Internet Security 101

Mark McKelvey
IBM Corporation
Rochester, MN

Internet Security Issues

How do we make the Internet a safe place to do business?

- Confidentiality/privacy
- Integrity
- Authentication
- Non-repudiation

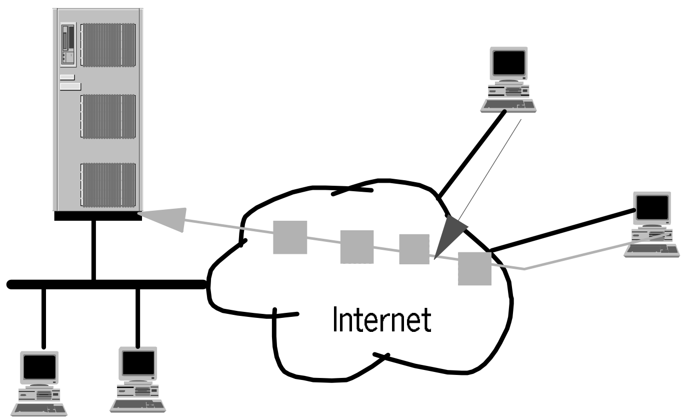
Resources to Protect

There are many things that must be protected

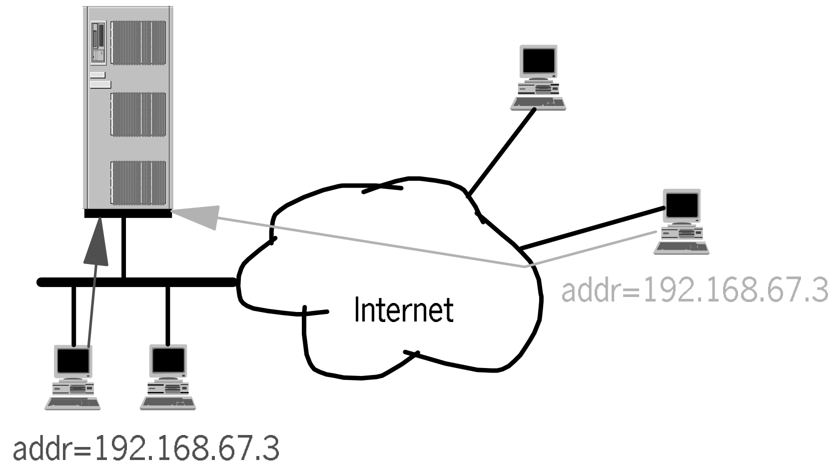
- Public systems
- Private systems
- Network
- Data
- Transactions
- Reputation

What Are We Up Against?

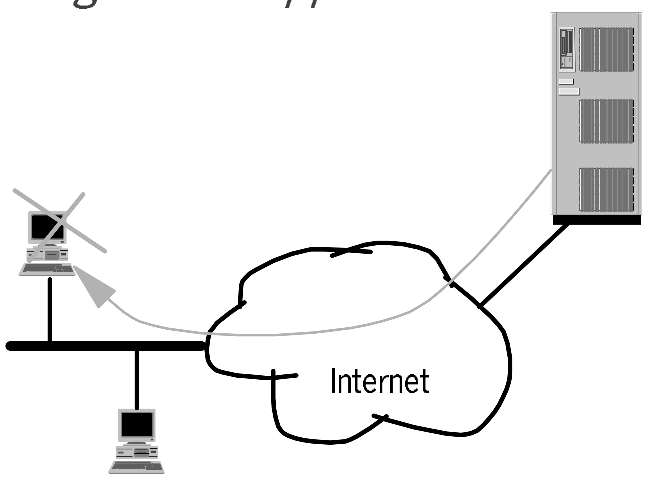
Denial of service



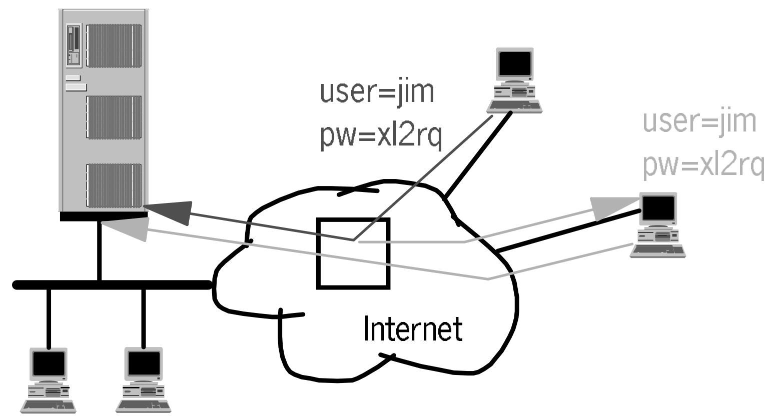
Spoofing



Rogue Java applets



Sniffing



How Bad Is It?

