UNIT-V System Security

Internet Security:

Security threats goes on emerging in Internet world due to mobile codes (software agents or rogue software) which are responsible to create virus threat

Mobile codes is software agent which have ability to move from one computer to other and also have ability to get themselves invoked without the external influence

Threats are divided in major two categories

1. Threat to the local computing Environment
2. Access control and threat to the server

Security threats arise when downloaded data is passes through local interpreter on client machine without users knowledge. Client threats arises mostly due to malicious code refers to viruses like Trojan horse, worms rabbits, chameleon, ordinary software bombs, timed software bombs and logical software bombs

Threats to Server:

Threats to server consist of

1. Unauthorized modification of server
2. Unauthorized modification of incoming data packets by exploiting the bug in server software
3. Server can be attacked by denial of service where intruder make system unusable by destroying resources so that they can be used

Most common form of denial of service attacks is service overloading and message overloading

Service Overloading:

Servers are vulnerable to service overloading for ex we can easily overload www server by writing small loop that send request continuously for a particular file to server. Server tries to respond as it assumes the request is genuine one Hence while providing services to all the request a stage will reach when server is not able to satisfy the need or request so it deny for providing services to the request i.e. Denial of service will occur due to overloading of the server

Message Overloading:

Message overloading will occur when someone sends a very large file to the message box of sever at every few seconds. Due to of which message box grows in size and begins to occupy the hard disk space and increases they no of receiving processes on recipient machine and thereby causes disk crash

Virus: -

- A small program written to alter the way a computer operates, without the permission or knowledge of the user. A virus must execute and replicate itself.

- Program that replicates itself so as to infect more computers

- A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are manmade.

- A computer program written by a smart person who chooses to be an idiot. (e-mail signature file)

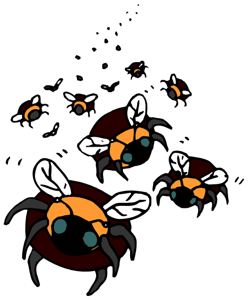
- Computer "Viruses" and related programs have the ability to replicate themselves on an ever increasing number of computers. They originally spread by people sharing floppy disks. Now they spread primarily over the Internet (a "Worm").

- Other "Malicious Programs" may be installed by hand on a single machine. They may also be built into widely distributed commercial software packages. These are very hard to detect before the payload activates (Trojan Horses, Trap Doors, and Logic Bombs).

Ways Viruses Are Transmitted

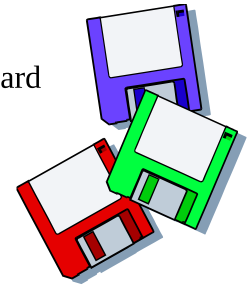
- Software (floppy disks and CDs)
- E-mail

7 Types of Viruses



- File infector viruses
- Boot sector viruses
- Master boot record viruses
- Multi-partite viruses
- Macro viruses
- Script viruses
- Companion viruses

File Infector Viruses



- Infect program files.
- Can infect other files when infected program is run from floppy, hard drive, or network.
- Many are memory resident.
- After memory is infected, any non-infected executable that runs becomes infected.
  Examples: Jerusalem and cascade

Boot Sector Viruses

- Infect the system area of a disk. (boot record on floppy/hard disks)
- Activated when user starts up from infected disk.
- Always memory resident in nature.
- Once in memory, all non-write protected floppy disks will become infected when accessed.
- Examples: Form, Disk Killer, Michelangelo, and Stoned

Master Boot Record Viruses

- Similar to boot sector virus except viral code is located in different area.
- Prevents computer from booting.
- Examples: NYB, AntiExe, and unashamed (Symantec.com)

Multi-Partite Viruses

- Infect boot records and program files.
- Difficult to repair.
- Boot area and files must both be cleaned of virus or re-infection will occur.
- Examples: One Half, Emperor, Anthrax, and Tequila
- Macro Viruses
- Most common type of virus.
- Infect data files – word, excel, power point and access files.
- Use another program's internal programming language which was created to allow users to automate certain tasks within that program.
- Examples:w97m.Melissa, WM.NiceDay, and W97M.Groov
- Script Viruses
- Infect various script languages such as DOS, Java Script, and Visual Basic Script.

Companion Viruses

- Execute through operating system rather than directly infecting programs or boot sectors.
- When you execute the command 'ABC', ABC.COM executes before ABC.EXE Thus, a companion virus could place its code in a COM file with its first name matching that of an existing EXE file. When the user next executed the 'ABC' command, the virus' ABC.COM program would be run.

- **Executable Viruses** - These are viruses hidden within executable files or posing as executable files.
- **Visual Basic Script Viruses -** Visual Basic Script (VBS) is a powerful programming language built into Windows. VBS viruses can send emails, delete files, rename files etc. VBS viruses often pretend to be something that they are not.
- **Boot Sector Virus -** resides in the boot sector of a hard disk or floppy. The boot sector is that portion of a disk that gives it its identity. After a given number of boots, the virus activates and the system is usually destroyed.

- **Stealth Virus -** Can be any one of the previously mentioned types, but were designed to defeat anti-viral scanning and other anti-viral detection software and methods.

- **Macro Viruses – These** are very common and make use of the macro functionality in Microsoft Office. Macros are mini-programs that allow users to automate various commands within the program.

Other Threats to Computers

Worm

- Self-replicating program that are self contained and doesn't require host program. It creates copies of itself and executes them and generally it utilizes the network services to propagate to other host system. They will consume all resources on network and affects response time

- A program or algorithm at replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down.
- A virus that spreads by creating duplicates of itself on other drives, systems, or networks**.**
- Worms – spreads by creating duplicates of itself on other drives, systems, or networks

Rabbits

- Rabbits are similar to worms they too are full programs. However as soon as they are executed they are replicating themselves on the disk until its capacity is exhausted this process is then repeated on other nodes so that complete network comes to stand still.

- Rabbits are less harmful as compared to worms since they are easily detected.

Trojan Horse

- Program which appears to be harmless but has piece of code which is very harmful . Trojan horse is derived from the greek mythology Trojan horse here means to fool the common users , Hence all the rogue s/w delivered comes under this category
- The term comes from a story in Homer's Iliad, in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering. But after the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture Troy

- A destructive program that masquerades as a good/useful application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive.

- One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

Ordinary Software bombs:

S/w bombs are the piece of code segment, which “explodes” as soon as it executed without any delay and brings system to grinding halt

Timed Software bombs:

Similar to ordinary software bomb except that it becomes active only at specific time or frequency

Logical Software bombs:

Similar to ordinary software bomb , except its activated only if the logical condition is satisfied(e.g. Delete employees master data when gross salary exceeds say 10,000)

Chameleon:

Are similar to Trojan horses It normally seems like a useful and correct program and throws a logon screen to collect all the valid user names and passwords and then display a message system shut down and then it makes the utilization of collected password later on

Backdoor

- Also called a *trapdoor*. An undocumented way of gaining access to a program, online service or an entire computer system. The backdoor is written by the programmer who creates the code for the program. It is often only known by the programmer. A backdoor is a potential security risk.

Malware

- Short for malicious software. Software designed specifically to damage or disrupt a system, such as a virus or a Trojan Horse.

Spyware

- Also called *adware*, spyware is any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes.

- Spyware applications are typical bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet.

- Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else.

- Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.

- Spyware is similar to a Trojan horse in that users unwittingly install the product when they install something else.

- Aside from the questions of ethics and privacy, spyware steals from the user by using the computer's memory resources and also by eating bandwidth as it sends information back to the spyware's home base via the user's Internet connection.

- Because spyware is using memory and system resources, the applications running in the background can lead to system crashes or general system instability.

Top Ten Viruses as of 05-23-2002

TrendMicro	Sophos	McAfee	MessageLabs
• WORM_KLEZ.H • PE_FUNLOVE.4099 • PE_ELKERN.D • WORM_KLEZ.E • PE_NIMDA.A • JS_EXCEPTION.GEN • WORM_SIRCAM.A • PE_MAGISTR.B • PE_NIMDA.E • WORM_HYBRIS.M	• W32/Klez-G • W32/Klez-E • W32/Badtrans-B • W32/ElKern-C • W32/Magistr-B • W32/Klez-A • W32/MyLife-F • W32/Magistr-A • W32/Sircam-A • W32/Nimda-D	• W95/Elkern.cav.c • W32/Nimda.eml • W32/Klez.e@MM • W32/Nimda.gen@MM • JS/IEStart.gen • VBS/Loveletter@MM • JS/NoClose • VBS/Haptime@MM • W32/Klez.gen@MM • JS/Kak@M	• W32/Klez.H-mm • W32/Klez.E-mm • W32/SirCam.A-mm • W32/Magistr.B-mm • W32/Magistr.A-mm • W32/Hybris.B-mm • EML/Fortnight • W32/BadTrans.B-mm • W32/Yaha.C-mm

The Rogue's Gallery
Some of our more common and infamous viruses.

Klez
http://www.virus.uga.edu/klezalrt.html

- **What does it do?**

– The Klez virus propagates by taking a randomly picked e-mail address from web pages, ICQ databases or Windows Address Books and inserts it as the From: address before sending out its payload to the rest of your address book. When you receive an e-mail from someone whose computer is infected, it may appear to come from an entirely different person.

Klez

- **What does it do? (cont.)**

– This means that the e-mail address in the From: field of the infected e-mail you receive is probably not infected with the virus. The From: e-mail address happens to be in the infected machine's address book.

Klez

- **What else does it do?**

– The virus can infect personal documents and send them out to others and, therefore, possibly send out confidential information.

Sircam
http://www.virus.uga.edu/scalrt.html

- **What does it do?**

– Sircam is a mass mailing e-mail worm with the ability of spreading through Windows Network shares. It sends e-mails with variable user names and subject fields, and attaches user documents with double extensions to them.

– Since the worm can pick any of the user's personal documents it might send out confidential information.

– When a Sircam-infected e-mail attachment is opened it shows the document it picked up from the sender's machine. The file is displayed with the appropriate program according to its extension. This is so the recipient is unaware of virus infecting his machine.

- **How Does It Spread?**

– The worm uses Windows Address Book, which is used by both the Outlook and Outlook Express e-mail clients to collect e-mail addresses. The worm also tries to look for e-mail addresses in the *\Windows\Temporary Internet Files* folder, which is where Internet Explorer and other programs store temporary copies of downloaded web pages and other Internet files.

Nimda
http://www.f-secure.com/v-descs/nimda.shtml

- **What does it do?**

– Nimda is a complex virus with a mass mailing worm component which spreads itself in attachments named README.EXE. If affects Windows 95, Windows 98, Windows Me, Windows NT 4 and Windows 2000 users.

– It uses normal end user machines to scan for vulnerable web sites. It is looking for the **Unicode exploit to** infect IIS web servers.

– The actual lifecycle of Nimda can be split to four parts: 1) Infecting files, 2) Mass mailing, 3) Web worm and 4) LAN propagation.

- **How does it spread?**

– Infecting files

- Nimda locates EXE files from the local machine and infects them. These files then spread the infection when people exchange programs.

Nimda

– Mass mailing

- It then locates e-mail addresses from your e-mail client as well as searching local HTML files for additional addresses. Then it sends one e-mail to each address. These mails contain an attachment called README.EXE, which might be executed automatically on some systems.

– Web worm

- Nimda starts to scan the internet, trying to locate web servers. Once a web server is found, the worm tries to infect it by using several known security holes. If this succeeds, the worm will modify random web pages on the site, which if viewed may infect the web surfer's computer.

Hybris
http://www.fsecure.com/v-descs/hybris.shtml

- **What does it do?**

– Hybris is an Internet worm that spreads itself as an attachment to e-mail messages.

– It can upgrade itself via the Internet.

– Depending on the installed plugins, it can:

- Infect all ZIP and RAR archives on all available drives. The worm renames EXE files in archive with .EX$ extension and add its copy with .EXE extension to the archive.
- Infect DOS and Windows executable files (*.exe) files. The worm changes them so that they become droppers. When run, they copy worm's EXE file to TEMP directory and execute it.
- Depending on system date and time, a "spiral" effect is shown on the Windows Desktop.

- **How does it spread?**

– The worm intercepts Windows functions that establishes network connections, including those to the Internet. It reads the data that is sent and received, looking for e-mail addresses. When an address is found, the worm waits and then sends an infected message to each person.

Magistr
http://www.fsecure.com/v-descs/magistr.shtml

- **What does it do?**

– Magistr is a very dangerous memory resident worm combined with virus infection routines.

– The virus has an extremely dangerous payload, and depending on different conditions it erases hard drive data, CMOS memory and Flash Bios contents.

– When the virus is run (from infected message for example, if a user clicks on it installs itself to the Windows memory, then runs in background, sleeps for a few minutes and run its routines: local and network EXE file infection, e-mail spreading, etc.

Magistr

– Depending on its internal counters the virus manifests itself: it gets access to Windows desktop and does not allow access to icons on the desktop by mouse. When mouse cursor is moved to an icon, the virus moves the icon out of the cursor. It looks like desktop icons try to "escape" mouse cursor.

- **How does it spread?**

– Magistr virus spreads via Internet with infected emails, infects Windows executable files on a infected machine (local machine) and is able to spread itself over a local network.

- Mass mailing:

– To send infected emails, the virus reads the settings of installed e-mail client settings--Outlook Express Netscape Messenger Internet Mail & News

– The virus then scans email database files of those clients, gets e-mail addresses from there and sends itself to those addresses.

- The attachment name is variable, it can have an EXE or SCR extension. The virus looks on the system for an EXE file, infects it and attaches it to the message.

– The Subject and Body are randomly constructed from words and sentences that are found in .DOC and .TXT files in the system (the virus also scans local drives for these files and get texts from there).

How big is the virus problem?
Should I really worry about it? Can it really happen to me?

YES!!!

- The number of known viruses surpassed 50,000 in August 2000. According to the anti-virus vendor, Sophos the number of new viruses discovered every month continues to rise.
- Virus trends between 1999 and 2001 illustrate the threat to an e-mail system.
- In 1999, 1 in 1400 e-mails contained a virus. In 2000, it was 1 in 700, and 1 in 300 this year. Message Labs, an anti-virus vendor that specializes in scanning e-mail, predicts that if trends continue that by 2008, 1 in 10 e-mails will contain a virus.
- There are 808 viruses listed on the May 2002 WildList and Supplemental list.
- For a virus to be considered “in the wild”, it must be spreading as a result of normal day-to-day operations on and between the computers of unsuspecting users.

