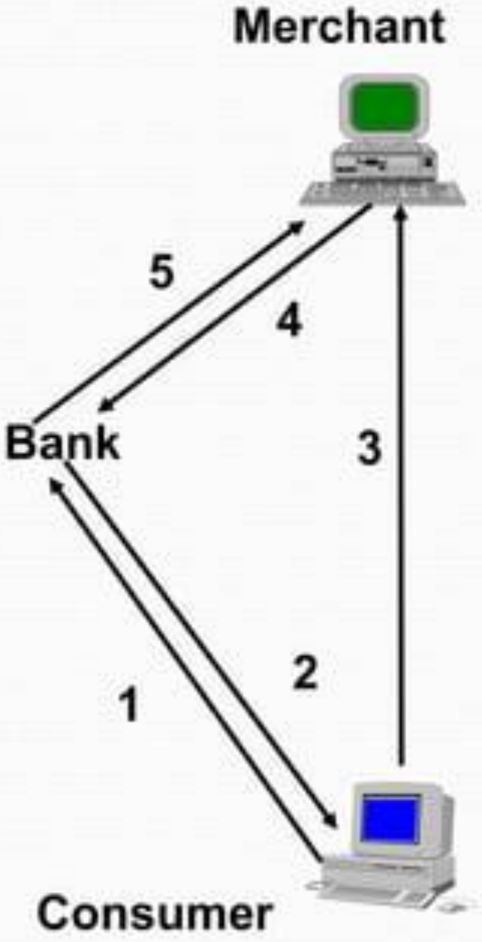
- This is issued by a bank and represents a specified sum of real money.

- It is anonymous and reusable.

Electronic Cash Security

- Complex cryptographic algorithms prevent double spending
  - Anonymity is preserved unless double spending is attempted
- Serial numbers can allow tracing to prevent money laundering

E-Cash Processing



1. Consumer buys e-cash from Bank

2. Bank sends e-cash bits to consumer (after charging that amount plus fee)

3. Consumer sends e-cash to merchant

4. Merchant checks with Bank that e-cash is valid (check for forgery or fraud)

5. Bank verifies that e-cash is valid

6. Parties complete transaction

E-Wallet

- The E-wallet is another payment scheme that operates like a carrier of e-cash and other information.

- The aim is to give shoppers a single, simple, and secure way of carrying currency electronically.

- Trust is the basis of the e-wallet as a form of electronic payment.

Procedure for using an e-wallet

1. Decide on an online site where you would like to shop.

3. Download a wallet from the merchant's website.

5. Fill out personal information such as your credit card number, name, address and phone number, and where merchandise should be shipped.

7. When you are ready to buy, click on the wallet button, the buying process is fully executed.

Smart Cards

- A **smart card**, is any pocket-sized card with embedded integrated circuits which can process data

- This implies that it can receive input which is processed and delivered as an output

Smart card Processing

1. User opens account and receives smart card
2. User downloads tokens onto card
3. User inserts card in reader
4. Tokens are transferred from user card to vendor
5. Goods delivered
6. Vendor redeems tokens

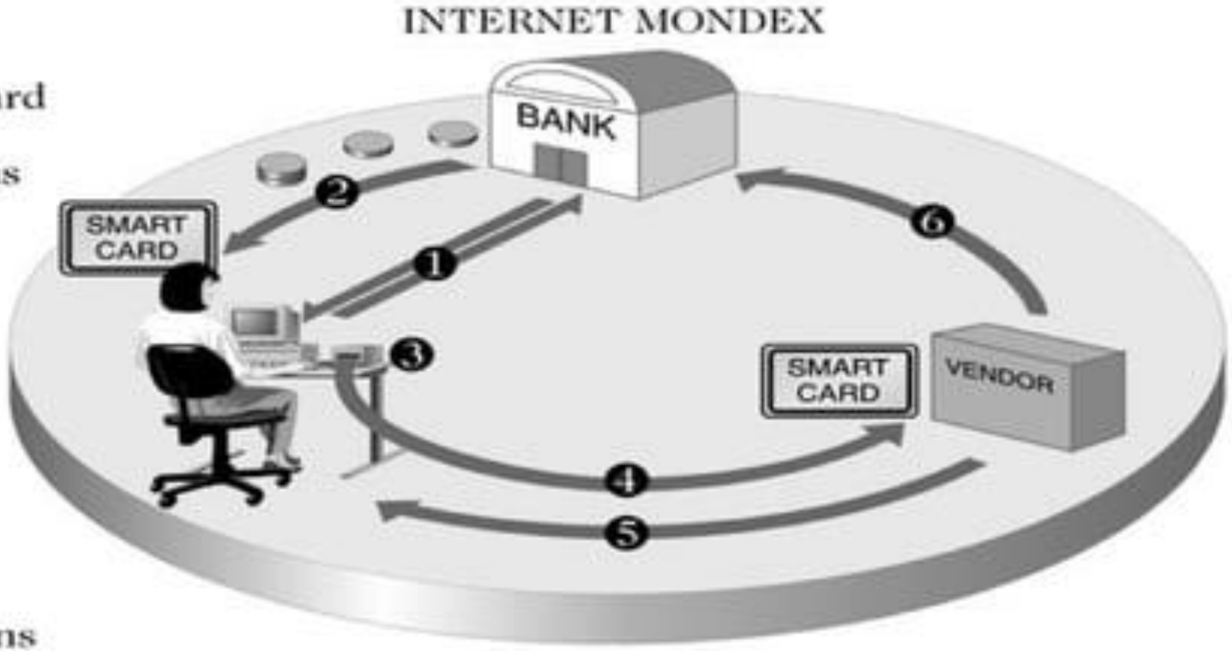


FIGURE 7-12 *Mondex smart card processing*

Credit cards

- It is a Plastic Card having a Magnetic Number and code on it.
- It has Some fixed amount to spend.
- Customer has to repay the spend amount after sometime.