Recent Headlines

Security flaw found in Internet browser

Computer attack knocks out 3,000 Web sites

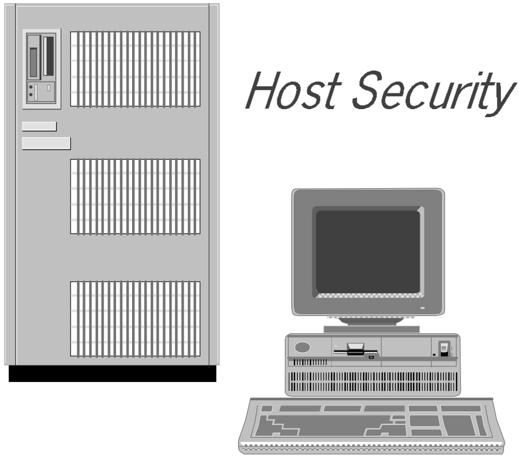
Hackers vandalize CIA home page

Internet service provider out for over a week

Achieving Security

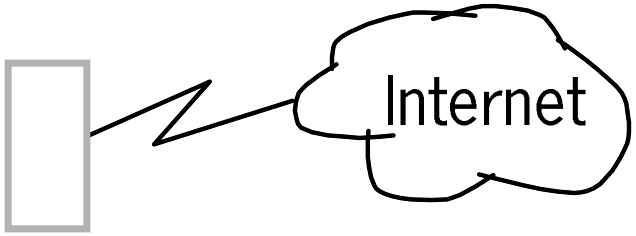
Security Policy

User Procedures



Host Security

Network Access Security

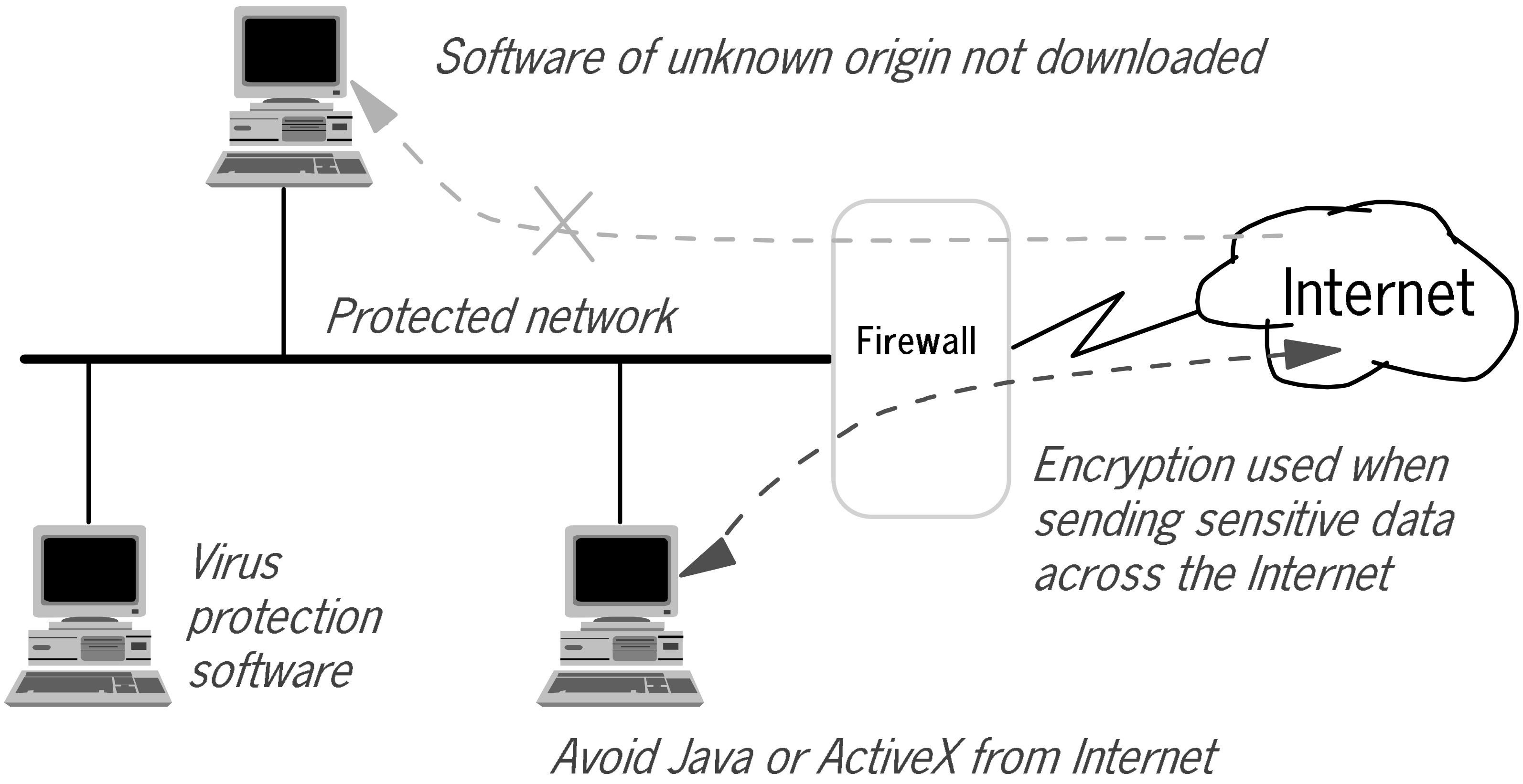


Cryptography *g6Ktgk$79hl]!aD4$