How do I get a virus?
I know what they are, but how do they work?

Methods of Attack

- E-Mail Attachments
- Web Pages
- Open Network Shares (Peer to Peer Networking)
- Internet Relay Chat & Instant Messaging
- Floppy Disks
- MS Office Document Macros
- Macromedia Flash Documents
- And, new ways appearing all the time…

How do I protect myself from viruses?

How can I avoid this agony?

Steps to Protect Yourself

- Be paranoid.
- According to Murphy’s law--"If anything can go wrong, it will“
- In computing, this is not as far from the truth as you might hope.
- Make sure you have an up to date anti-virus package installed on your computer.
- EITS currently provides the F-Secure Anti-Virus package for UGA student, faculty, and staff use.
- It is available for download from the Anti-Virus @ UGA website: http://www.virus.uga.edu
- Do not open unexpected attachments.
- Increasingly, viruses are sent as attachments to e-mails. This is a particularly insidious method of transmission because often people will open attachments that have been sent by acquaintances, co-workers, or friends, only to find that the attachment is in fact a virus.
- Install patches for the software you use in a timely manner
- There are viruses that exploit 'holes' or vulnerabilities in operating systems and applications. Anti-virus programs are generally able to protect you from this kind of 'malware' even if you have not installed the appropriate patch for that vulnerability.
- It is recommended that you visit your software manufacturer's Web site regularly to download and install new patches in a timely fashion.
- From **http://online.securityfocus.com/infocus/1288**
- Always scan floppy disks and CDs for viruses before using them
- Despite the fact that approximately 85% of all registered cases of computer infection are transmitted through e-mail, we should not ignore the traditional transport for malware: the mobile media (diskettes, compact disks, etc.).
- Users should always check these external media for viruses before using it on their computers. It is a simple, straightforward procedure to scan a disk with an anti-virus program. It takes just a few seconds, and can save hours of aggravation.
- From **http://online.securityfocus.com/infocus/1288**
- Be careful with software, even from a credible source
- It is not just pirated software that may be infectious. Sometimes even licensed CDs with software from well-established, credible vendors may contain viruses. Also, software downloaded from the Internet may carry a virus.
- Another source of infection may be a computer that has been taken in for maintenance that may be returned to its owner with a hard drive that is infected with a virus.

- From http://online.securityfocus.com/infocus/1288

- Create a virus-free start-up disk for your computer and keep it in a safe place.
- Sometimes an infected computer cannot be started. This does not mean that a virus has deleted data from your hard drive; it only means that your operating system cannot be loaded any more.
- To solve this problem, you should use a virus-free start-up diskette containing an anti-virus program that has been developed for your operating system. This diskette will help you to start your computer and delete any viruses in your operating system.

- From http://online.securityfocus.com/infocus/1288
- Back up your files regularly.
- Although this rule will not protect against virus infection, it will allow you to protect your valuable data in case your computer becomes infected (or, as an added bonus, if you have any other problems with your hardware).
- It is advisable to back up your most valuable data using external media, such as diskettes, MO disks, magnetic tapes, CDs, etc. In this case, whatever might happen, you will always be prepared.

- From http://online.securityfocus.com/infocus/1288

- Make file extensions visible.
- It is safe to run non-executable file content, such as JPGs, MPGs, GIFs, WAVs, etc. You just need to make sure they aren't executables in disguise.
- Most Windows versions will hide known file extensions. Thus, a seemingly innocuously named file, *PICTURE.JPG*, may be *PICTURE.JPG.EXE*. In Windows Explorer, look for the file extension hiding option under Folder Options.

- From http://security.oreilly.com/news/maliciouscode_0801.html
- Don't share your hard drive (disable file sharing on your hard drive).
- If you do need to provide some file and print sharing, don't give the keys to the kingdom; use a password, and ONLY give the minimum that you have to a directory (folder) is much better than giving all of the C:\, read only is better than full access. If you have to give a C:\ administrative share, limit the number of people who can use it.

- There is a very simple way for Windows users to eliminate the threat of "accidentally" executing a VBS attachment to an e-mail.

- By doing the following steps, if you ever "accidentally" click on a worm or virus written in Visual Basic, it will pop open in notepad rather than executing.

[1] Go to any open Windows Explorer or File Manager window.

[2] On the pull-down menus select "Options" on the "View" pull-down.

[3] Select the "File Types" tab.

[4] Scroll down until you see the .vbs file type.

[5] For each of them, highlight the entry and select "Edit."

[6] Highlight "Open" and select "Edit."

[7] Change the "application use to perform action" from "wscript.exe" to the path name for where "notepad.exe" is located. This is likely either "C:windowsnotepad.exe" or "C:WINNTnotepad.exe." You can use the file find feature to locate the proper path.

[8] Once changed, click "OK" and "Close."

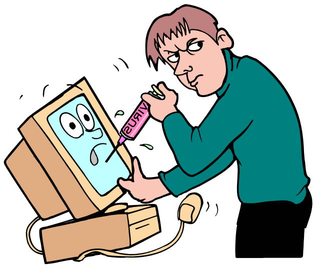
[9] Repeat for the .vbe file type.

Ways to Protect Your Computer From Viruses

- Install an anti-virus program.
- Remove disks from disk drive before shutting down/restarting computer.
- Be cautious of email attachments from unknown sources.
- Do not set your email program to auto-run attachments.
- Write protect floppy disks when finished.

Some Popular Antivirus Programs

- Norton Antivirus
- McAfee virus scan



FIREWALL

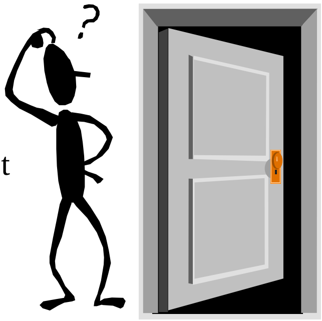
Every time corporate connects its Intranet to Internet and it faces potential danger, Due to the openness of Internet there is a possibility of attack by the hackers and Intruders to cause the harm to local computing Environment in no of ways like

- They can steal or damage the important data
- Damage individual computer or entire network
- Use the corporate 's computers resources

Solution for all such types of threats and many more to build a firewall to protect Intranet.

What is a firewall?

- **A firewall is any mechanism that acts to restrict access to a network *according to a set of defined rules*.**
- Function as "front doors" to a network.
- A firewall is combination of hardware and software and are build up by using routers, servers and variety of software's and are placed in between Internet & Intranet



A set of programs residing on a "gateway server" that

protect the resources of an internal network

- A network device or an host that connect 2 or more networks
- A device able to monitor each packet to determine whether to forward it toward its destination
- A device able to evaluates packets with the objective to Control, Modify and Filter network traffic

Advantages

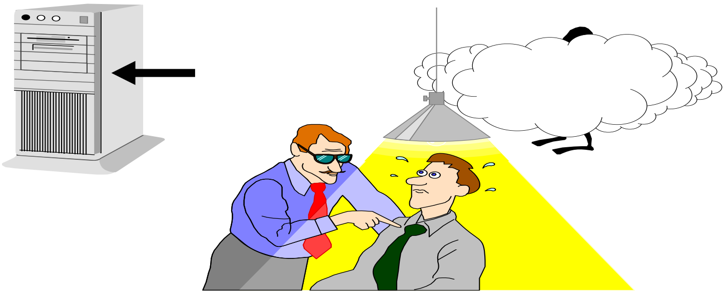
- Hiding network information
- application/content-level filtering
- fail over and load balancing features
- single-point of control (easy to control access)
- powerful logging features

Disadvantages

- increases the communication latency/delay
- proxy per application and no generic one
- client might need to be modified/reconfigured to use the proxy server
- connections which bypass firewall services through the firewall
- introduce vulnerabilities
- insiders can exercise internal vulnerabilities
- performance may suffer single point of failure

How do they work?

- By inspecting traffic that travels across/through them according to the policy that's been set.



How are they set up?

- Act as a go-between for any two given networks

- All traffic between external and internal networks must go through the firewall

- Firewall has opportunity to ensure that only suitable traffic goes back and forth

Firewall Architecture's

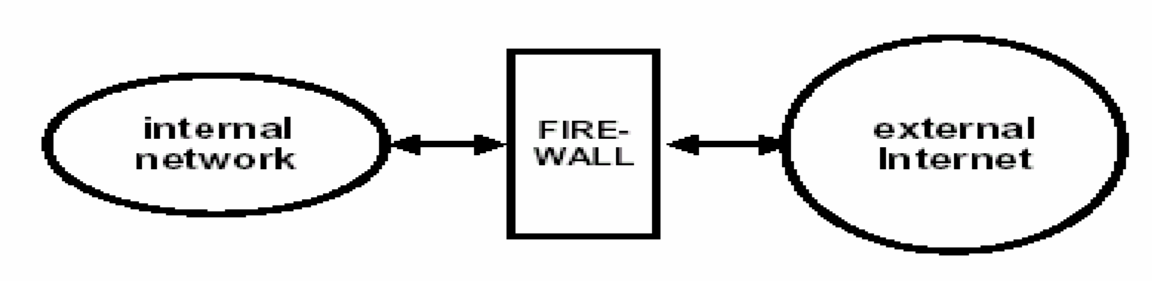
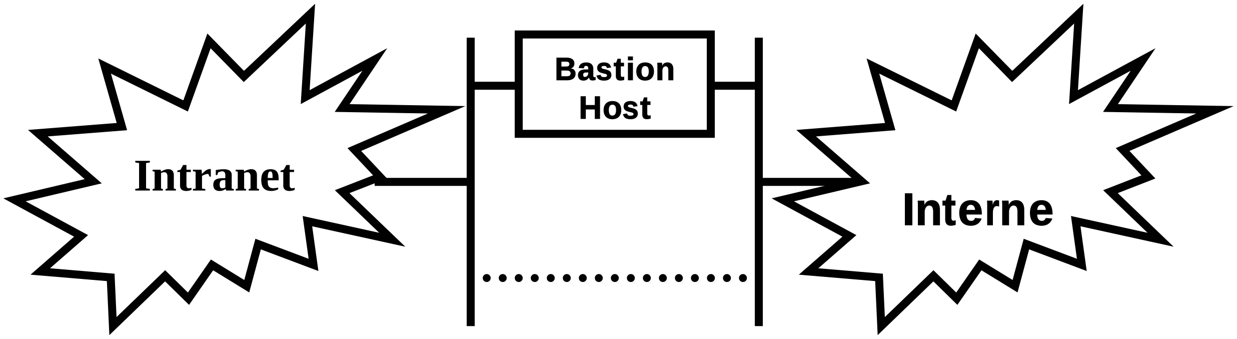
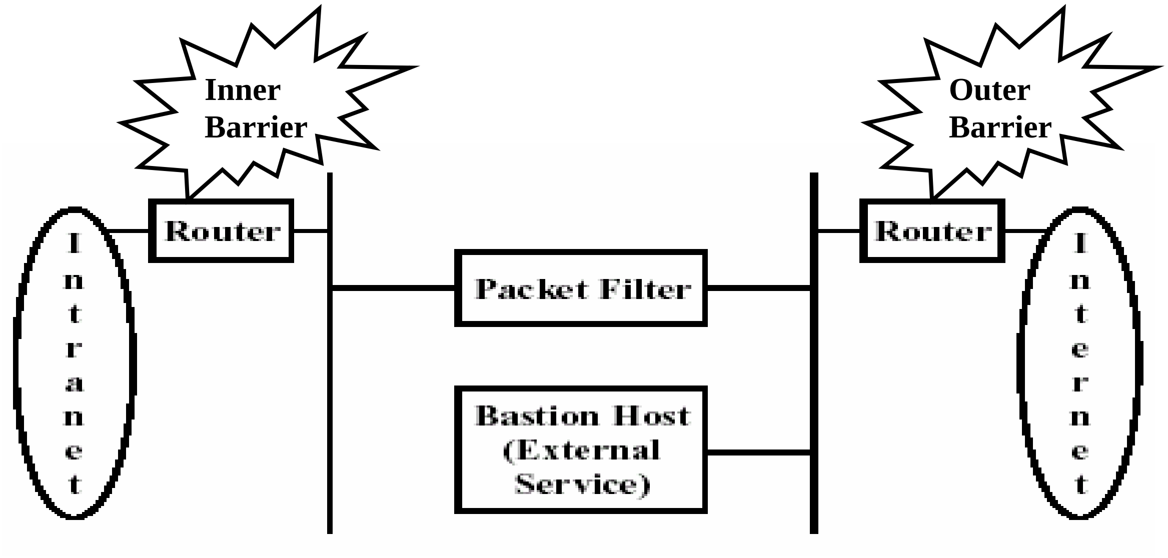
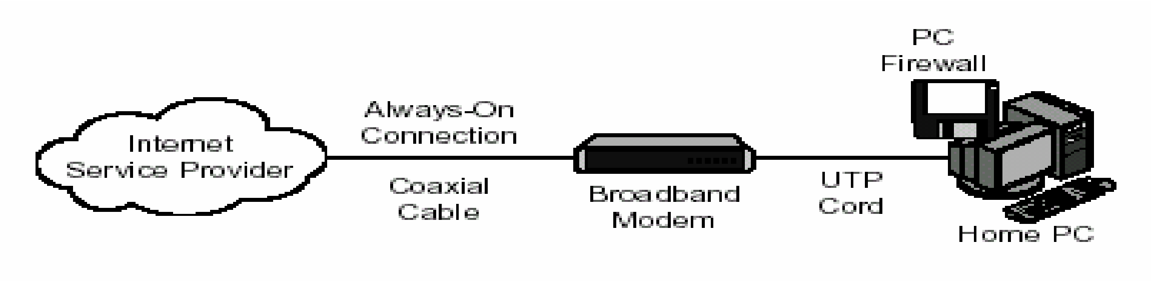


Fig : Shows Simple Firewall Architecture





Inner Barrier
Outer Barrier
Router
Router
Intranet
Internet
Packet Filter
Bastion Host (External Service)


Internet
Service Provider
Always-On
Connection
Coaxial
Cable
Broadband
Modem
UTP
Cord
PC
Firewall
Home PC

Requisites of Good Firewall Systems:

Requisites are totally depends on security requirements however one should check some attributes before commissioning any type of firewall system

- Firewall system should be able to support or deny services except those are specifically permitted
- Firewall system should posses flexibility i.e. it must have ability to new changes based on company's policy
- It should contain advanced authentication measures
- It should employ filtering techniques