Processing a Credit cards payment

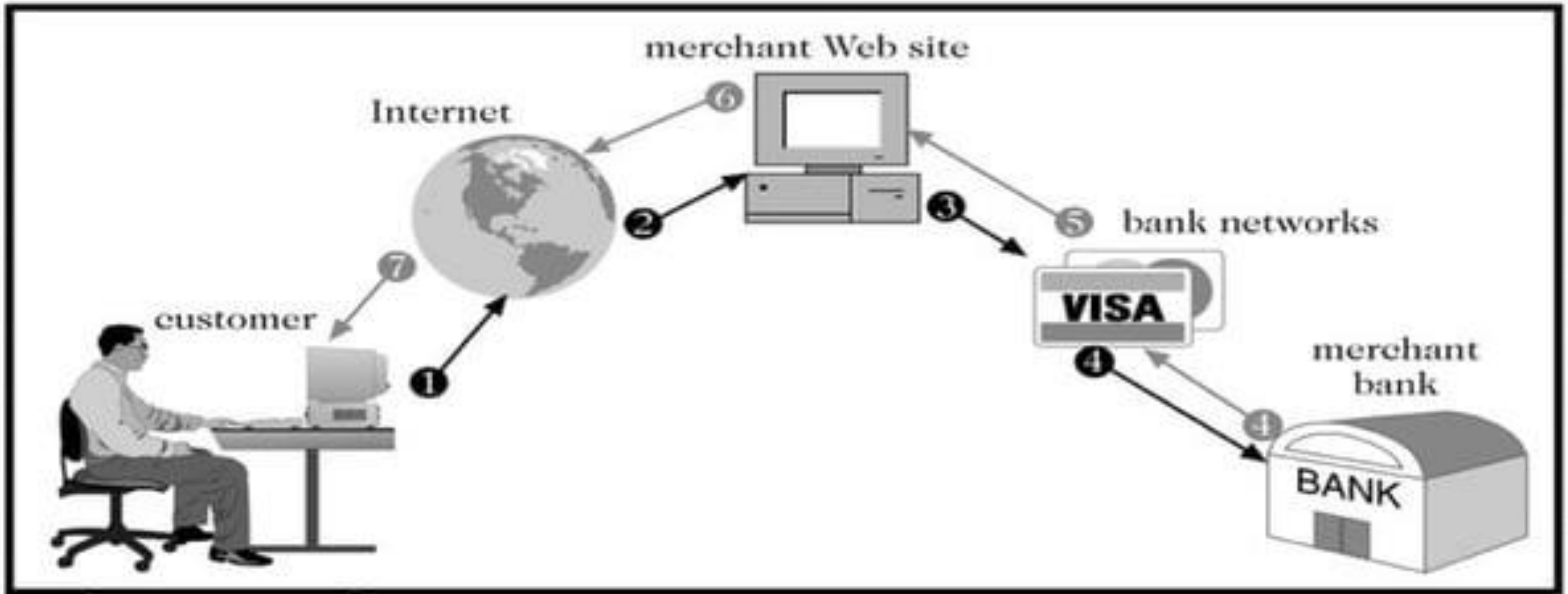


FIGURE 7-13 *Processing a payment card order*

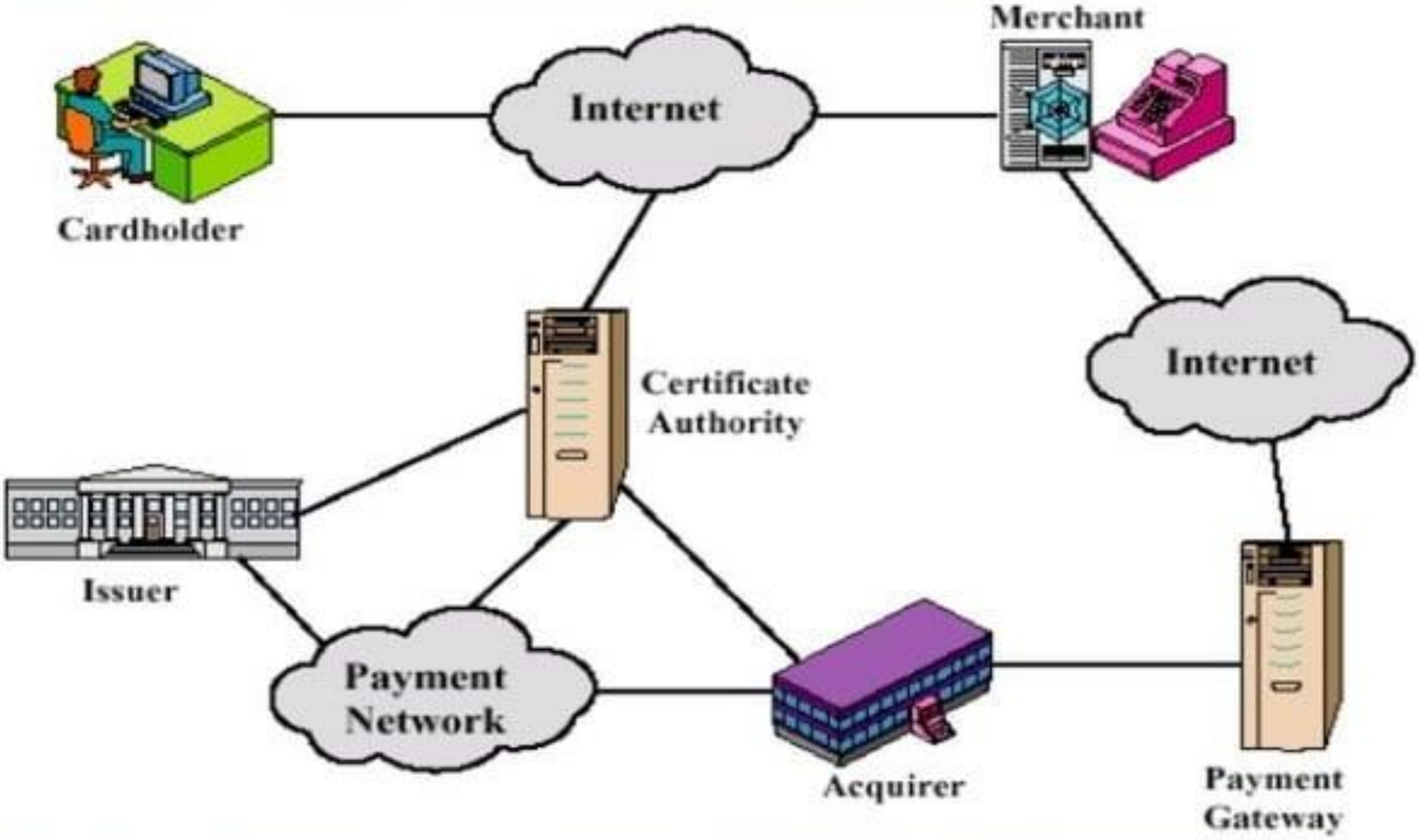
Risk in using Credit cards

- Operational Risk
- Credit Risk
- Legal Risk

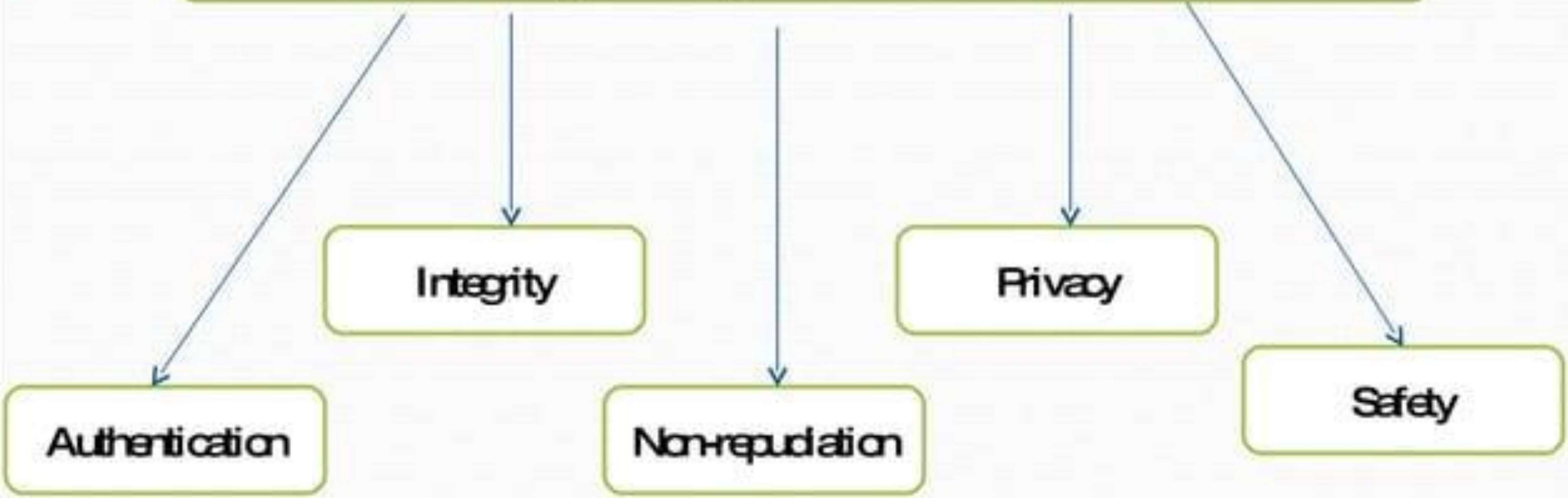
Secure Electronic Transaction (SET) Protocol