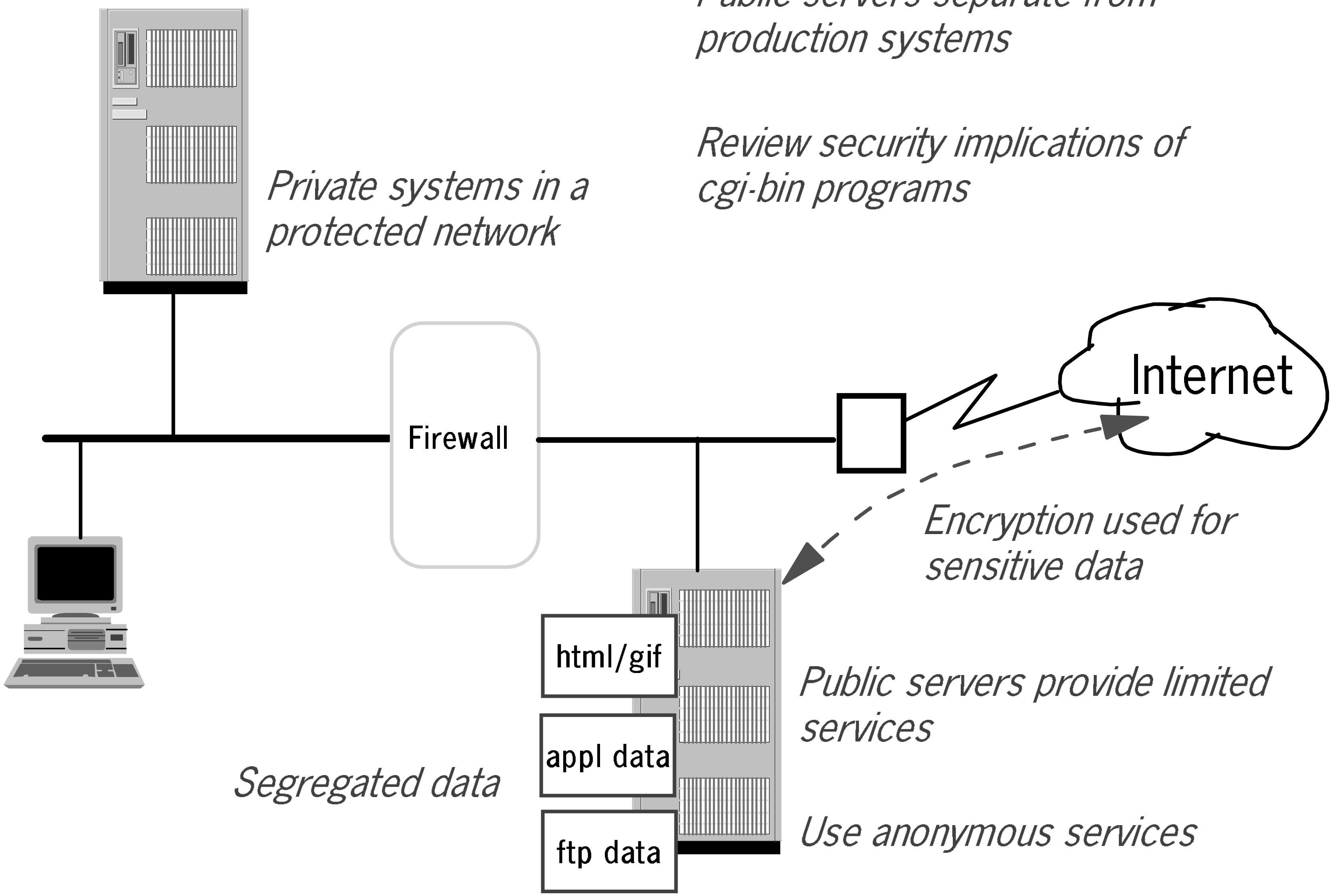
Protecting Client Systems

Educated users

- Know what types of Internet access are appropriate



Protecting Server Systems



Private systems in a protected network

Public servers separate from production systems

Review security implications of cgi-bin programs

Encryption used for sensitive data

Public servers provide limited services

Use anonymous services

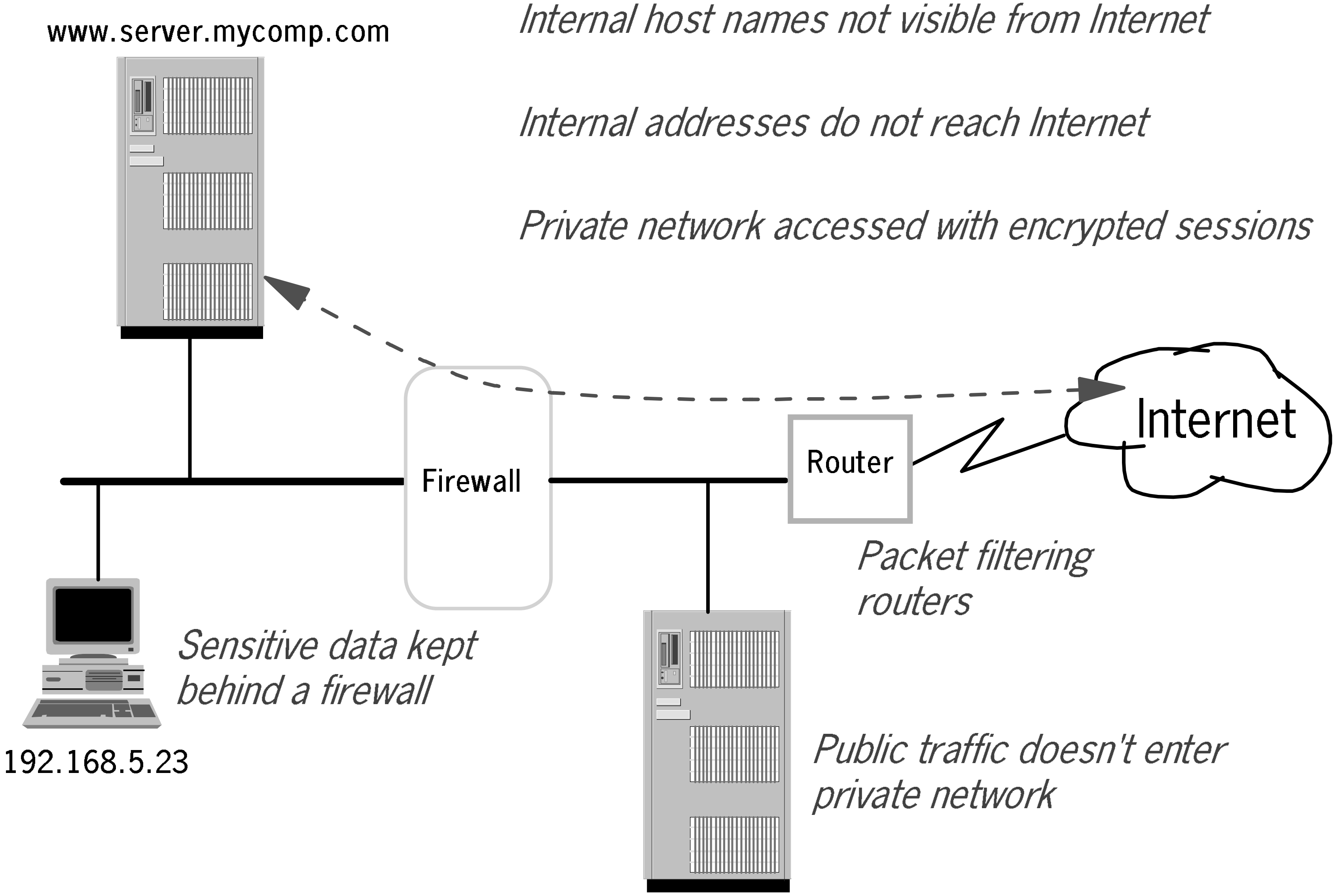