Firewalls Rules

- Packet Filters/FW Rules: to implement the FW policy
- Questions to ask:
- Which services do want to offer on the network and in which direction?
- Do want to restrict user Internet access: which, what and when?
- Is there any trusted external hosts to which you want to give network access?
- Fields used to Filter Packets:
- IP headers: options, proto, src/dest IP,
- TCP and UDP: src/dest port, flags, SYN and ACK bits

Firewall Rules Basis

- Interface name (FW may have more than one incoming/outgoing link
- Interface or traffic direction
- Source and destination IP address: this includes broadcast and multicast addresses
- IP options : need to check this for source routing
- ICMP
- Transport Protocols: UDP, TCP, IPX, ..
- Well-know TCP/UDP Services: WEB, FTP .. etc
- More restricted rules comes first to avoid rules conflict and shadow

1. Permit ANY TCP incoming (more general)
2. Deny DestPort=25 TCP incoming (will be shadowed by 1)

PACKET FILTERING FIREWALLS

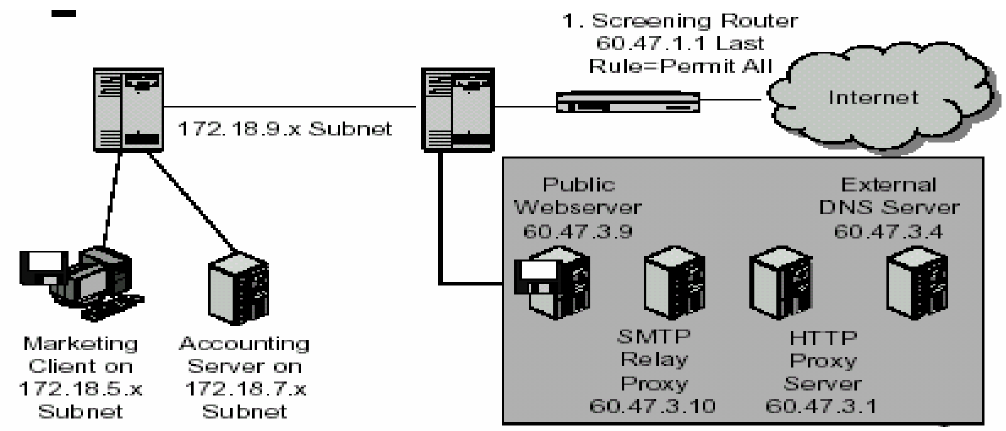
IP packet fitering firewall examines each and every incoming and outgoing packet flowing through it by examining the specific field in IP datagram headers, Firewall decides whether to allow the packet to come inside / go outside or discard the packet

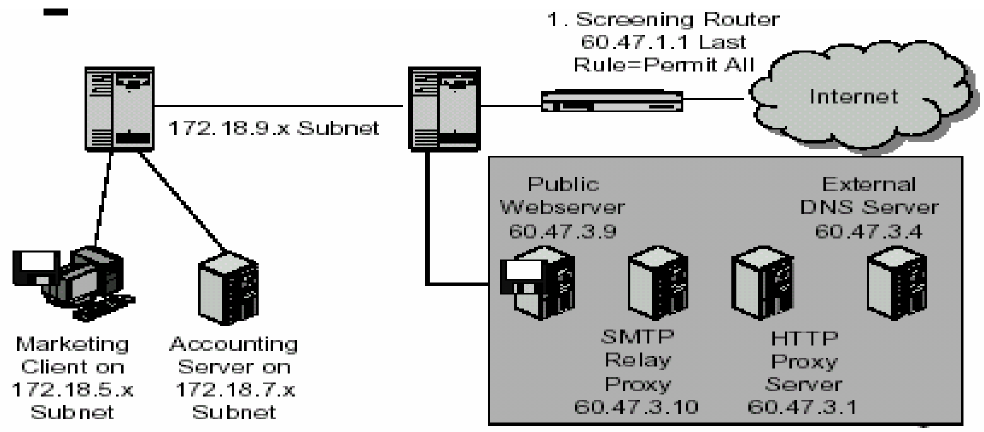
Key fields tested by the firewall are

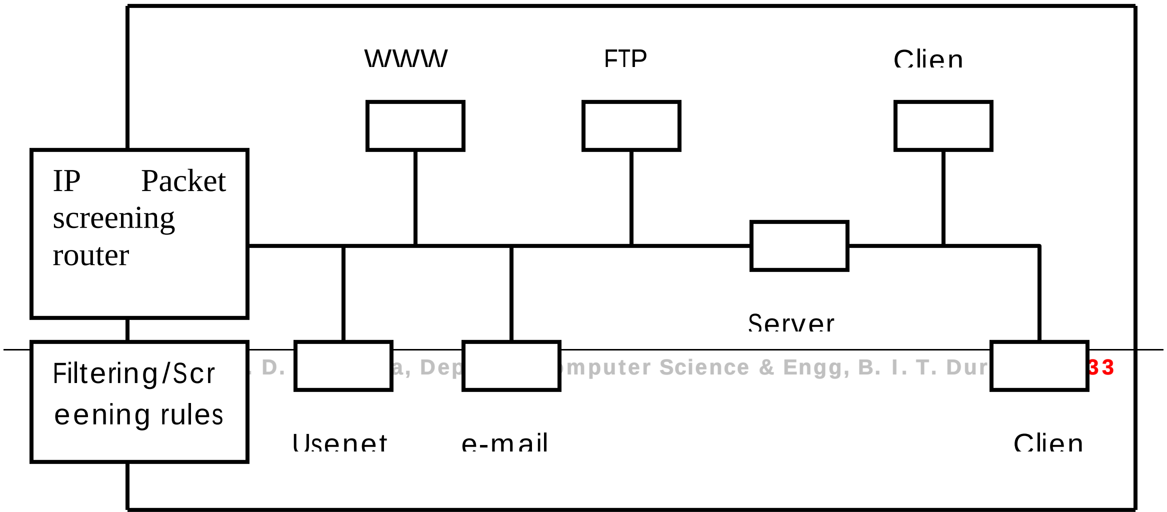
- Source Ip headers
- Destination IP headers
- TCP/UDP source port
- TCP/UDP destination port

Packet filtering firewalls

- Packet filtering firewalls decide whether or not to forward packets based on
  - source and destination IP addresses
  - protocol field
  - source and destination port numbers
  - SYN flag settings
- Rules dictate whether or not packets should be forwarded
- Inspects packets in isolation
- Does not keep track of connection state
- Susceptible to application layer attacks




1. Screening Router
60.47.1.1 Last
Rule=Permit All
Internet
172.18.9.x Subnet
Public
Webserver
60.47.3.9
External
DNS Server
60.47.3.4
SMTP
Relay
Proxy
60.47.3.10
HTTP
Proxy
Server
60.47.3.1
Marketing
Client on
172.18.5.x
Subnet
Accounting
Server on
172.18.7.x
Subnet


WWW
FTP
Clien
IP Packet screening router
Server
Filtering/Screening rules
Usenet
e-mail
Clien

As shown in above fig firewall router filters incoming and outgoing Packets based on the security rules that are set at the time of configuring the firewall host based on the company's policies

can do: allow incoming telnet from a particular host

cannot do: allow incoming telnet from a particular user

e.g. If company doesn't offer FTP services to outsiders then firewall is configured to reject the request related with FTP

An example: Ports >1024! (I)

Objective: allow a network application (based on sockets), to be accessible by hosts outside your local LAN:

- The software is made by a main process that receive connection requests on port 999.
- Then the main process create a new process for each new connection. New processes waits for client data on ports from 40001 to 41000.
- The main process send a reply to the client (in the payload of an UDP packet) with port to use to connect to the dedicate process
- The client receive the packet, read the port (ex:40001) and send the next packet to port 40001 of the same server
- A statless firewall REJECT the packet cause port>1024 are closed
- With a stateless firewall, if you want to allow your server to work properly with hosts outside your LAN you must open all port>1024
- A statfull Firewall allow to leave ports >1024 closed

Statefull vs. Stateless Firewalls

- Statless firewalls can make filter decision based only on:
    - source/destination addresses and ports
    - Statfull firewall associate a packet to a state and can make decision base on:
    - source/destination addresses and ports
    - state of the packet

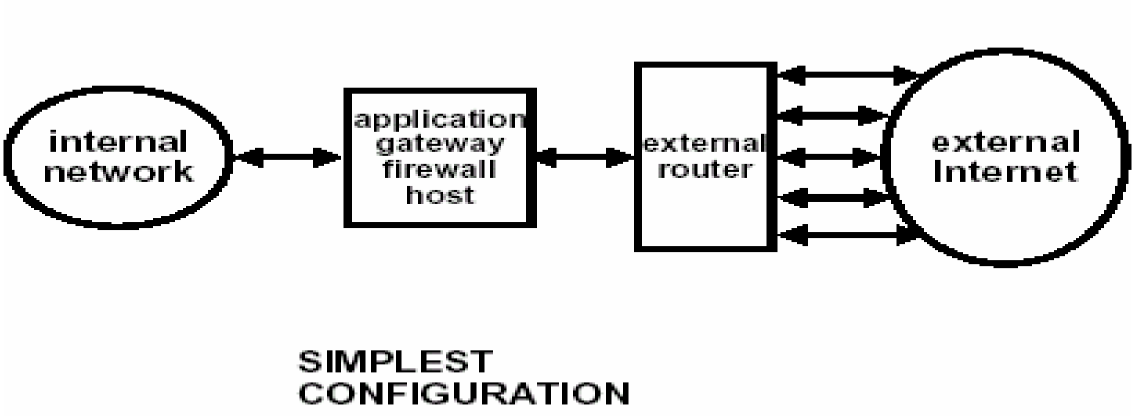
Drawbacks Of packet filtering firewall:

1. Packet filtering rules can be complex
2. Logging facility is not provided by such firewall
3. If TCP /UDP packet filtering is not implemented fully , it can lead to security hole
4. Can not handle RPC(Remote procedure calls)

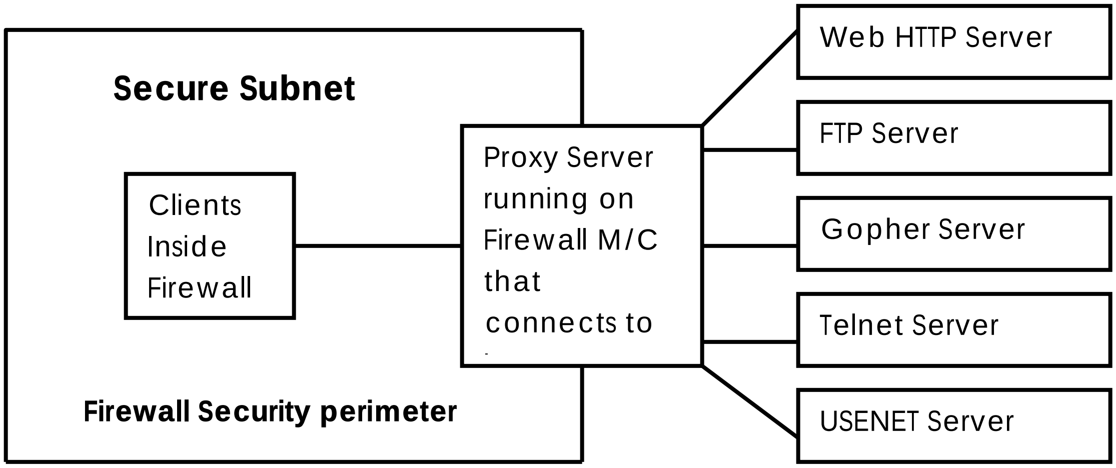
- Two *main* types of filtering firewall
    - Routing based filters
- From where did you come?
- Where are you going?
- Don't care what you do once you get there.
    - Content based filters
- What are you trying to do?
- Not *as* common as Routing based because it's harder to implement successfully

Proxy Application Gateways

In such type of firewall remote host or network can interact only with proxy server



(proxy application gateway) proxy server is responsible for hiding the details of the Internal network ie Intranet. If the remote host is interested to avail the facilities placed inside the company in that case first proxy authenticates remote host/user then it creates the session between application gateway and the Internal host and allows the transmission of packet as well maintain the log details of user too.



As shown in fig. Proxy application gateway is special server which runs on firewall machine and user ie inside or outside if they have to share the data in that case they have to divert the request to the proxy server proxy applies the security policy by authenticating the user and then maintains or establishes the session between the end users

Gopher: Is as server application that allows you to browse huge amount of information by performing remote logins and FTP

Advantages Of Application Gateways:

1. Proxy authenticates only those services for which it is configured /installed
2. Robust authentication and logging facility
3. Cost effectiveness
4. Less complex filtering rules

Hardened Firewall Hosts (HFH):

Hardened firewall hosts are similar to proxy application gateways and are configured for increased security . This type of firewall requires inside or outside user to connect to some trusted application running on firewall machine before getting connected furthur. *These firewalls are configured to protect against unauthorized interactive logins from the external world*

Steps required to setup HFH:

- Remove all users account except those are necessary for the operation of firewall machine
- Remove all noncrucial files and executables especially network server programs and client programs like FTP and Telnet
- Exten the feature of traffic logging and monitoring to check remote access
- Disable IP forwarding to prevent firewall to forward unauthorized packets

Advantages:

- Concentration of security
- Information hiding: Having ability to hide the company's Intranet
- Centralized and simplified network services management

Drawbacks:

- Concentrates security at one spot as apposed to distribute it among system
- S/w support is not enough as few vendors are offering HFH

AAA Security:

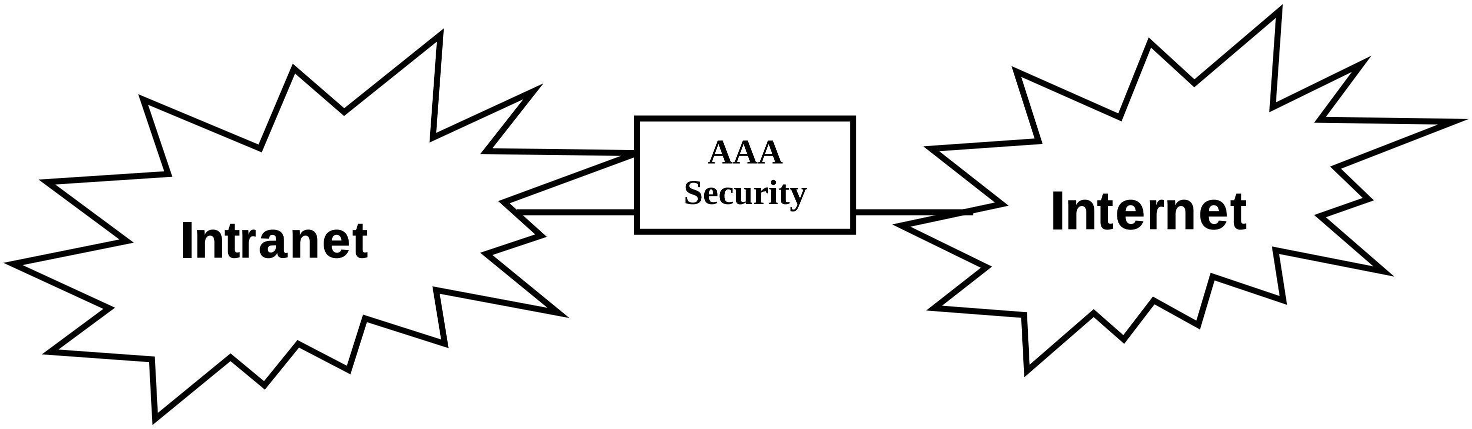


Fig : Shows AAA(Authentication Authorization and Accounting) Security

AAA Security works similar to Proxy application gateway in this too user must have to get himself authenticated by security system for availing the facilities that are kept inside or outside of the company ,ie its an compulsion over clients to get themselves logged on Security system and then only they would be authorized for availing facilities based on the policies set on the security system, after giving the authorization AAA system will maintain the details data packet transaction for the purpose of further accounting/auditing

- Two ways to approach the rule sets:
  - Allow all except what is defined as unwanted
    - Place roadblocks/watch gates along a wide open road.
  - Deny all except what is defined as wanted
    - Build a wall and carve paths for everyone you like.
- Problems:
  - Firewalls as filters can be considered for most part to be infallible... but as a security measure? They can only enforce rules (generally static)
  - **Crunchy on the outside, but soft and chewy on the inside."**

  - Conclusions
  - People don't just put up a thick front door for their sensitive belongings, you shouldn't for your network either.
  - Firewalls are an effective *start* to securing a network. Not a finish.
  - Care must be taken to construct an appropriate set of rules that will enforce your policy.

SET

(Secure Electronic Transaction)

Secure Electronic Transaction

- SET is open encryption & Security specification
- Designed for protecting credit card transaction
- Pioneered in 1996 by Master and Visa card jointly
- Master & Visa cards later joined by IBM, Microsoft, Netscape, RSA, Tersa and Verisign
- In 1998 First generation of SET compliant products appeared in market

SET …….

- SET is not payment system
- It is security protocol
- Enable user to employ existing payment infrastructure on Internet in Secure Manner

SET Services

- Provides secure communication channel among all parties in E-Com
- Provides authentication by use of digital certificates
- Ensures confidentiality by providing information to the parties involved in a transaction that too only when and where necessary

Summary of SET Participants

SET is having complex specification. when released it was of 971 pages so we see summary

1. Cardholder:Authorized holder of payment card such as master & Visa card
2. Merchant:Person or organisation that want to sell goods or services to card holder
3. Issuer:Is financial institution that provides payment card to cardholder

SET Participants ……………

4.Acquirer:Financial Institution that has relationship with merchant for processing payment cards,authorization & payments

5.Payment gateway:Payment gateway processes the payment messages on behalf of the merchant

Payment gateway acts as interface between SET and existing card payment network for payment authorization

SET Process

1. Customer opens an account: Customer opens credit card account with bank that support electronic paymet mechanism and SET Protocol
2. Customer receives certificate:After customers identity verification customer receives digital certificate from CA
3. Merchant receives a certificate:Merchant that want to receive a particular brand of card must posses digital certificate

SET Process….

4. Customer places an order: Typical shopping cart process and order placement. Merchant send back detail of purchase and total bill back to customer for his record

5. Merchant is verified:Merchant sends its digital certificate to customer to assure he is dealing with valid merchant

SET Process….

6. Order and payment details are sent:Customer sends both order and payment details to merchant along with digital certificate

7. Merchant Request Payment authorization: Merchant forwards payment details send by customer to payment gateway via acquirer with request to authorize the payment(To ensure validity and limit of credit)

SET Process….

8. Payment gateway authorizes the payment: Payment gateway verify the received details of customer credit card with issuer and either authorizes or rejects payment

9. Merchant Confirms the order :Assuming that the payment gateway authorizes the payment , the merchant sends a confirmation of the order to customer

SET Process….

10. Merchant provides goods or services:Merchant now ships the goods or provides the services as per customers order
11. Merchant requests Payment:Payment gateway receives request from the merchant for making payment

    Payment gateway interacts with financial institution such as issuer acquirer and clearing house to effect payment from customer to merchants account

How SET achieves its objective of Confidentiality

- Main concern In online transaction is merchant demand credit card no
- There are two aspect of above

1. Credit card no may travel in clear text format which provides intruder opportunity to know no and make misuse of it
2. Credit card no. can be available with the merchant who make the misuse of it

How SET achieves its objective of Confidentiality……….

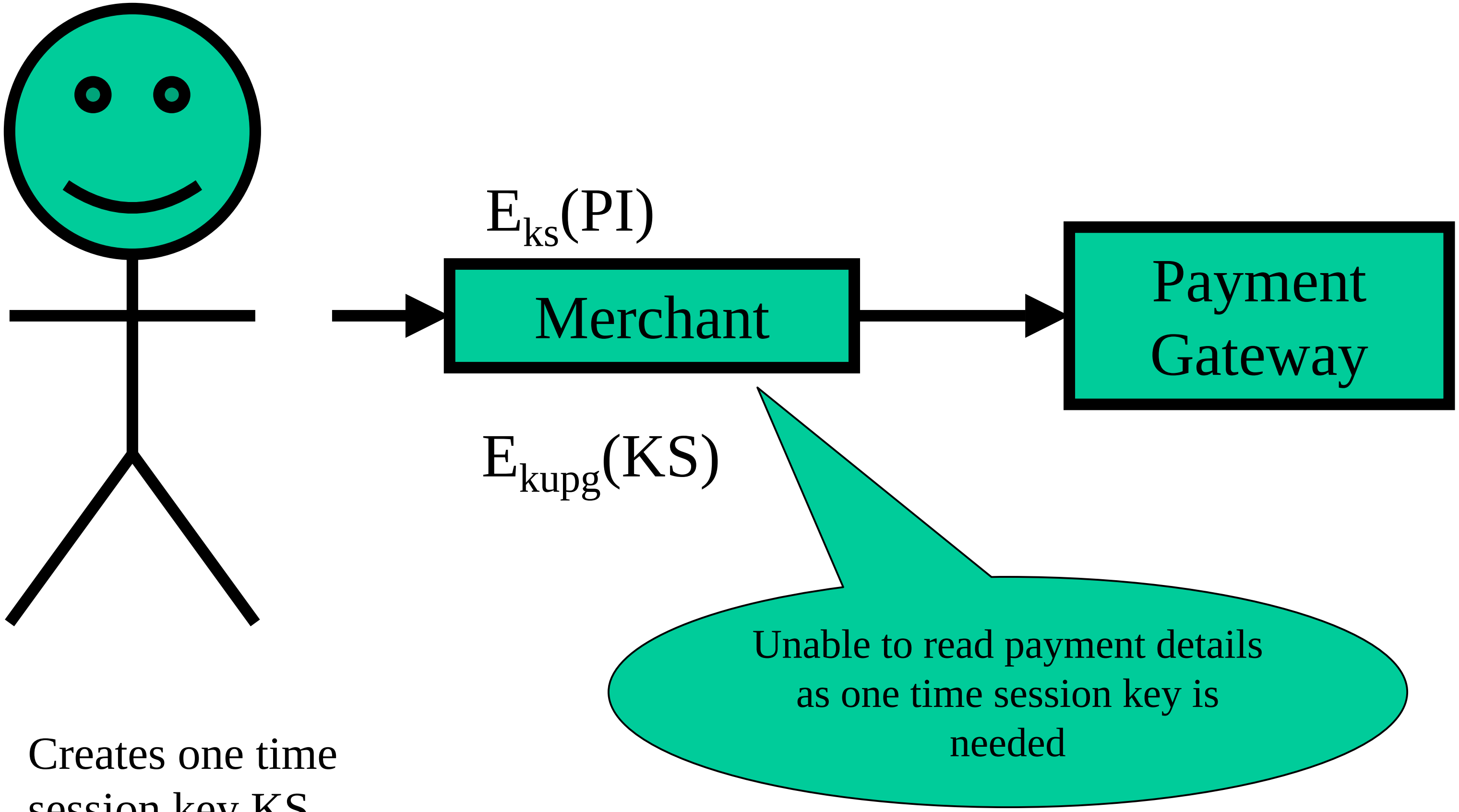
- First aspect dealt with SSL as all information exchange is done through SSL in encrypted format
- IInd aspect is important which is not achieved by SSL I.e. protection of credit card no. from merchant
- So SET is very important as it hides credit card details from merchant
- Concept of hiding credit card no from merchant is based on digital enveloping

Digital Enveloping in SET

- SET S/W prepare PI(Payment information) on card holders computer which contains credit card details
- Card holders computer now prepares one time session key
- Using one time session key card holders computer encrypts PI(Payment information)
- Now cardholders comp wraps one time session key with public key of payment gateway to form a digital envelope
- It then sends encrypted PI and digital envelope together to the merchant who pass it to gateway

Important points

- Merchant has access of encrypted PI so he can not read PI
- If he is interested to read PI it requires one time session key that was used to encrypt the payment information
- Interesting fact is one time session key itself is encrypted by public key of payment gateway to form digital envelope


$E_{ks}(PI)$
Merchant
Payment Gateway
$E_{kupg}(KS)$
Unable to read payment details as one time session key is needed

1. Creates one time session key KS
2. Encrypts PI with Ks
3. Encrypts Ks with public key of Payment gateway

SET Internals

Major transactions supported by SET are

1. Purchase request
2. Payment authorization
3. Payment capture

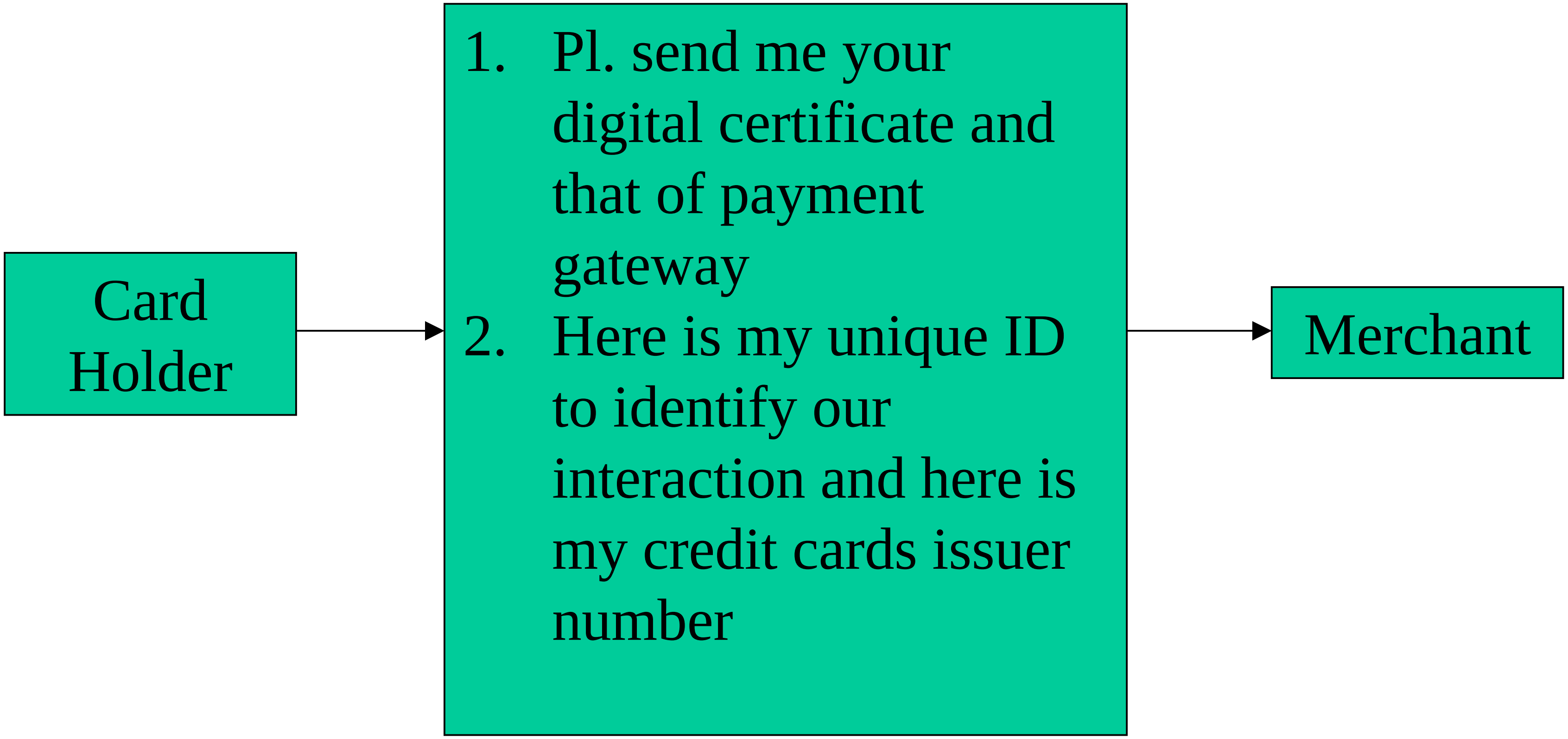
Purchase Request: Before transaction begins cardholder is assumed to have completed browsing selecting and ordering the items

Purchase Request:

Purchase request exchange is made of four messages

1. Initiate request
2. Initiate response
3. Purchase request
4. Purchase response

Step-I Initiate Request

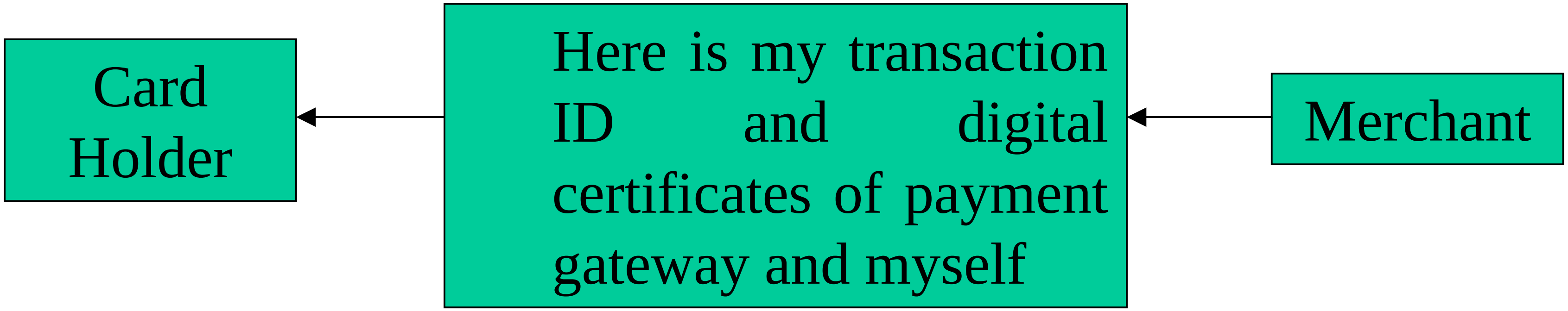


Card Holder

1. Pl. send me your digital certificate and that of payment gateway
2. Here is my unique ID to identify our interaction and here is my credit cards issuer number

Merchant

Step-II: Initiate Response



Card Holder

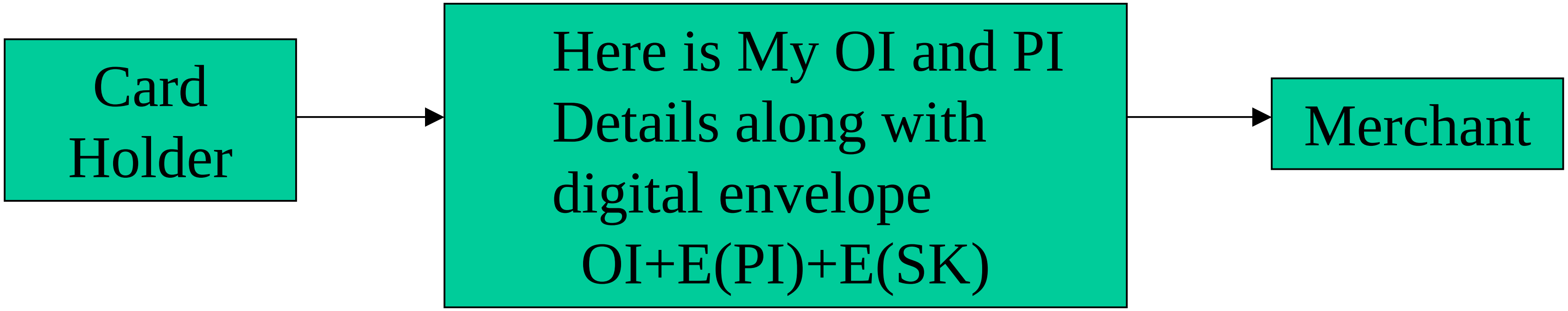
Here is my transaction ID and digital certificates of payment gateway and myself

Merchant

Step-III: Purchase Request

OI- Order information

PI – Purchase Information

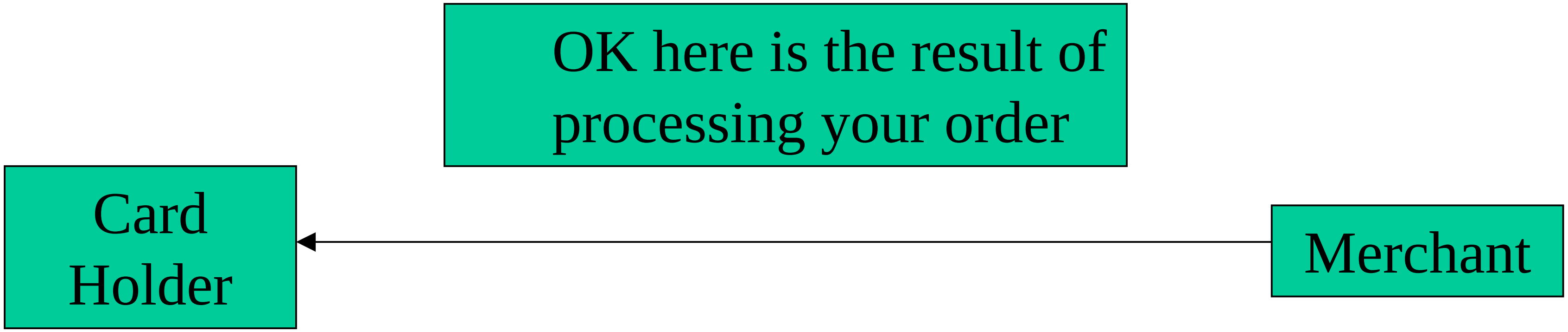


Card Holder

Here is My OI and PI Details along with digital envelope
OI+E(PI)+E(SK)

Merchant

Step-IV Purchase response



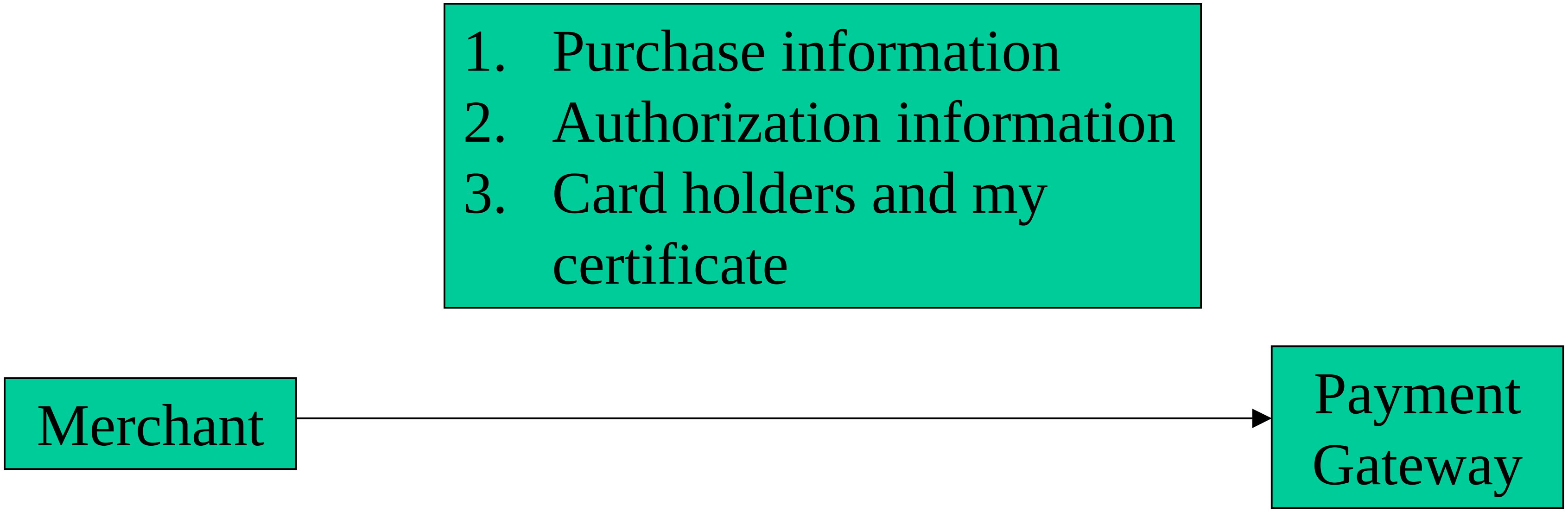
OK here is the result of processing your order

Card Holder

Merchant

II. Payment authorization

This process ensures that the issuer of card approaches the transaction

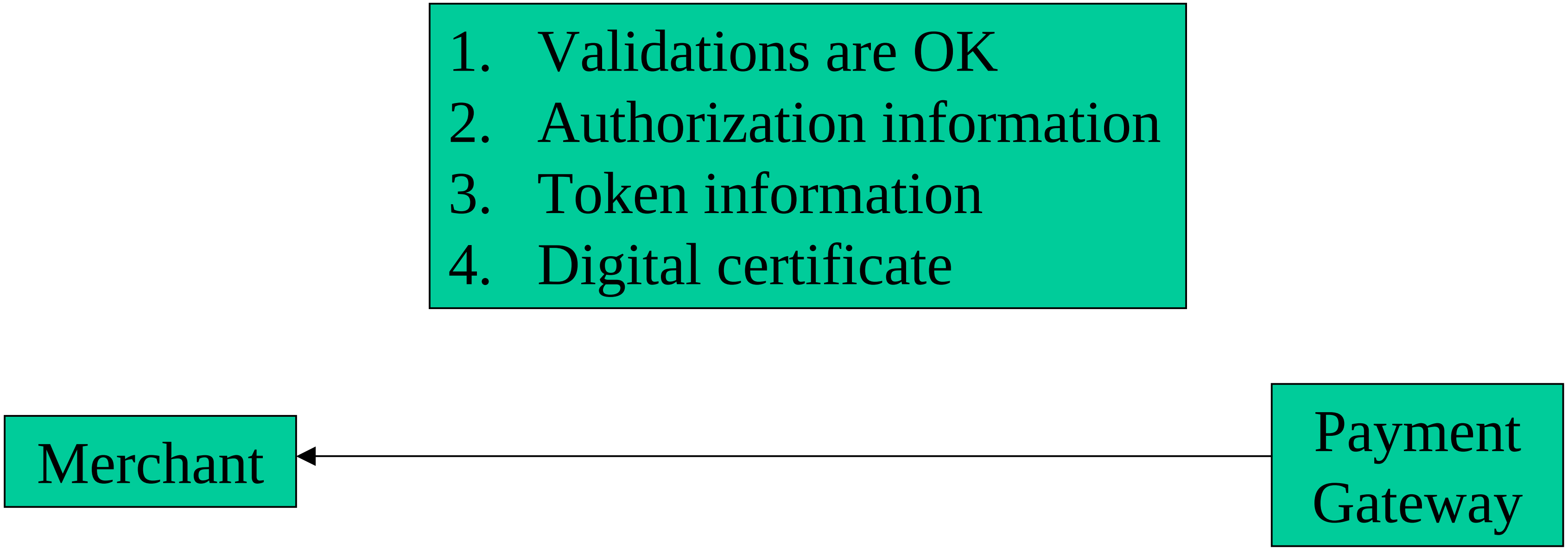


1. Purchase information
2. Authorization information
3. Card holders and my certificate

Merchant

Payment Gateway

Fig.: Authorization of request



1. Validations are OK
2. Authorization information
3. Token information
4. Digital certificate

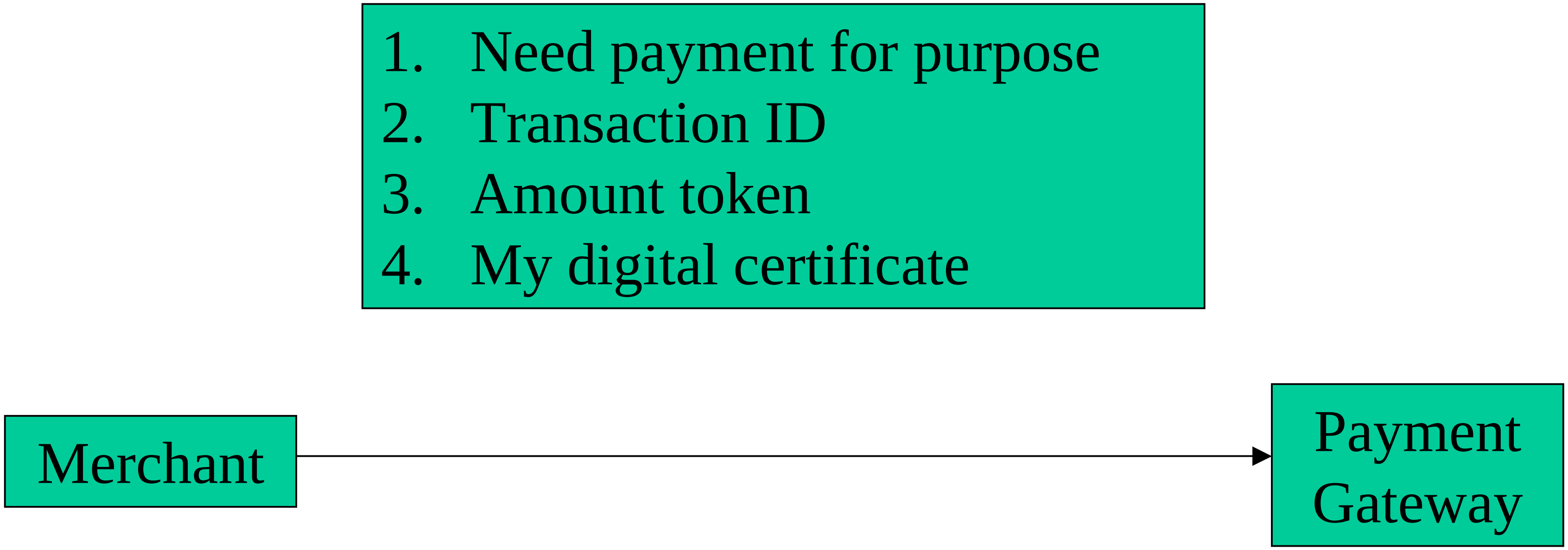
Merchant

Payment Gateway

Fig.: Authorization response

III Payment Capture

Step-I: Capture request: Merchant generates sign and encrypt capture request block that include payment amount and transaction Id in encrypted format