- Jointly designed by MasterCard and Visa with backing of Microsoft, Netscape, IBM, GTE, SAIC, and others
- Designed to provide security for card payments as they travel on the Internet
  - Contrasted with Secure Socket Layers (SSL) protocol, SET validates consumers and merchants in addition to providing secure transmission
- SET specification
  - Uses public key cryptography and digital certificates for validating both consumers and merchants
  - Provides privacy, data integrity, user and merchant authentication, and consumer nonrepudiation

The SET protocol



Security Requirements of EPS



Authentication

Integrity

Non-repudiation

Privacy

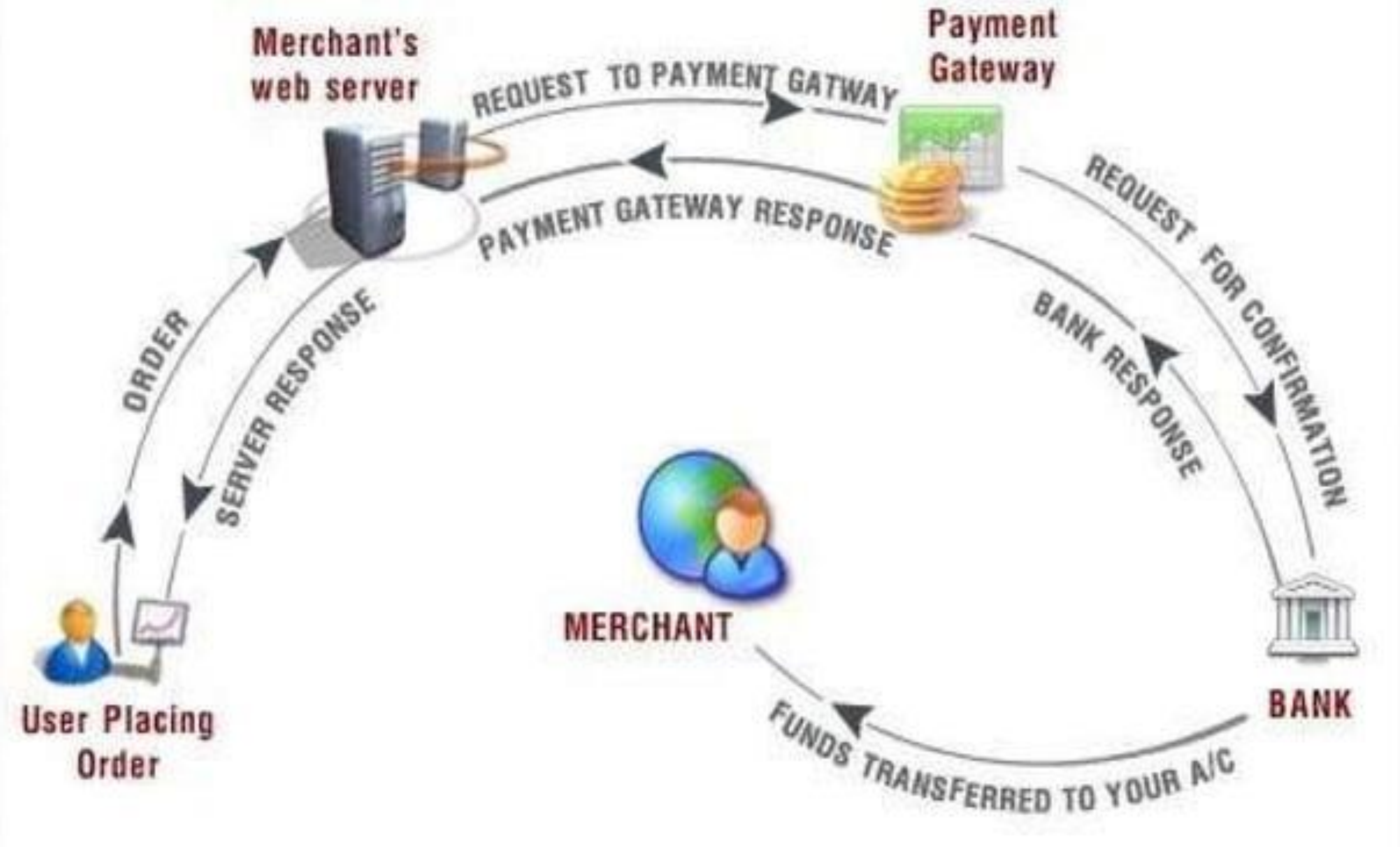
Safety

What Is payment Gateways??

- A **payment gateway** is an e-commerce application service provider service that authorizes payments for e-businesses, online Shopping, etc.

- Payment gateway protects credit cards details encrypting sensitive information, such as credit card numbers, to ensure that information passes securely between the customer and the merchant and also between merchant and payment processor.

How It works??


Merchant's web server
REQUEST TO PAYMENT GATWAY
Payment Gateway
PAYMENT GATEWAY RESPONSE
REQUEST FOR CONFIRMATION
BANK RESPONSE
ORDER
SERVER RESPONSE
MERCHANT
BANK
User Placing Order
FUNDS TRANSFERRED TO YOUR A/C

❑ Expand Market beyond Traditional geographic market

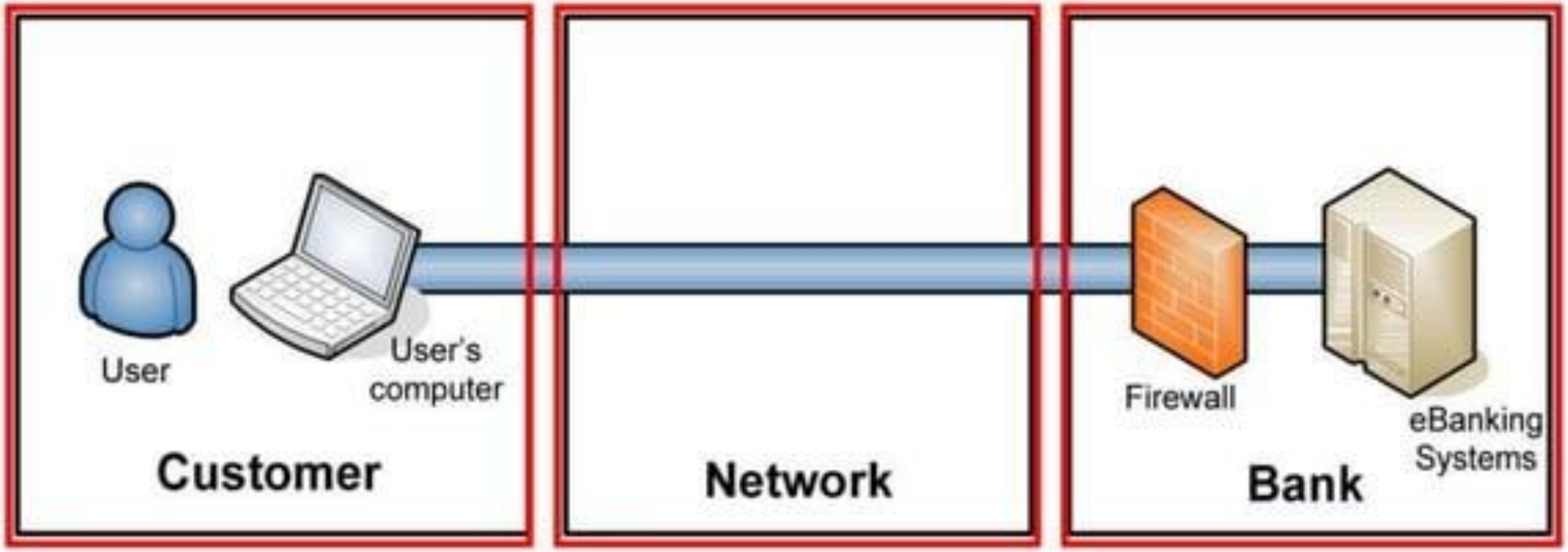
❑ Override traditional marketing system into digital marketing system.