Segregated data

Protecting Networks

Internal host names not visible from Internet

Internal addresses do not reach Internet

Private network accessed with encrypted sessions

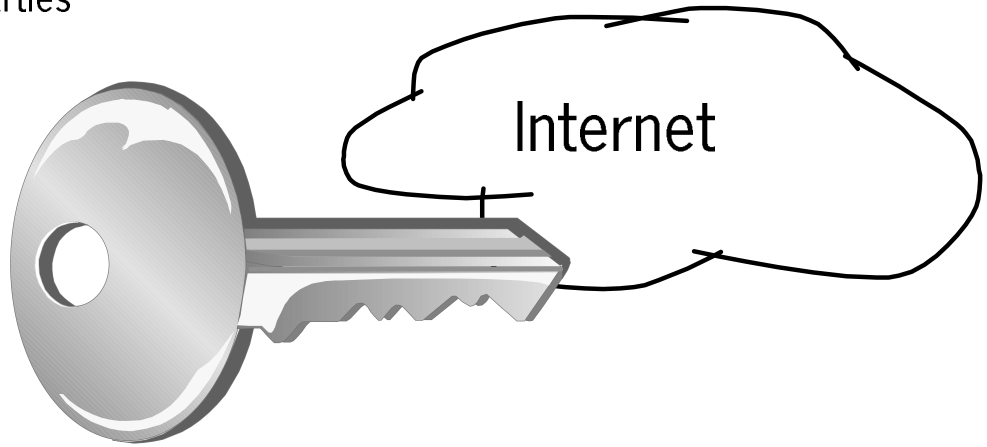


Internet Security Model

Public Key Infrastructure (PKI)

Cryptography used extensively

- Authentication of communicating parties
- Encrypted communication sessions
- Encrypted data envelopes
- Digital signatures