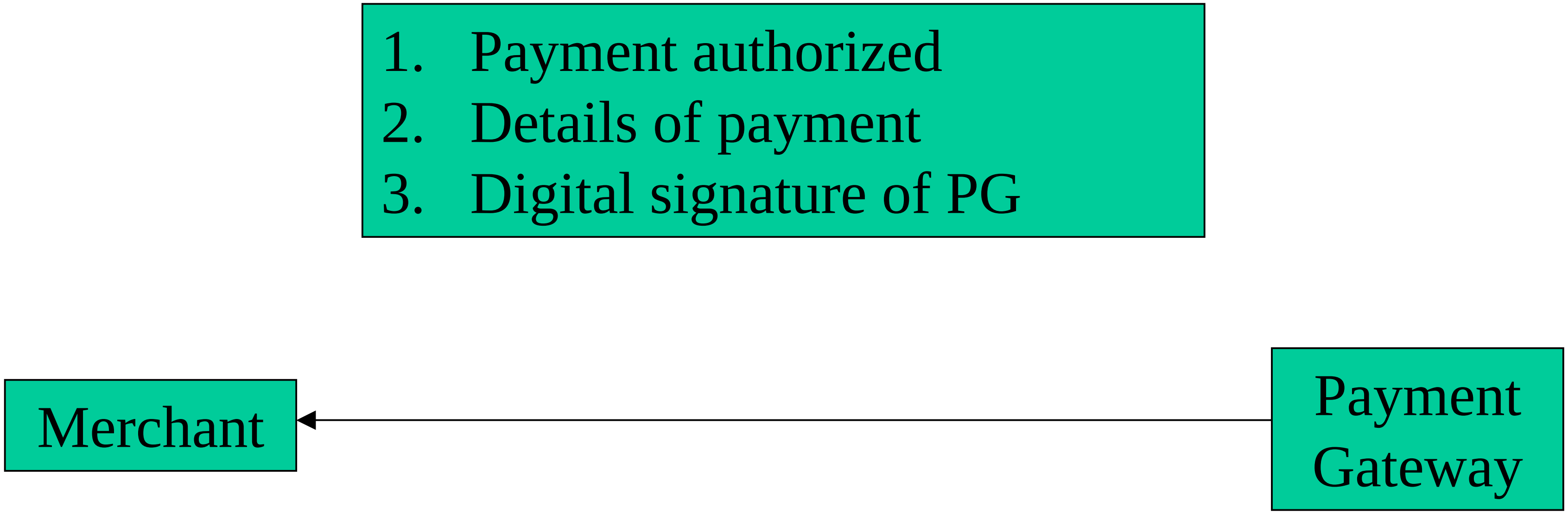
1. Need payment for purpose
2. Transaction ID
3. Amount token
4. My digital certificate

Merchant

Payment Gateway

Fig: Capture request for payment

Step-II: Capture response:



1. Payment authorized
2. Details of payment
3. Digital signature of PG

Merchant

Payment Gateway

Fig: Capture response

Advantages

- Extremely secure
  - Fraud reduced since all parties are authenticated
  - Requires all parties to have certificates

Problems with SET

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

That’s All !

Electronic Money
E-Cash

E-Cash

- E-cash is one or more way of paying /making payment on Internet
- E-cash is nothing but money represented by computer file
- i.e. Physical form of money is converted into binary form of computer data

Requirements for e-payments

- Atomicity
  - Money is not lost or created during a transfer
- Good atomicity
  - Money and good are exchanged atomically
- Non-repudiation
  - No party can deny its role in the transaction
  - Digital signatures

Desirable Properties of E-Cash

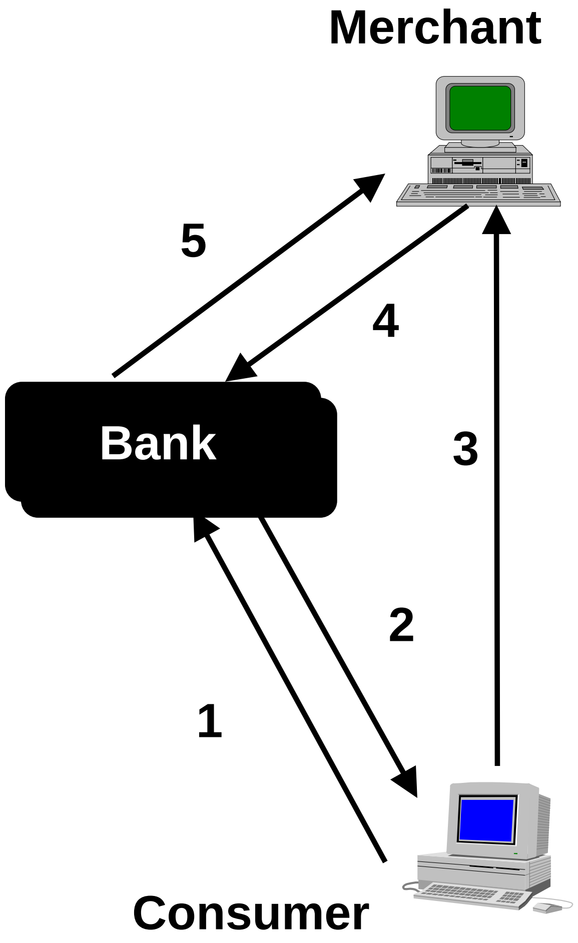
- Universally accepted
- Transferable electronically
- Non-forgeable, non-stealable
- Private (no one except parties know the amount)
- Anonymous (no one can identify the payer)
- Work off-line (no on-line verification needed)

No known system satisfies all.

Types of E-payments

- E-cash
- Electronic wallets
- Smart card
- Credit card

E-cash Concept



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

Consumer still has (invalid) e-cash

Obtaining e-money from Bank

CUSTOMER

- Customer opens account with bank

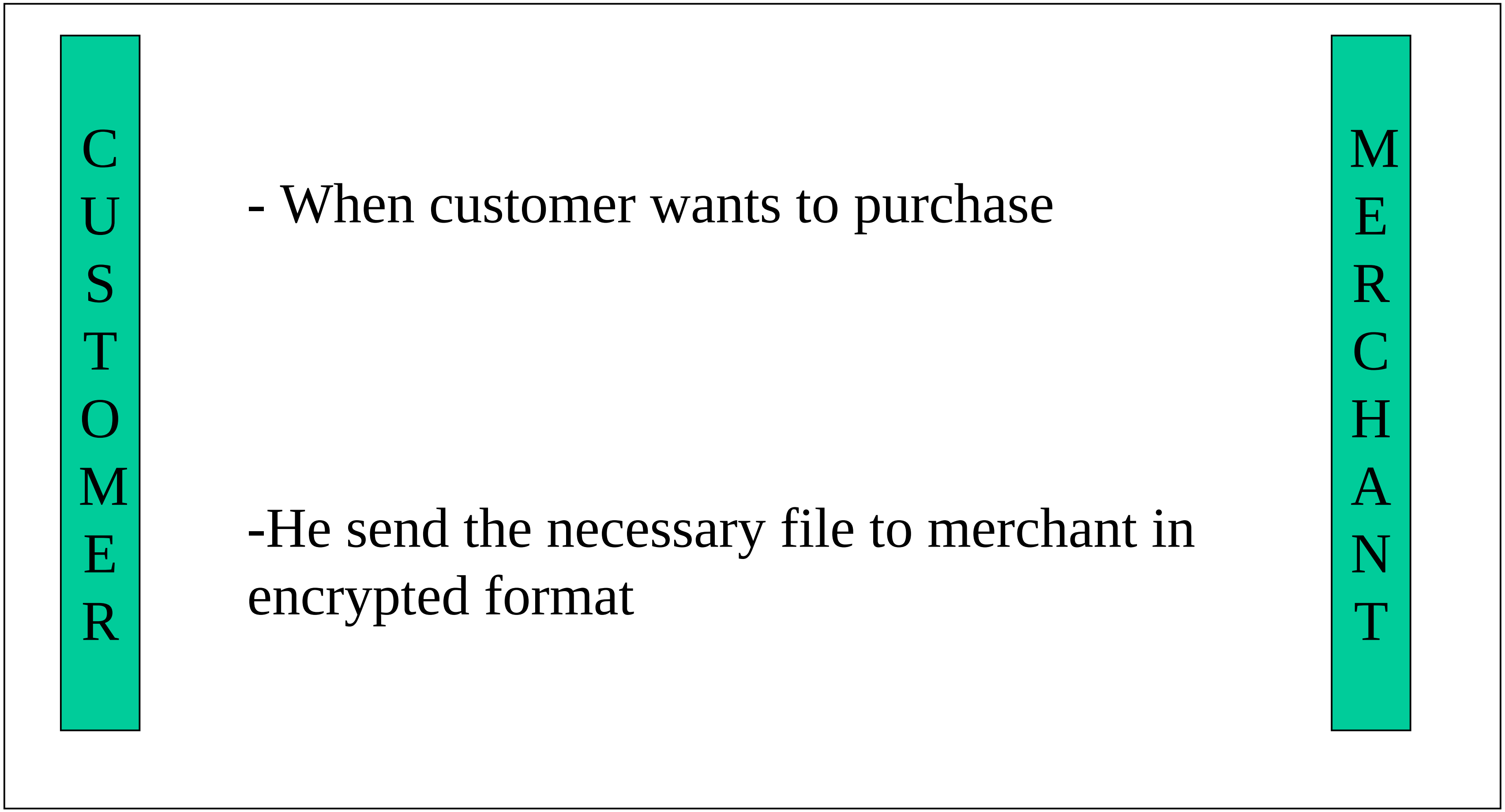
-When he needs money sends e-mail demanding money in encrypted format