❑ Made human life convenient as a person can pay his payments online while he is taking rest.

E-banking security

eBanking Attacks

Target of Attacks



Phishing Attacks
Trojan Attacks

Pharming
DNS Spoofing
Network Interception

Web Application Attacks
Attacking Server

Client Attacks

Most promising attack on the client:

- **Phishing**
  - Motivate user to enter confidential information on fake web site

- **Simple Trojans**
  - Limited to a handful of eBanking applications
  - Steal username, password and one time password
  - Steals session information and URL and sends it to attacker
  - Attacker imports information into his browser to access the same account

- **Generic Trojans**
  - In the wild since 2007, but still in development
  - Can attack any eBanking (and any web application)
  - New configuration is downloaded continously

Generic Trojans

- **Infection of client with user interaction**
  - Email attachments (ZIP, Exe, etc.)
  - Email with link to malicious web site
  - Links in social networks
  - Integrated in popular software (downloads)
  - File transfer of instant messaging/VoIP/file sharing
  - CD-ROM/USB Stick
- **Infection of client without user interaction**
  - Malicious web sites (drive by)
  - Infection of trusted, popular web sites (IFRAME ...)
  - Misusing software update functionality (like Bundestrojaner)
  - Attacks on vulnerable, exposed computer (network/wireless)

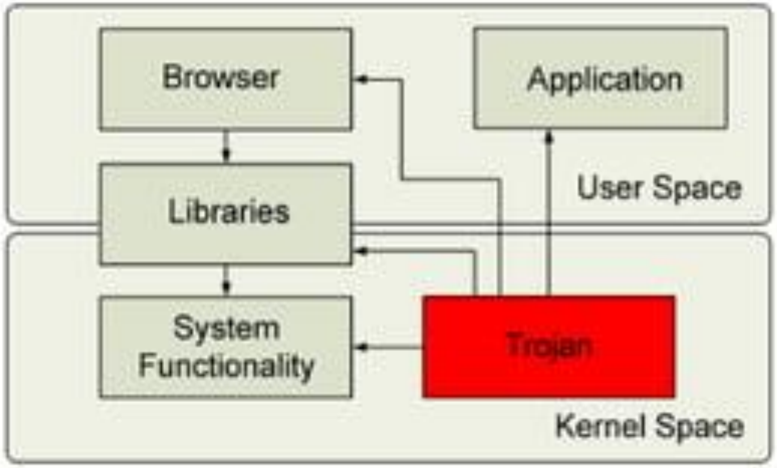
Note: About 1% of Google search query results point to a web site that can lead to a drive by attack.

Generic Trojans

- Features of Generic Trojans
  - Hide from security tools (anti-virus/personal firewall)
  - Inject code in running processes / drivers / operating system
  - Capture/Redirect/Send data
  - Download new configuration / functionality
  - Remote control browser instance

Generic Trojans(cont)

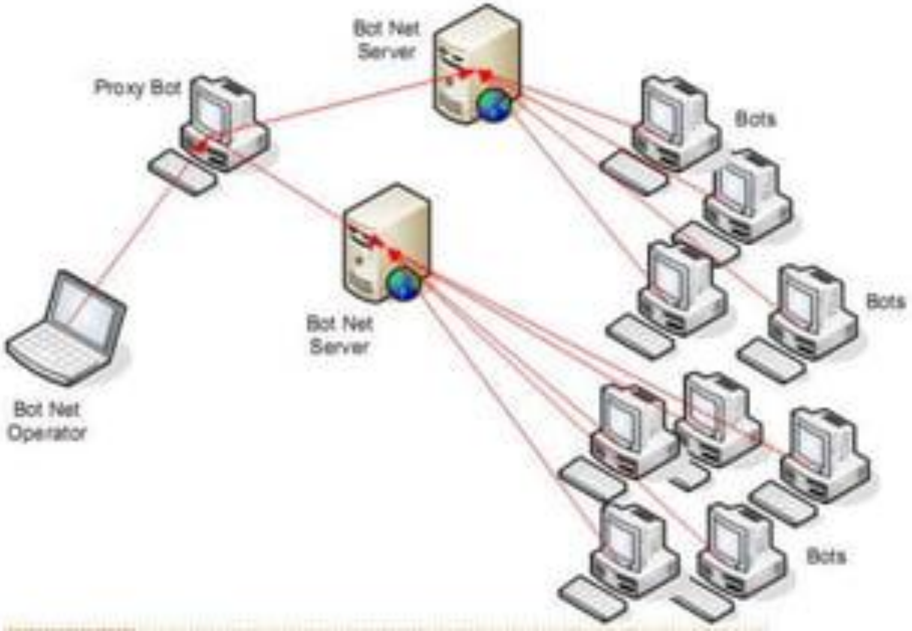
- Features useful for eBanking attacks
  - Send web pages of unknown eBanking to attacker
  - Download new patterns of eBanking transaction forms
  - Modify transaction in the background (on the fly)
  - Collect financial information



Generic Trojans(cont)

Tips and Tricks

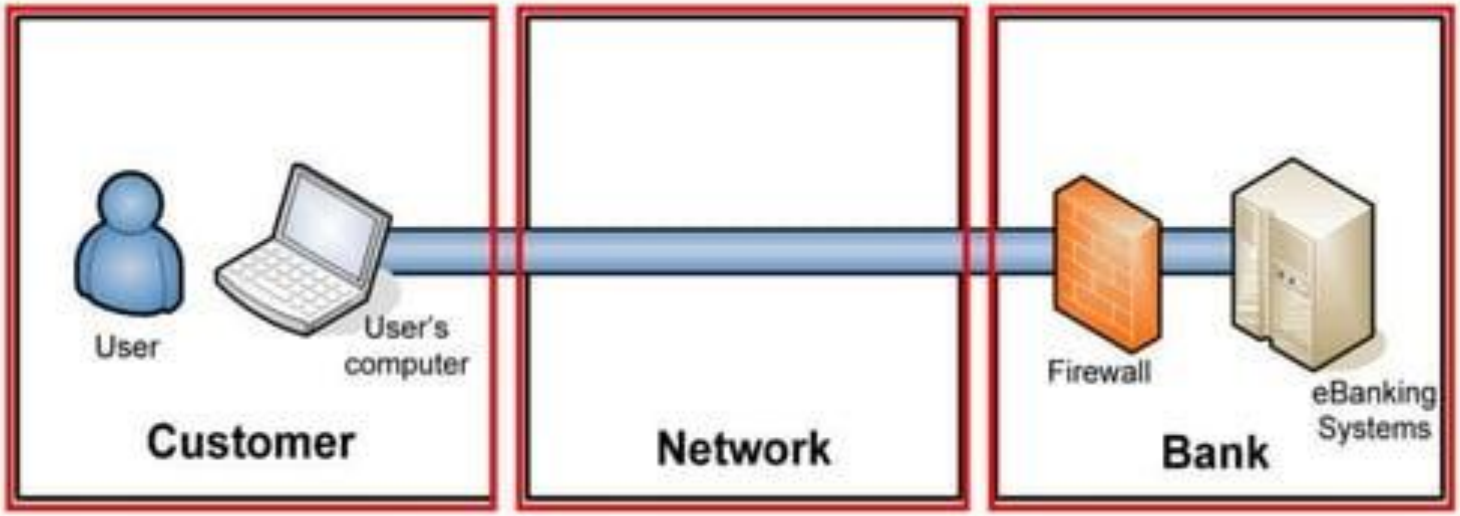
- Every Trojan binary is unique (packed differently)
  - Not detectable by Anti Virus Patterns
- Trojan code is injected into other files or other processes
  - Personal Firewall can not block communication
- Installs in Kernel
  - Full privileges on system
  - Invisible
- Bot Networks