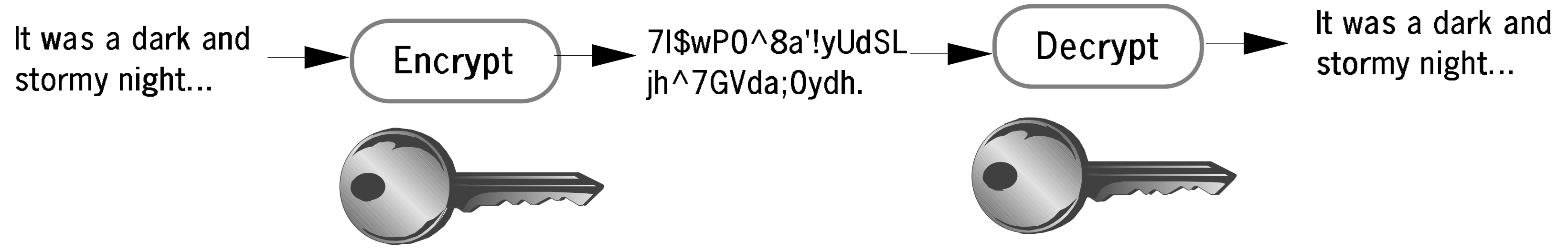


Applicable to Internet and intranets

Keys

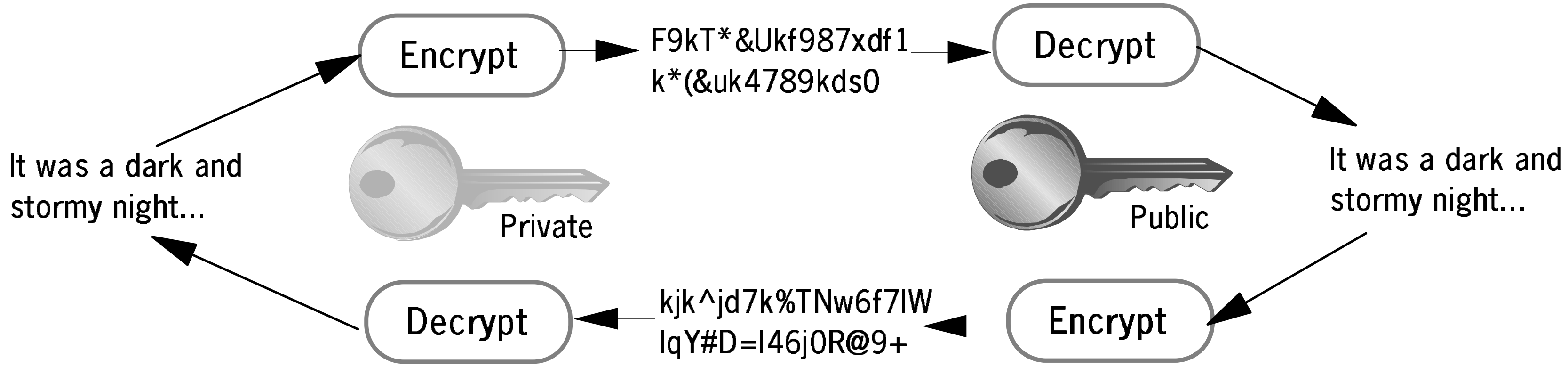
Symmetric Keys

- Same key is used for encryption and decryption

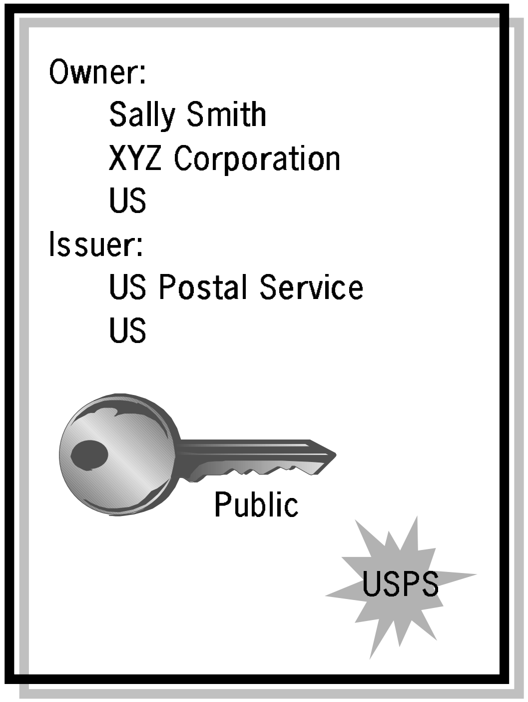


Asymmetric keys

- Encryption and decryption use different keys, a public key and a private key



Certificates



Identifies a user or a system

- Binds public key to an identity
- Created by trusted 3rd parties called Certificate Authorities
- Can be distributed freely
- Digital signature prevents tampering