-Bank authenticates message and debits customer AC

-Banks sends money as computer file to customer thus file is also encrypted

BANK

Making Purchase using E-money



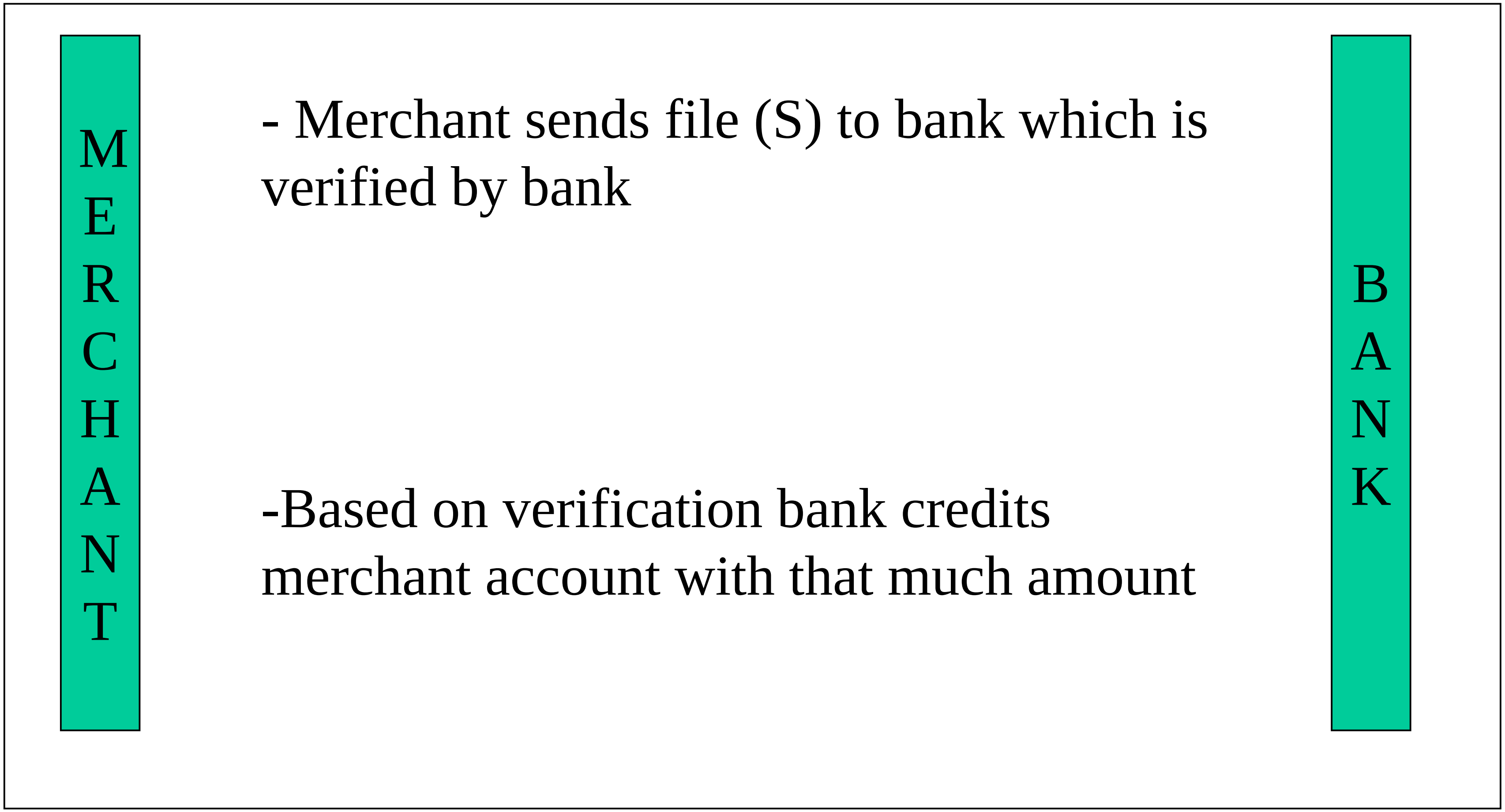
CUSTOMER

- When customer wants to purchase

-He send the necessary file to merchant in encrypted format

MERCHANT

Merchant paid from Bank



MERCHANT

- Merchant sends file (S) to bank which is verified by bank

-Based on verification bank credits merchant account with that much amount

BANK

Security Mechanism in E-Money

- Security mechanism is similar to SET & SSL

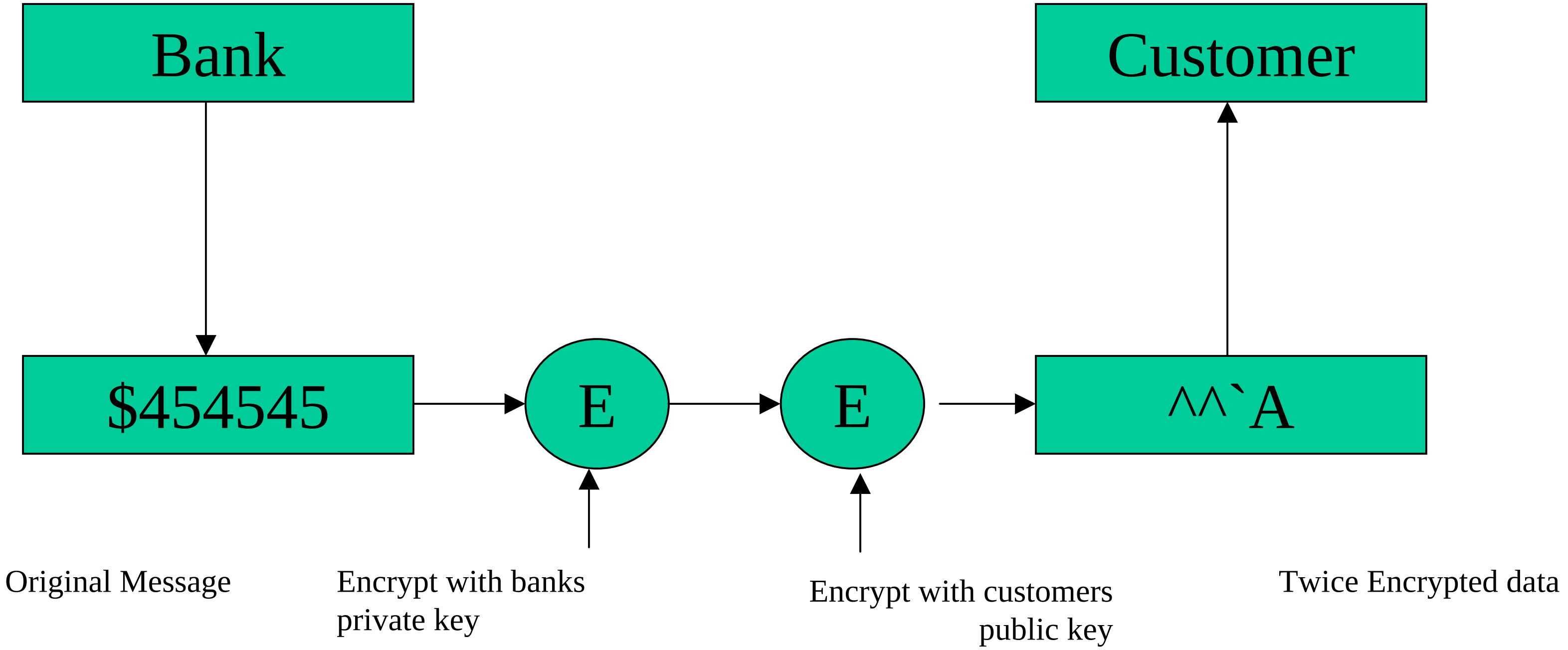
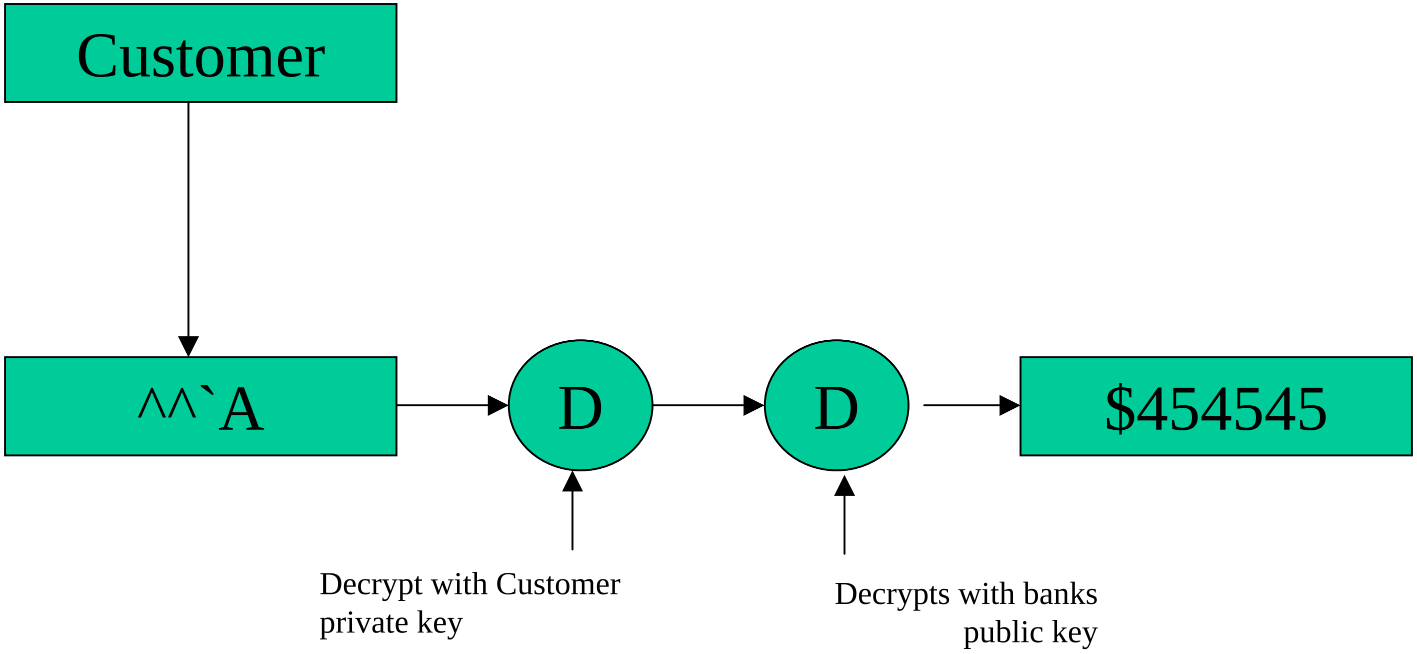

Bank
Customer
$454545
E
E
^^`A
Original Message
Encrypt with banks private key
Encrypt with customers public key
Twice Encrypted data

Fig: Bank sends Electronic Money to the customer after encrypting it twice

Customer receives money and decrypts it


Customer
^^`A
D
D
$454545
Decrypt with Customer private key
Decrypts with banks public key

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)
  - Atomicity problem

Advantages and Disadvantages of Electronic Cash

- Advantages
  - More efficient, eventually meaning lower prices
  - Lower transaction costs
  - Anybody can use it, unlike credit cards, and does not require special authorization
- Disadvantages
  - Tax trail non-existent, like regular cash
  - Money laundering
  - Susceptible to forgery

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
  - Does not prevent double spending, since the merchant or consumer could be at fault

Past and Present E-cash Systems

- Checkfree
  - Allows payment with online electronic checks
- Clickshare
  - Designed for magazine and newspaper publishers
  - Miscast as a micropayment only system; only one of its features
  - Purchases are billed to a user’s ISP, who in turn bill the customer

Past and Present E-cash Systems

- CyberCash
  - Combines features from cash and checks
  - Offers credit card, micropayment, and check payment services
  - Connects merchants directly with credit card processors to provide authorizations for transactions in real time
- CyberCoins
  - Stored in CyberCash wallet, a software storage mechanism located on customer’s computer
  - Used to make purchases between .25c and $10

Past and Present E-cash Systems

- DigiCash
  - Trailblazer in e-cash
  - Allowed customers to purchase goods and services using anonymous electronic cash
- Coin.Net
  - Electronic tokens stored on a customer’s computer is used to make purchases
  - Works by installing special plug-in to a customer’s web browser
  - Merchants do not need special software to accept eCoins.

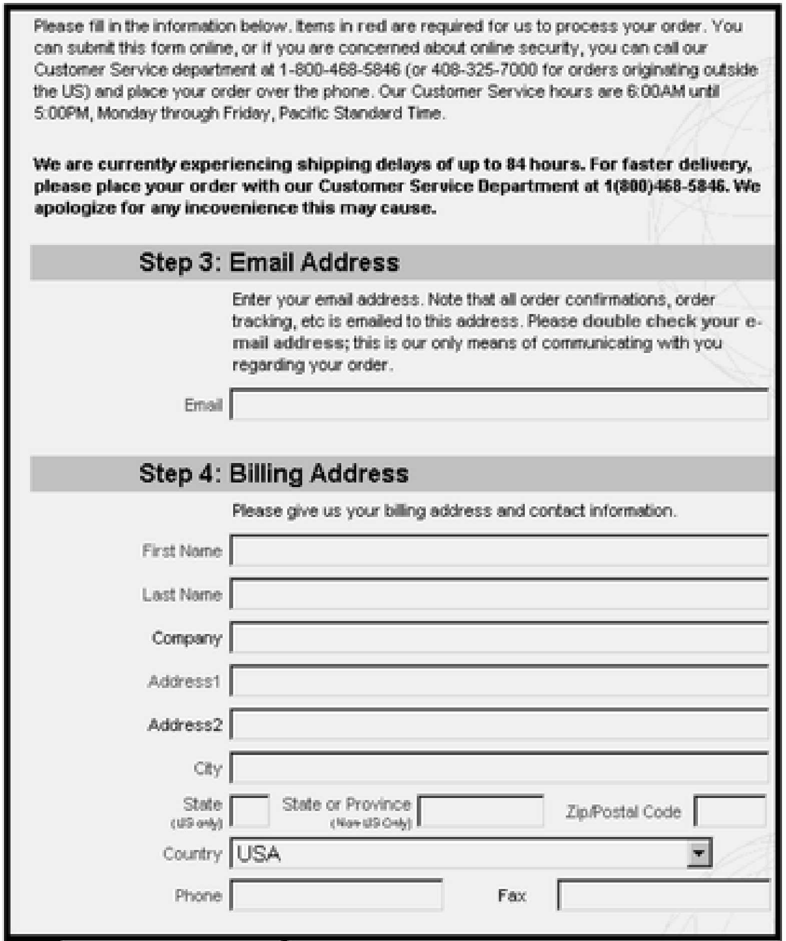
Past and Present E-cash Systems

- MilliCent
  - Developed by Digital, now part of Compaq
  - Electronic scrip system
  - Participating merchant creates and sells own scrip to broker at a discount
    - Consumers register with broker and buy bulk generic scrip, usually with credit card
    - Customers buy by converting broker scrip to vendor-specific scrip, i.e. scrip that a particular merchant will accept
  - Customers can purchase items of very low value

Electronic Wallets

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

An Electronic Checkout Counter Form



Please fill in the information below. Items in red are required for us to process your order. You can submit this form online, or if you are concerned about online security, you can call our Customer Service department at 1-800-468-5846 (or 408-325-7000 for orders originating outside the US) and place your order over the phone. Our Customer Service hours are 6:00AM until 5:00PM, Monday through Friday, Pacific Standard Time.

We are currently experiencing shipping delays of up to 84 hours. For faster delivery, please place your order with our Customer Service Department at 1(800)468-5846. We apologize for any incovenience this may cause.

Step 3: Email Address

Enter your email address. Note that all order confirmations, order tracking, etc is emailed to this address. Please double check your e-mail address; this is our only means of communicating with you regarding your order.

Email

Step 4: Billing Address

Please give us your billing address and contact information.

First Name

Last Name

Company

Address1

Address2

City

State (US only) State or Province (Non-US Only) Zip/Postal Code

Country USA

Phone Fax

FIGURE 7-9 *A typical electronic checkout counter form*

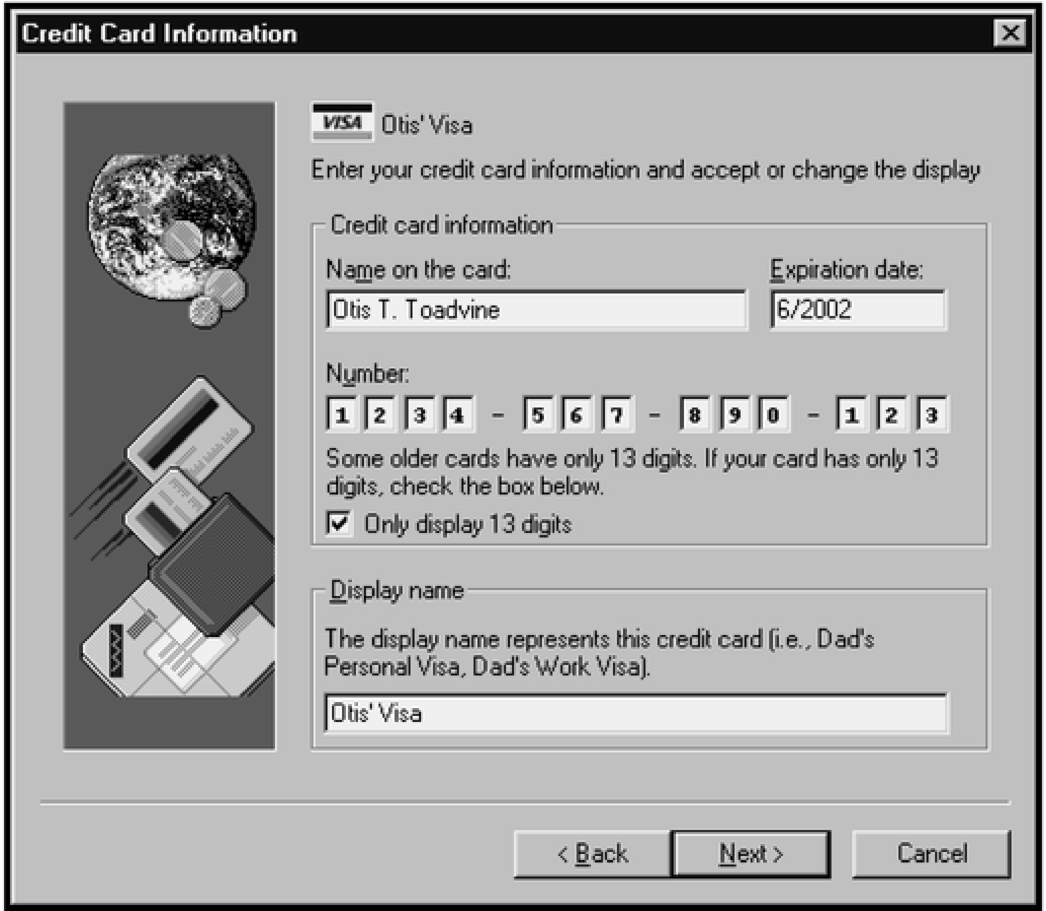
Electronic Wallets

- Agile Wallet
  - Developed by CyberCash
  - Allows customers to enter credit card and identifying information once, stored on a central server
  - Information pops up in supported merchants’ payment pages, allowing one-click payment
- eWallet
  - Developed by Launchpad Technologies
  - Free wallet software that stores credit card and personal information on users’ computer, not on a central server; info is dragged into payment form from eWallet

Electronic Wallets

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

Entering Information Into Microsoft Wallet



Credit Card Information

VISA Otis' Visa

Enter your credit card information and accept or change the display

Credit card information

Name on the card: Otis T. Toadvine

Expiration date: 6/2002

Number: 1234 - 567 - 890 - 123

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

☑ Only display 13 digits

Display name

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

Otis' Visa

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

Smart Cards

- Magnetic stripe
  - 140 bytes
- Memory cards
  - 1-4 KB memory, no processor
- Optical memory cards
  - 4 megabytes read-only (CD-like)
- Microprocessor cards
  - Embedded microprocessor
    - (OLD) 8-bit processor, 16 KB ROM, 512 bytes RAM
    - Equivalent power to IBM XT PC
    - 32-bit processors now available

Smart Cards

- Plastic card containing an embedded microchip
- Available for over 10 years
- So far not successful in U.S., but popular in Europe, Australia, and Japan
- Unsuccessful in U.S. partly because few card readers available
- Smart cards gradually reappearing success depends on:
  - Critical mass of smart cards that support applications
  - Compatibility between smart cards, card-reader devices, and applications

Smart Card Applications

- Ticketless travel
  - Seoul bus system: 4M cards, 1B transactions since 1996
  - Planned the SF Bay Area system
- Authentication, ID
- Medical records
- Ecash
- Store loyalty programs
- Personal profiles
- Government
  - Licenses
- Mall parking

. . .