Security Measures

Security Measures

- Attack Detection
- Second Channel / Secured Channel
- Secure Client



Secure Client

Second Channel
Secured Channel

Attack Detection

Attack Detection

- Detect session hijacking attacks
    - Monitor and compare request parameters
    - Identify SSL Session and IP address changes
- Transaction verification / user profiling
    - Statistic about normal user behaviour
    - Compare transaction with normal user behaviour
    - White list target accounts
    - Limits on transaction amount

Security Measures(cont)

- Second Channel
  - Send verification using another channel
  - Another application on the client computer
  - Another medium like mobile phones (SMS)
- Secured Channel
  - Enter data on an external device
  - External device can not be controlled by Trojan
  - Externel device contains a secret key

Security Measures

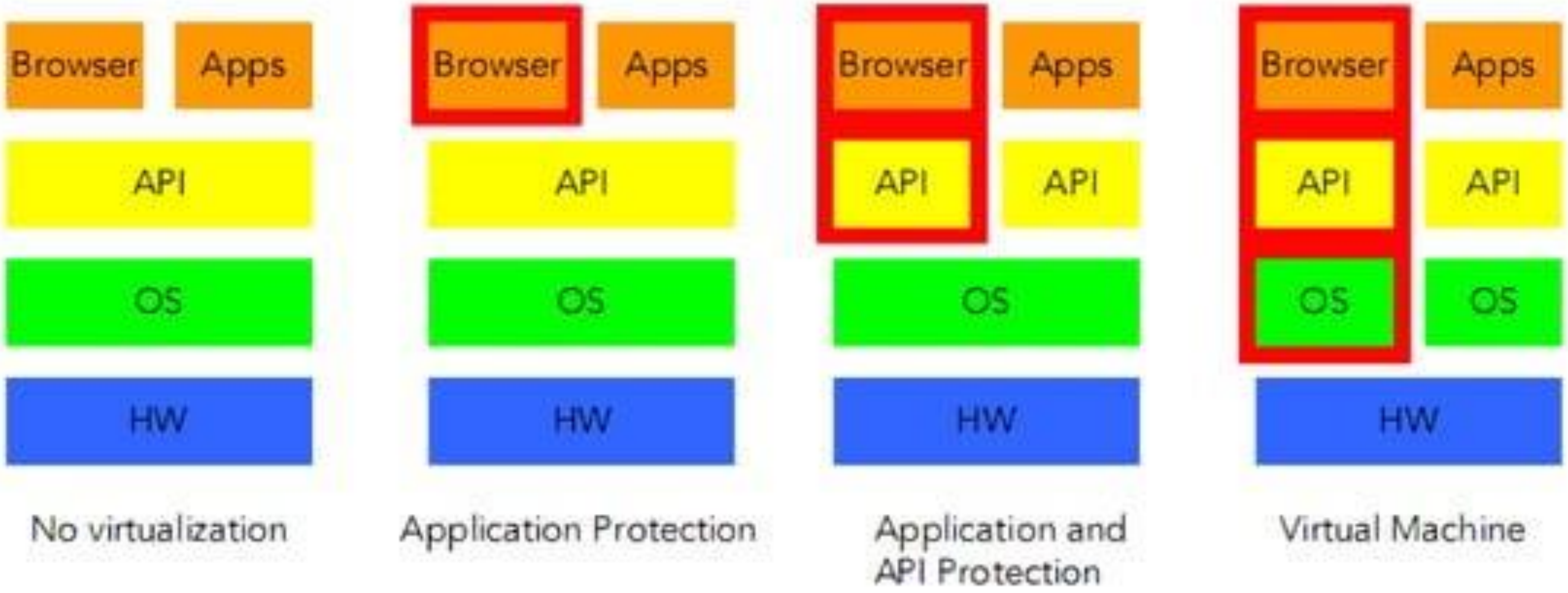
- Secure Platform
  - A computer that is only used for eBanking
  - Bootable CD-ROM, Bootable USB Stick
  - Virtual Machine
  - eBanking Laptop
- Secure Environment
  - Start an application (eg Browser) that protects itself from Trojans
  - Downstripped Browser
  - Proprietary Application (fat client)
  - Verify environment before login is possible

Security Trends

Current client security approaches:

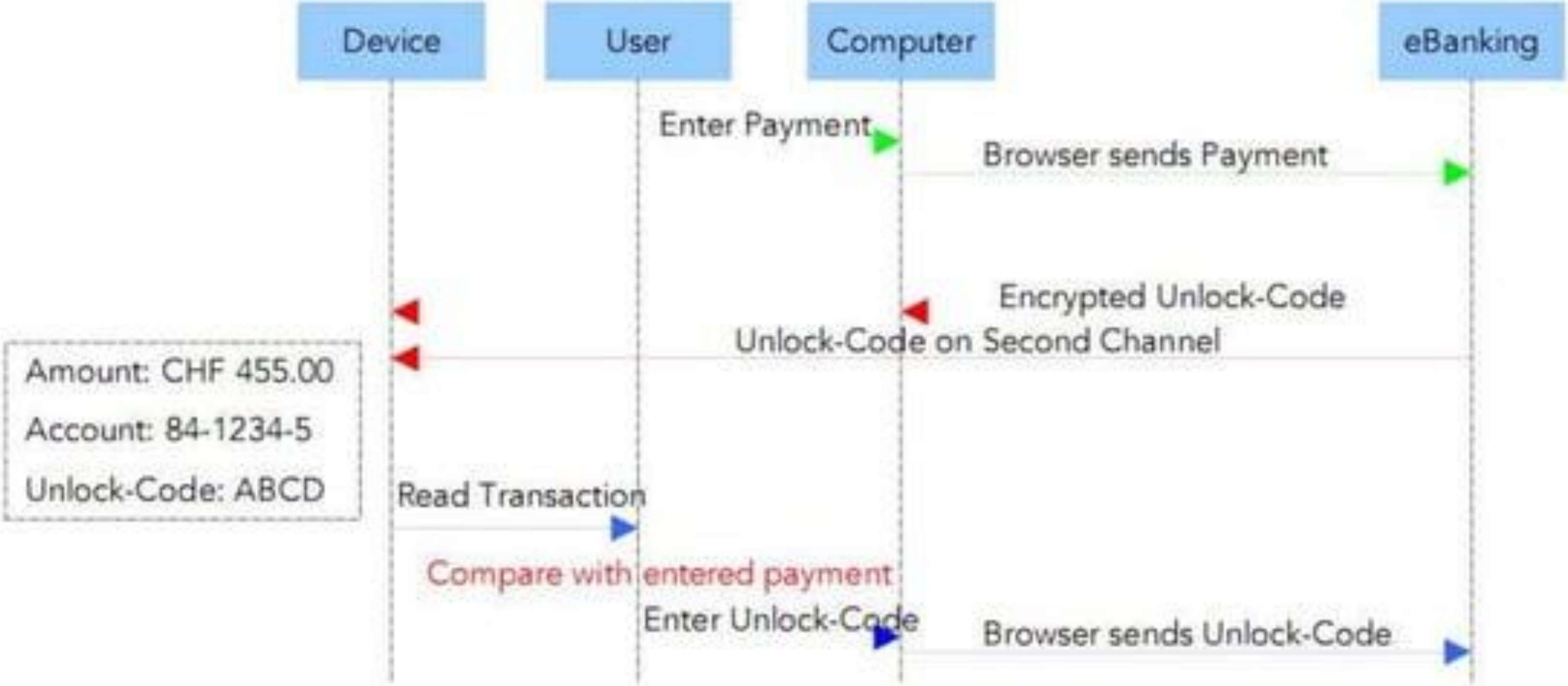
- A) Secured Application/Virtualization
  - Hardened Browser on USB stick
  - Application to secure the client
  - Virtual operating system on host system
  - Bootable CD-ROM/USB stick
- B) Transaction Signing
  - Transaction details and unlock code on mobile (SMS)
  - External device with SmartCard
  - Read information from screen and decrypt on external device