Internet (public) Certificate Authorities

- Verisign
- US Postal Service
- AT&T
- MCI
- ...many others

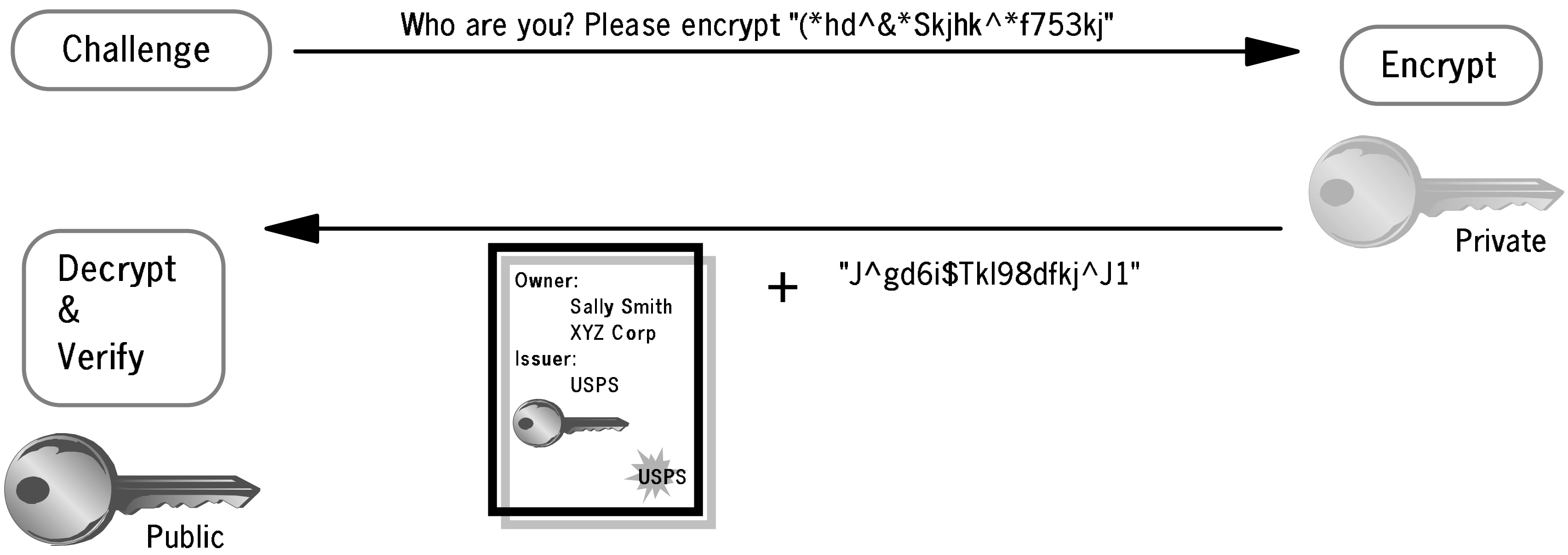
Intranet Certificate Authorities

- Most corporations will have their own Certificate Authority
- IBM Net.Registry product