Advantages of Smart Cards

- Advantages:
  1. Atomic, debt-free transactions
  2. Feasible for very small transactions (information commerce)
  3. (Potentially) anonymous
  4. Security of physical storage
  5. (Potentially) currency-neutral

Disadvantages of Smart Cards

- Disadvantages:
  1. Low maximum transaction limit (not suitable for B2B or most B2C)
  2. High Infrastructure costs (not suitable for C2C)
  3. Single physical point of failure (the card)
  4. Not (yet) widely used

Mondex Smart Card

- Holds and dispenses electronic cash (Smart-card based, stored-value card)
- Developed by MasterCard International
- Requires specific card reader, called Mondex terminal, for merchant or customer to use card over Internet
- Supports micropayments as small as 3c and works both online and off-line at stores or over the telephone
- Secret chip-to-chip transfer protocol
- Value is not in strings alone; must be on Mondex card
- Loaded through ATM
  - ATM does not know transfer protocol; connects with secure device at bank

Mondex Smart Card Processing

1. User opens account and receives smart card

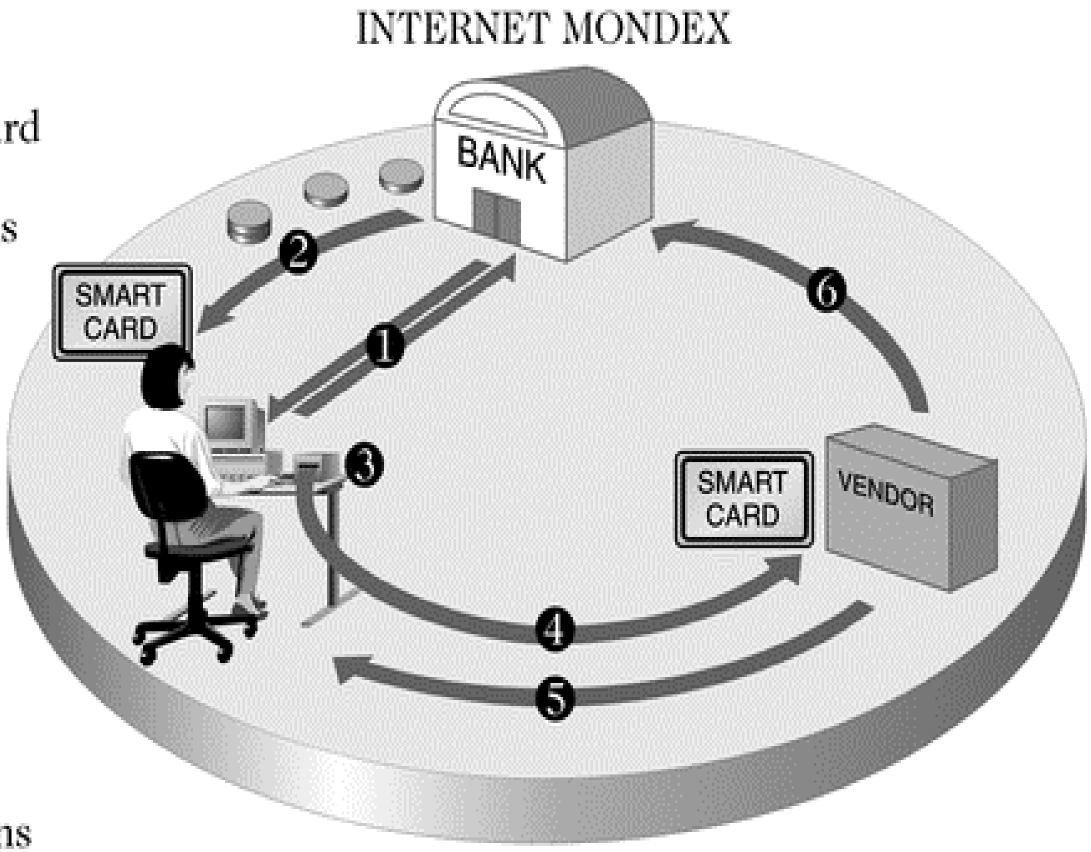
2. User downloads tokens onto card

3. User inserts card in reader

4. Tokens are transferred from user card to vendor

5. Goods delivered

6. Vendor redeems tokens



Mondex transaction

- Placing the card in a Mondex terminal starts the transaction process:
    1. Information from the customer's chip is validated by the merchant's chip. Similarly, the merchant's card is validated by the customer's card.
    2. The merchant's card requests payment and transmits a "digital signature" with the request. Both cards check the authenticity of each other's message. The customer's card checks the digital signature and, if satisfied, sends acknowledgement, again with a digital signature.

Mondex transaction

Only after the purchase amount has been deducted from the customer's card is the value added to the merchant's card. The digital signature from this card is checked by the customer's card and if confirmed, the transaction is complete.

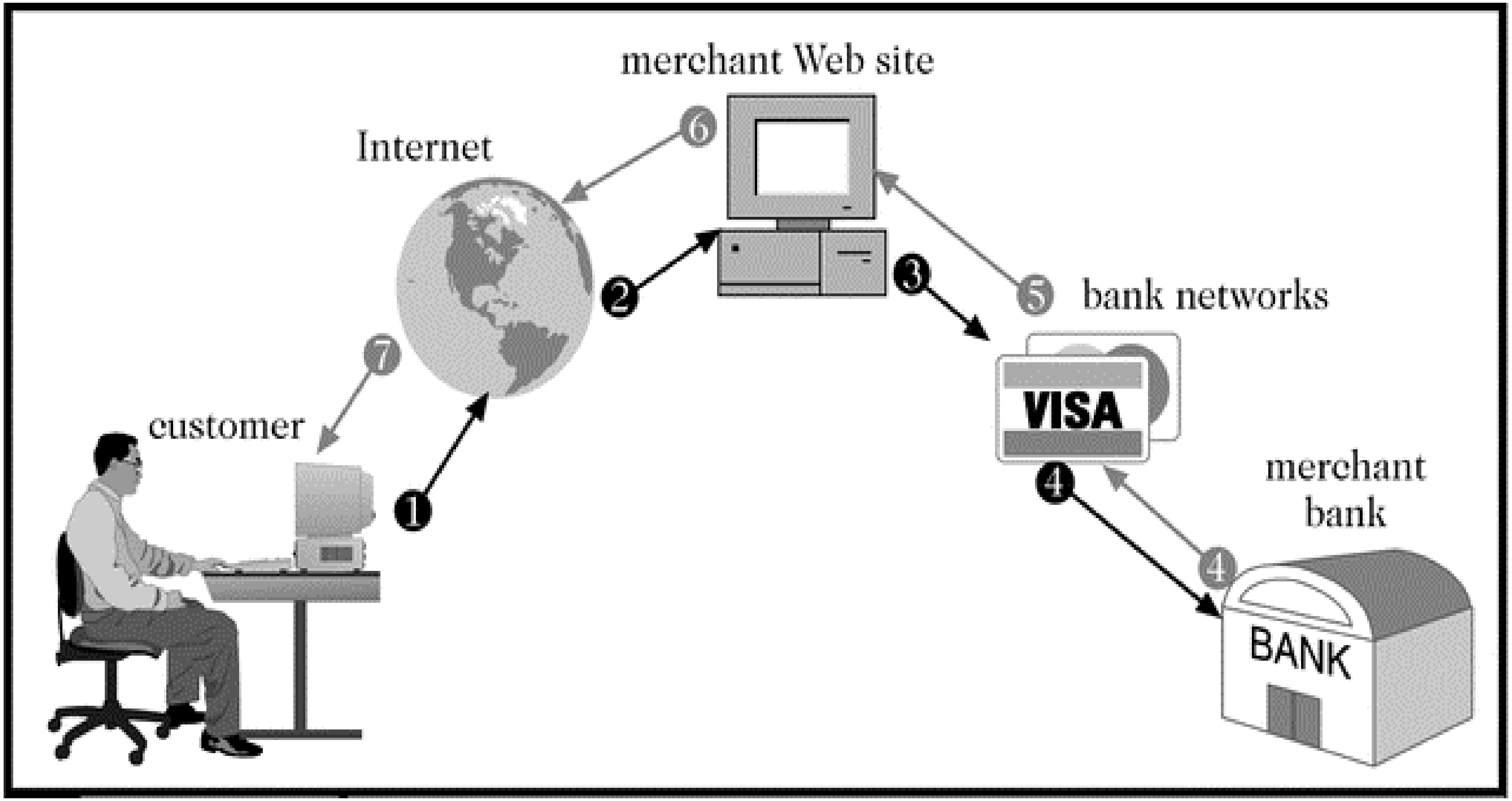
Credit Cards

- Credit card
  - Used for the majority of Internet purchases
  - Has a preset spending limit
  - Currently most convenient method
  - Most expensive e-payment mechanism
    - MasterCard: $0.29 + 2% of transaction value
  - Disadvantages
    - Does not work for small amount (too expensive)
    - Does not work for large amount (too expensive)
- Charge card
  - No spending limit
  - Entire amount charged due at end of billing period

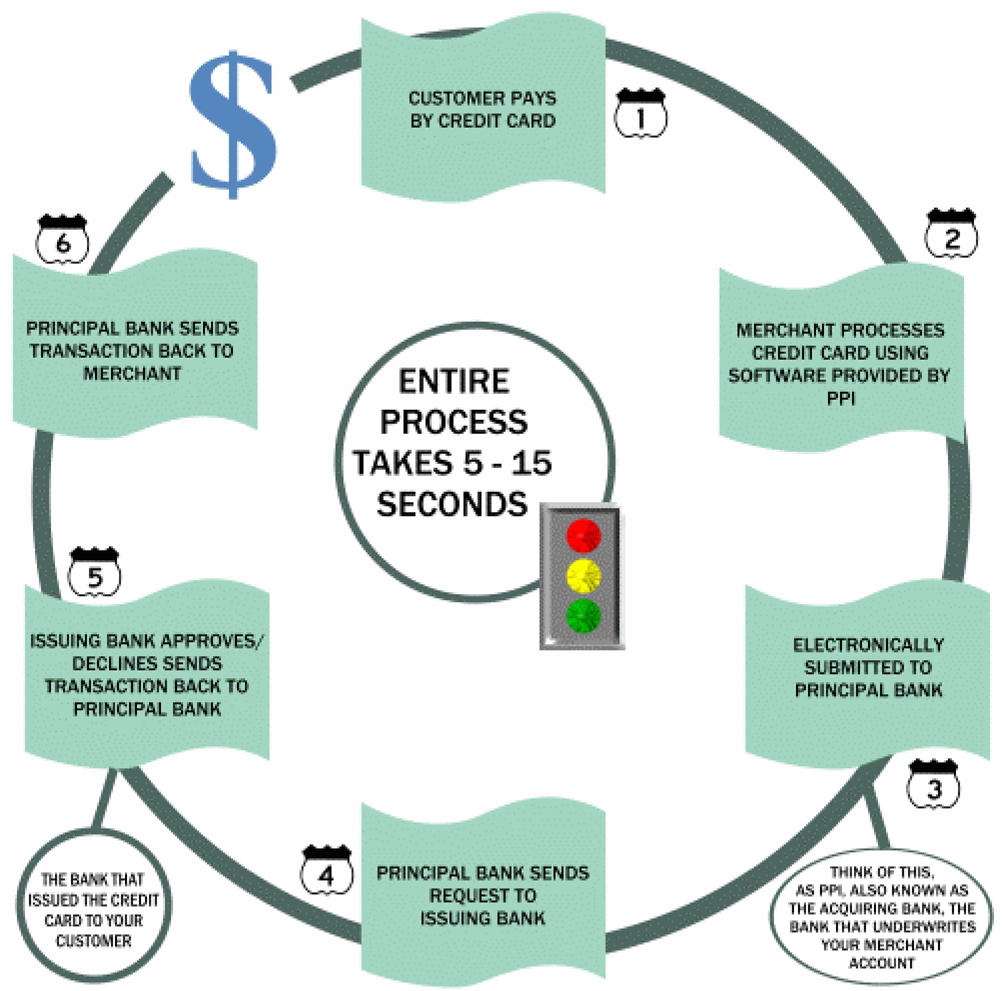
Payment Acceptance and Processing

- Merchants must set up merchant accounts to accept payment cards
- Law prohibits charging payment card until merchandise is shipped
- Payment card transaction requires:
  - Merchant to authenticate payment card
  - Merchant must check with card issuer to ensure funds are available and to put hold on funds needed to make current charge
  - Settlement occurs in a few days when funds travel through banking system into merchant’s account

Processing a Payment Card Order



Credit Card Processing


$
CUSTOMER PAYS BY CREDIT CARD
1
MERCHANT PROCESSES CREDIT CARD USING SOFTWARE PROVIDED BY PPI
2
ELECTRONICALLY SUBMITTED TO PRINCIPAL BANK
3
THINK OF THIS, AS PPI, ALSO KNOWN AS THE ACQUIRING BANK, THE BANK THAT UNDERWRITES YOUR MERCHANT ACCOUNT
PRINCIPAL BANK SENDS REQUEST TO ISSUING BANK
4
ISSUING BANK APPROVES/ DECLINES SENDS TRANSACTION BACK TO PRINCIPAL BANK
5
THE BANK THAT ISSUED THE CREDIT CARD TO YOUR CUSTOMER
PRINCIPAL BANK SENDS TRANSACTION BACK TO MERCHANT
6
ENTIRE PROCESS TAKES 5 - 15 SECONDS

SOURCE: PAYMENT PROCESSING INC.