A) Secured Application/Virtualization



- Solutions (some examples):
  - Portable Apps, Thinstall
  - CLX Stick, Kobil mIdentity
  - Browser Appliance (eg VMWare, VirtualPC, etc.)

B) Transaction Signing



- Devices (some examples):
  - Mobile phones
  - IBM ZTIC, EVM CAP, Axsionics
  - Tricipher

Security Trends

Axsionics
Internet Passport

SmartCard
Reader

IBM ZTIC

TriCipher
Armored Transactions

IBM ZTIC

Crealogix
CLX Stick

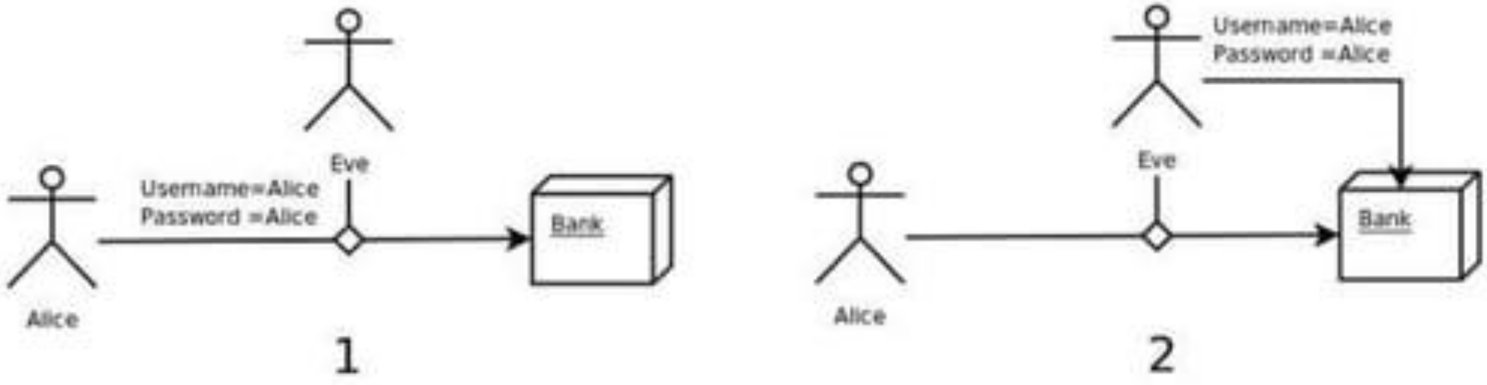
Kobil mIDentity

Secure Communication

Most Internet shopping sites use usernames and passwords to authenticate its users, so called 'password authentication'. They are typically more concerned with the validity of the credit card than the identity of the user. This will be our starting point.

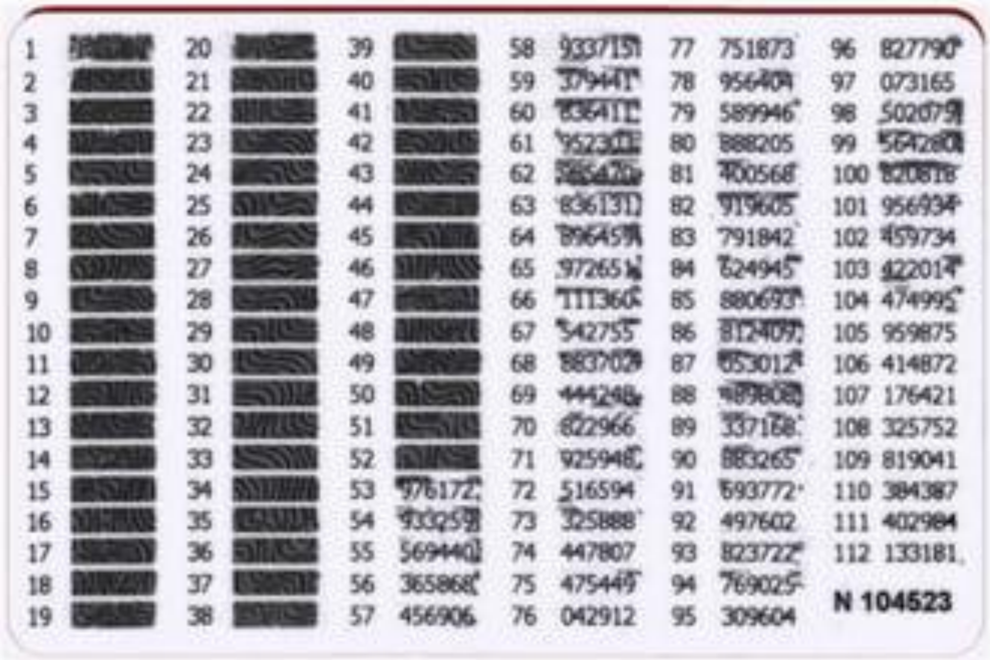
Password authentication

- In our fictious example we have a user Alice who wishes to login to her bank. We also have a vicious attacker Eve who is trying to steal Alice's hard-earned money. The bank is using a username and password to protect
- Alice's account but no encryption. This scheme is obviously vulnerable to a snooping attack as illustrated in below Figure. One way to improve security is by employing **One-time Passwords**.



One-time Passwords

- One-time passwords (OTPs) are, like the name suggests, passwords that are used only once.



1	[redacted]	20	[redacted]	39	[redacted]	58	933715	77	751873	96	827790
2	[redacted]	21	[redacted]	40	[redacted]	59	379441	78	956404	97	073165
3	[redacted]	22	[redacted]	41	[redacted]	60	836411	79	589946	98	502079
4	[redacted]	23	[redacted]	42	[redacted]	61	952311	80	888205	99	564280
5	[redacted]	24	[redacted]	43	[redacted]	62	365420	81	400568	100	820818
6	[redacted]	25	[redacted]	44	[redacted]	63	836131	82	919605	101	956934
7	[redacted]	26	[redacted]	45	[redacted]	64	896459	83	791842	102	459734
8	[redacted]	27	[redacted]	46	[redacted]	65	972651	84	624945	103	422014
9	[redacted]	28	[redacted]	47	[redacted]	66	111360	85	880693	104	474995
10	[redacted]	29	[redacted]	48	[redacted]	67	542755	86	812409	105	959875
11	[redacted]	30	[redacted]	49	[redacted]	68	883702	87	653012	106	414872
12	[redacted]	31	[redacted]	50	[redacted]	69	444248	88	489808	107	176421
13	[redacted]	32	[redacted]	51	[redacted]	70	822966	89	337168	108	325752
14	[redacted]	33	[redacted]	52	[redacted]	71	925948	90	883265	109	819041
15	[redacted]	34	[redacted]	53	976172	72	516594	91	693772	110	384387
16	[redacted]	35	[redacted]	54	933259	73	325888	92	497602	111	402984
17	[redacted]	36	[redacted]	55	569440	74	447807	93	823722	112	133181
18	[redacted]	37	[redacted]	56	365868	75	475449	94	769025	N 104523	
19	[redacted]	38	[redacted]	57	456906	76	042912	95	309604		

A code scratch card with OTPs

Implementations

Chip Authentication Program (CAP)

- CAP is a relatively new protocol based on the older EMV standard.
- It was developed by MasterCard and is based on digitally signing transactions.
- CAP can operate in three modes: identify, respond and sign.

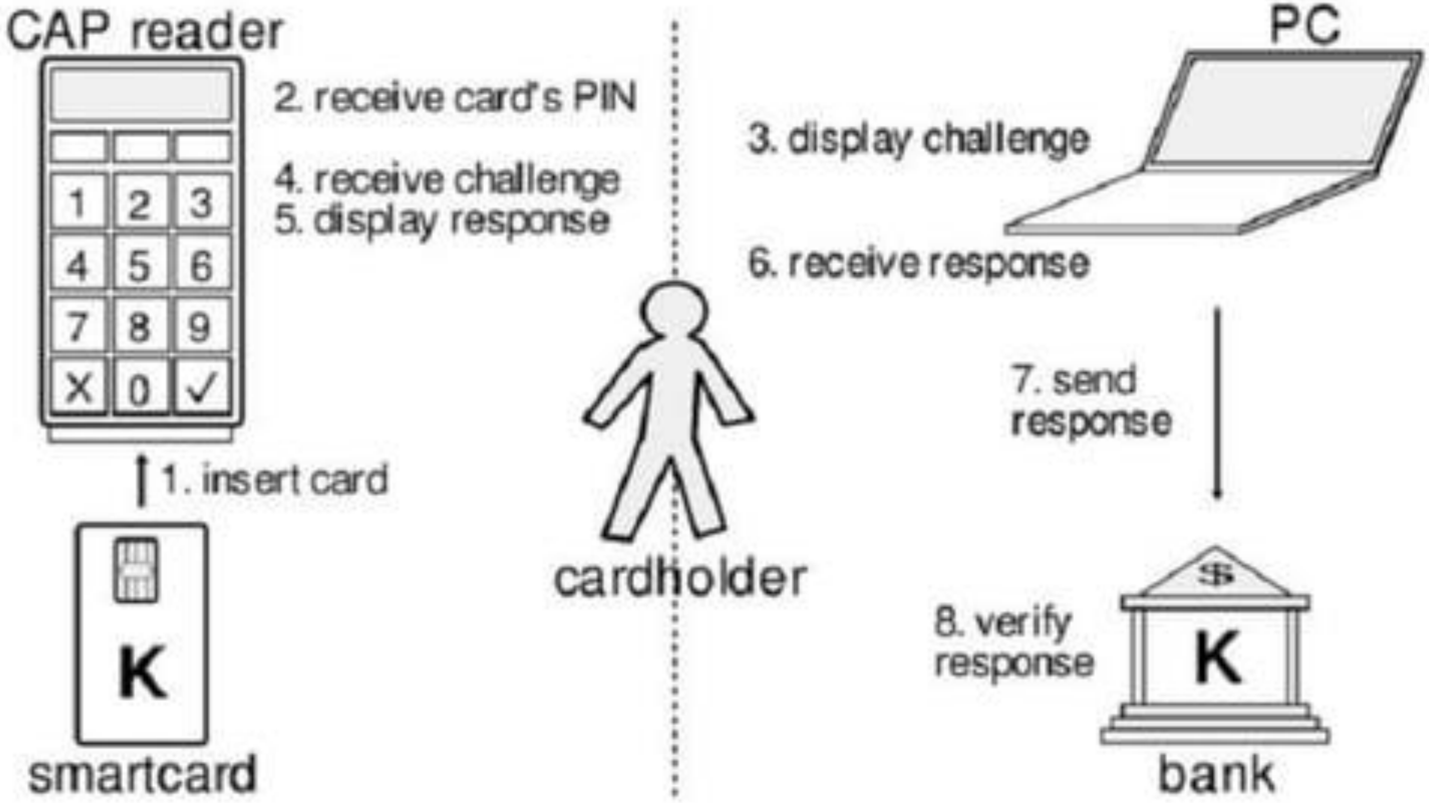
RSA SecurID

- This scheme basically works very similar to the identify-mode of CAP.
- The 6 to 8-digit response of the SecurID tokens is computed over the PIN,the present time and a 128 bit key, which is unique to every token, using a variant of the AES algorithm.

Open Authentication (OATH)

- The open authentication initiative is an attempt at developing an open standard for 2-factor authentication which should provide means for federated authentication systems like OpenID.
- The core of OATH is the HOTP-algorithm, which provides the OTP component.

Response-mode of the CAP-protocol



Outlook / Thesis

Personal Risk Management!

- How do we manage our personal financial risk?
  - Only as much money we need at home or in the wallet
  - Different bank accounts for different purposes
  - Limits on bank accounts or ATM cards
  - Insurances for damages we can not afford
- Applied to eBanking
  - Only required amount of money accessible by eBanking
  - Move savings to other accounts / banks
  - Set limit in payment height per month
  - Insurance for eBanking losses?

ELECTRONIC BANKING

Electronic banking has many names like e banking, virtual banking, online banking, or internet banking. It is simply the use of electronic and telecommunications network for delivering various banking products and services. Through e-banking, a customer can access his account and conduct many transactions using his computer or mobile phone.

E-BANKING TOOLS

1. Centralized Online Real Time Electronic Banking (CORE)
2. Electronic Clearing Service (ECS)
3. Electronic Fund Transfer (EFT)
4. Real Time Gross Settlement (RTGS)
5. National Electronic Fund Transfer (NEFT)
6. Society for Worldwide Interbank Financial Telecommunications (SWIFT)
7. E-Cheque
8. Any Time Money - ATMs
9. Credit Cards, Debit Cards, Smart Cards
10. Internet Banking
11. Phone Banking
12. Mobile Banking

ELECTRONIC CLEARING SERVICE (ECS)

It is a mode of electronic funds transfer from one bank account to another bank account using the services of a Clearing House.

It is generally used for bulk transfers performed by institutions for making payments like dividend, interest, salary, pension, etc. ECS can also be used to pay bills and other charges such as payments to utility companies such as telephone, electricity, water, or for making equated monthly instalments payments on loans as well as investments.

ECS Credit is used for affording credit to a large number of beneficiaries by raising a single debit to an account, such as dividend, interest or salary payment.

ECS debit is used for raising debits to a number of accounts of consumers or account holders for affording a single credit to a particular institution. Eg. utility payments like electricity bills and telephone bills.

ANY TIME MONEY – ATM

The Full form of ATM is Automated Teller Machine. ATM is an electro-mechanical machine that is used for making financial transactions from a bank account. These machines are used to withdraw money from personal bank accounts. Many ATMs have a sign above them indicating the name of the bank or organisation that owns the ATM, and possibly including the networks to which it can connect

Customers are typically identified by inserting a plastic ATM card into the ATM, with authentication being by the customer entering a personal identification number (PIN), which must match the PIN stored in the chip on the card, or in the issuing financial institution's database.

SMART CARDS

A smart card is any plastic card that has a built in chip and is able to process financial transactions.. A smart card, chip card, or integrated circuit card (ICC) is a physical electronic authorization device, used to control access to a resource. It is typically a plastic credit card sized card with an embedded integrated circuit. Many smart cards include a pattern of metal contacts to electrically connect to the internal chip. Others are contactless, and some are both. Smart cards can provide personal identification, authentication, data storage, and application processing. Applications include identification, financial, mobile phones (SIM), public transit, computer security, schools, and healthcare. Smart cards may provide strong security authentication for single sign-on (SSO) within organizations. Several nations have deployed smart cards throughout their populations.

Smart Card is a technology, while Debit Card is a financial instrument

DEBIT CARDS

A Debit card is a plastic card which provides an alternative payment method to cash when making purchases. Functionally, it can be called an electronic check, as the funds are withdrawn directly from either the bank account, or from the remaining balance on the card.

A debit card is a payment card that deducts money directly from a consumer's checking account to pay for a purchase. Debit cards eliminate the need to carry cash or physical checks to make purchases.

CREDIT CARDS

A credit card is a valuable financial tool that enables cardholders to make purchases on credit. From paying utility bills to online shopping, buying home appliances, groceries, and much more, a credit card helps you cover all your expenses easily.

A credit card is a payment card issued to users (cardholders) to enable the cardholder to pay a merchant for goods and services based on the cardholder's promise to the card issuer to pay them for the amounts plus the other agreed charges. The card issuer (usually a bank) creates a revolving account and grants a line of credit to the cardholder, from which the cardholder can borrow money for payment to a merchant or as a cash advance

CENTRALIZED ONLINE REAL TIME ELECTRONIC BANKING (CORE)

Core banking is a banking service provided by a group of networked bank branches where customers may access their bank account and perform basic transactions from any of the member branch offices.

It is often associated with retail banking and many banks treat the retail customers as their core banking customers. Core banking covers basic depositing and lending of money.

Core banking functions will include transaction accounts, loans, mortgages and payments. Banks make these services available across multiple channels like automated teller machines, Internet banking, mobile banking and branches.

Banking software and network technology allows a bank to centralise its record keeping and allow access from any location.

CLEARING HOUSE

A clearing house is a financial institution formed to facilitate the exchange (i.e., clearance) of payments, securities, or derivatives transactions. The clearing house stands between two clearing firms (also known as member firms or participants). Its purpose is to reduce the risk of a member firm failing to honor its trade settlement obligations.

In acting as the middleman, a clearing house provides the security and efficiency that is integral for financial market stability.

ELECTRONIC FUND TRANSFER (EFT)

Electronic funds transfer (EFT) are electronic transfer of money from one bank account to another, either within a single financial institution or across multiple institutions, via computer-based systems, without the direct intervention of bank staff.

EFTs include, but are not limited to:

1. Automated teller machine (ATM) transfers;
2. Direct deposit payment or withdrawals of funds initiated by the payer
3. Direct debit payments for which a business debits the consumer's bank accounts for payment for goods or services;
4. Transfers initiated by telephone
5. Transfers resulting from credit or debit card transactions, whether or not initiated through a payment terminal.
6. Wire transfer via an international banking network such as swift
7. Electronic bill payment in online banking, which may be delivered by EFT or paper check
8. Transactions involving stored value of electronic money, possibly in a private currency;
9. Instant payment.

NEFT (NATIONAL ELECTRONIC FUND TRANSFER)

The National Electronic Fund Transfer or NEFT is the simplest and most liked form of money transfer from one bank to bank. To make any NEFT transaction, you just need two important pieces of information -- firstly, account number and secondly, the IFSC Code of the destination account.

In NEFT, there is no cap on the amount of money that can be transferred. However, individual banks may set a limit.

Steps for a NEFT money transfer

Step 1: Go to Fund Transfer tab, and select 'Transfer to other bank' (NEFT)
Step 2: Select the recipient account and enter the relevant details
Step 3: Accept the (Terms and Conditions)
Step 4: Recheck the details, if all and complete the process

REAL TIME GROSS SETTLEMENT (RTGS)

RTGS is almost similar to NEFT but the minimum payment and how it credits to the destination account differs. There is no upper cap on the amount. An RTGS money transfer happens on a real-time basis. The bank of the person to whom the money is transferred gets 30 minutes to credit it to his/her account.

It is the continuous process of settling payments on an individual order basis without netting debits with credits across the books of a central bank (e.g., bundling transactions). Once completed, real-time gross settlement payments are final and irrevocable.

The fundamental difference between RTGS and NEFT, is that while RTGS is based on gross settlement, NEFT is based on net-settlement. Gross settlement is where a transaction is completed on a one-to-one basis without bunching with other transactions. Usually RTGS costs more than NEFT Transactions.

IMPS (IMMEDIATE PAYMENT SERVICE)

Immediate Payment Service or IMPs an instant fund transfer service and it can be used anytime. IMPS can be simply defined as NEFT+RTGS.

In order to avoid fraud complaints, the cap on transaction limit is set very low.

SOCIETY FOR WORLDWIDE INTERBANK FINANCIAL TELECOMMUNICATIONS (SWIFT)

The Society for Worldwide Interbank Financial Telecommunication (SWIFT), legally S.W.I.F.T. SCRL, provides a network that enables financial institutions worldwide to send and receive information about financial transactions in a secure, standardized and reliable environment. SWIFT is a vast messaging network used by banks and other financial institutions to quickly, accurately, and securely send and receive information, such as money transfer instructions.

SWIFT assigns each financial organization a unique code that has either eight characters or 11 characters. The code is interchangeably called the bank identifier code (BIC), SWIFT code, SWIFT ID, or ISO 9362 code.

SWIFT is only a messaging system – SWIFT does not hold any funds or securities, nor does it manage client accounts.

E-CHEQUE

An electronic check, also referred to as an e-check, is a form of payment made via the Internet, or another data network, designed to perform the same function as a conventional paper check. Since the check is in an electronic format, it can be processed in fewer steps.

The electronic cheques are modeled on paper checks, except that they are initiated electronically. They use digital signatures for signing and endorsing and require the use of digital certificates to authenticate the payer, the payer's bank and bank account. They are delivered either by direct transmission using telephone lines or by public networks such as the Internet.

INTERNET BANKING

Online banking, also known as internet banking, is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website. The online banking system will typically connect to or be part of the core banking system operated by a bank and is in contrast to branch banking which was the traditional way customers accessed banking services.

Some banks operate as a "direct bank" (or “virtual bank”), where they rely completely on internet banking.

Internet banking software provides personal and corporate banking services offering features such as viewing account balances, obtaining statements, checking recent transaction and making payments.

PHONE BANKING

Telephone banking is a service provided by a bank or other financial institution, that enables customers to perform over the telephone a range of financial transactions which do not involve cash or Financial instruments (such as cheques), without the need to visit a bank branch or ATM.

Telephone banking times are usually longer than branch opening times, and some financial institutions offer the service on a 24-hour basis. However, some banks impose restrictions on which accounts may be accessed through telephone banking and usually limit the amounts that can be transacted

MOBILE BANKING

Mobile banking is a service provided by a bank or other financial institution that allows its customers to conduct financial transactions remotely using a mobile device such as a smartphone or tablet. Unlike the related internet banking it uses software, usually called an app, provided by the financial institution for the purpose. Mobile banking is usually available on a 24-hour basis. Some financial institutions have restrictions on which accounts may be accessed through mobile banking, as well as a limit on the amount that can be transacted. Mobile banking is dependent on the availability of an internet or data connection to the mobile device.

Transactions through mobile banking depend on the features of the mobile banking app provided and typically includes obtaining account balances and lists of latest transactions