Proving Your Identity

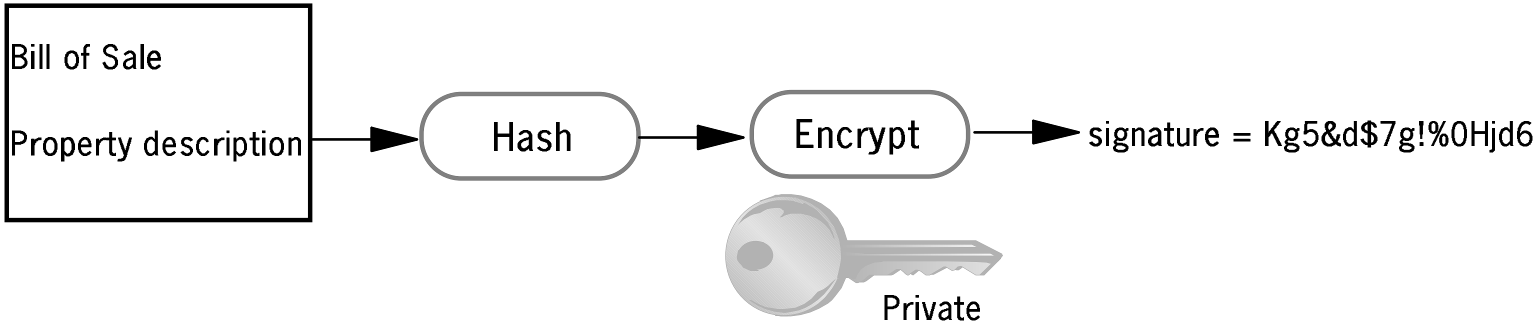
Provide your signed certificate

Encrypt random data with your private key

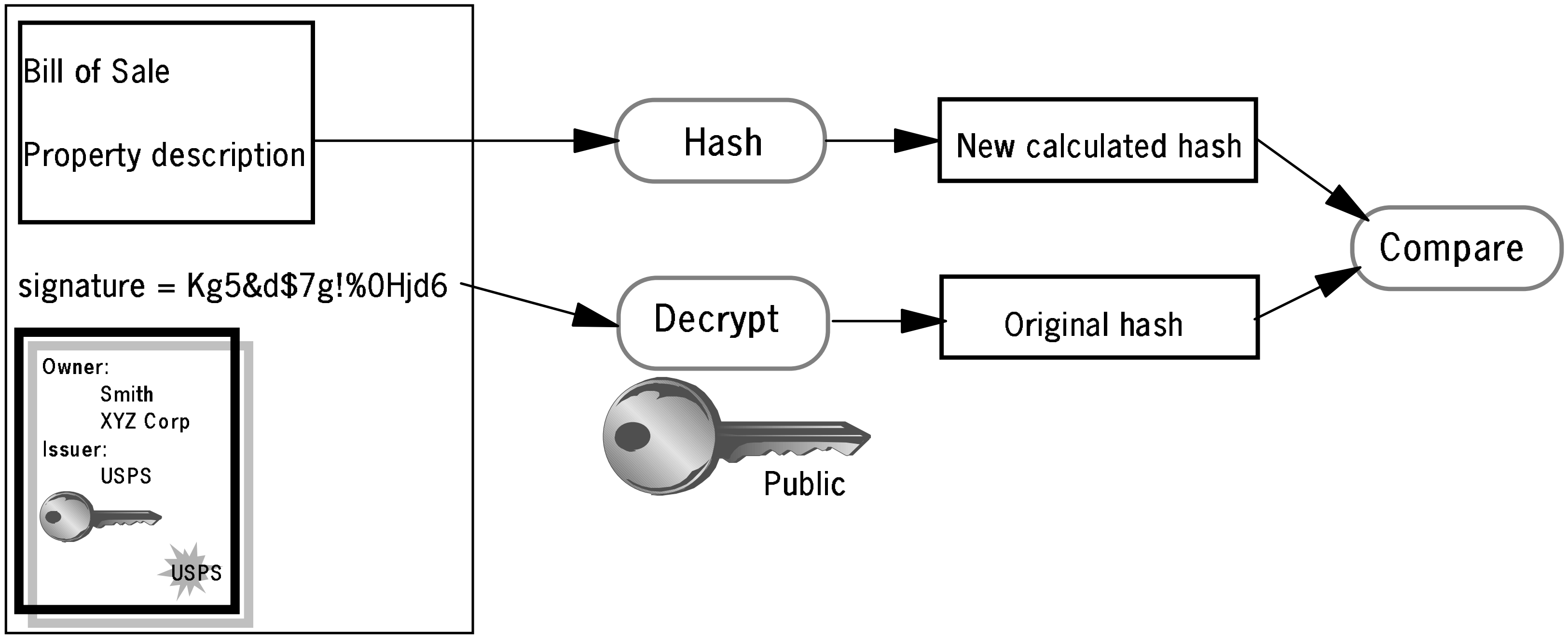


Signing Data

Hash the data to be signed and encrypt hash with private key

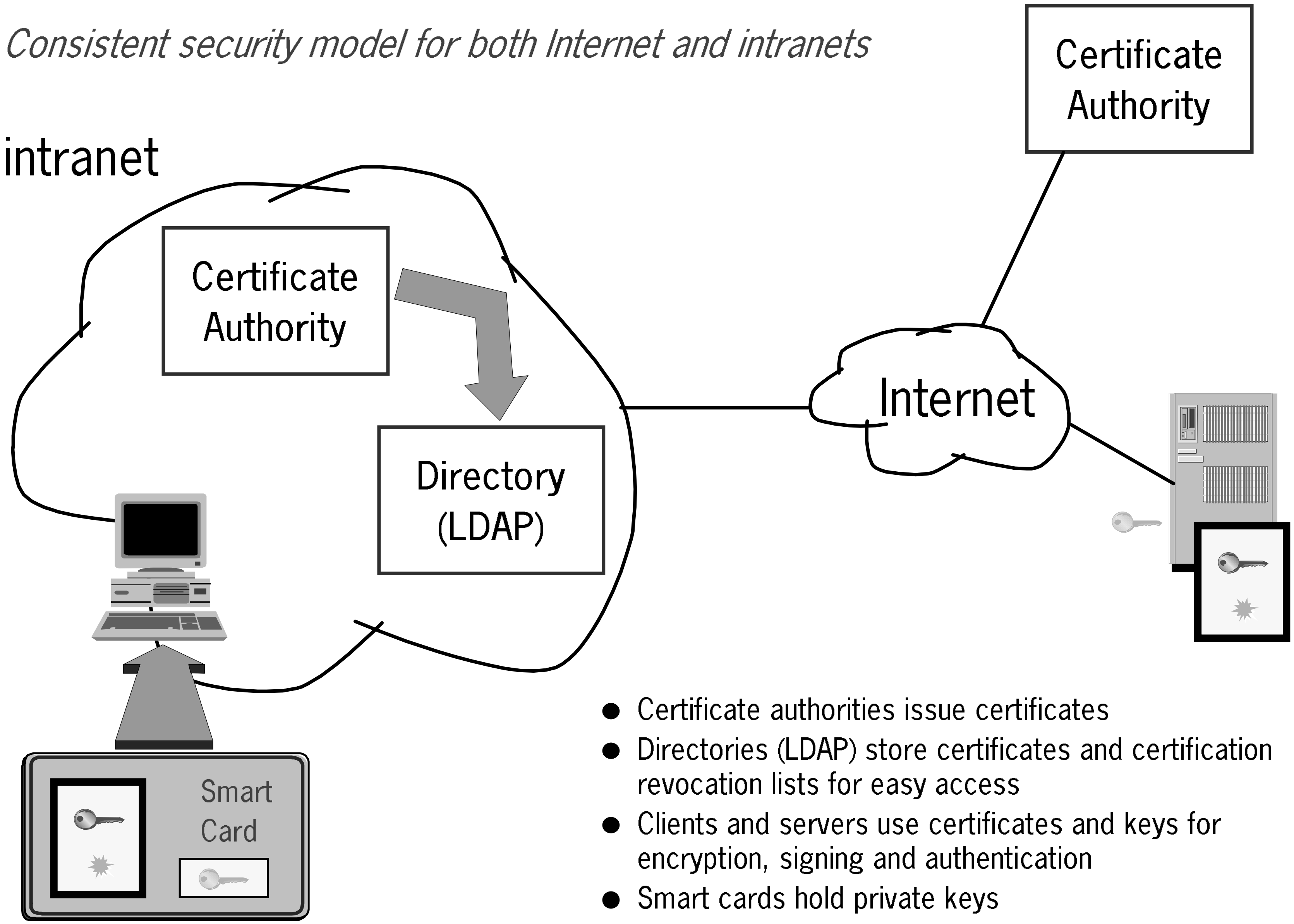


Verify by recalculating hash and comparing against decrypted signature



Public Key Infrastructure

Consistent security model for both Internet and intranets

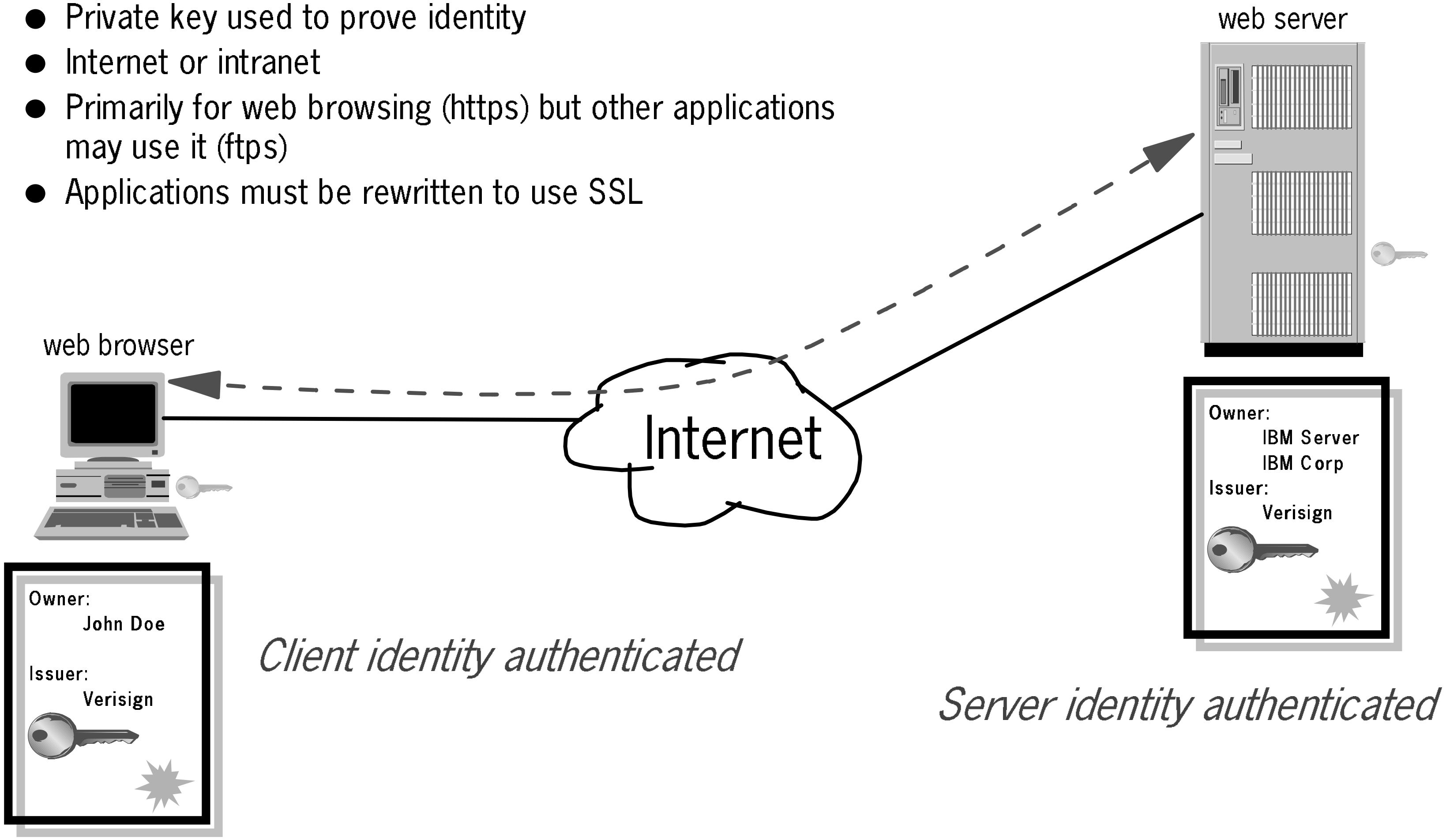


- Certificate authorities issue certificates
- Directories (LDAP) store certificates and certification revocation lists for easy access
- Clients and servers use certificates and keys for encryption, signing and authentication
- Smart cards hold private keys

Secure Sockets Layer (SSL)

End-to-end encrypted communication session

- Uses certificates for identification
- Private key used to prove identity
- Internet or intranet
- Primarily for web browsing (https) but other applications may use it (ftps)
- Applications must be rewritten to use SSL



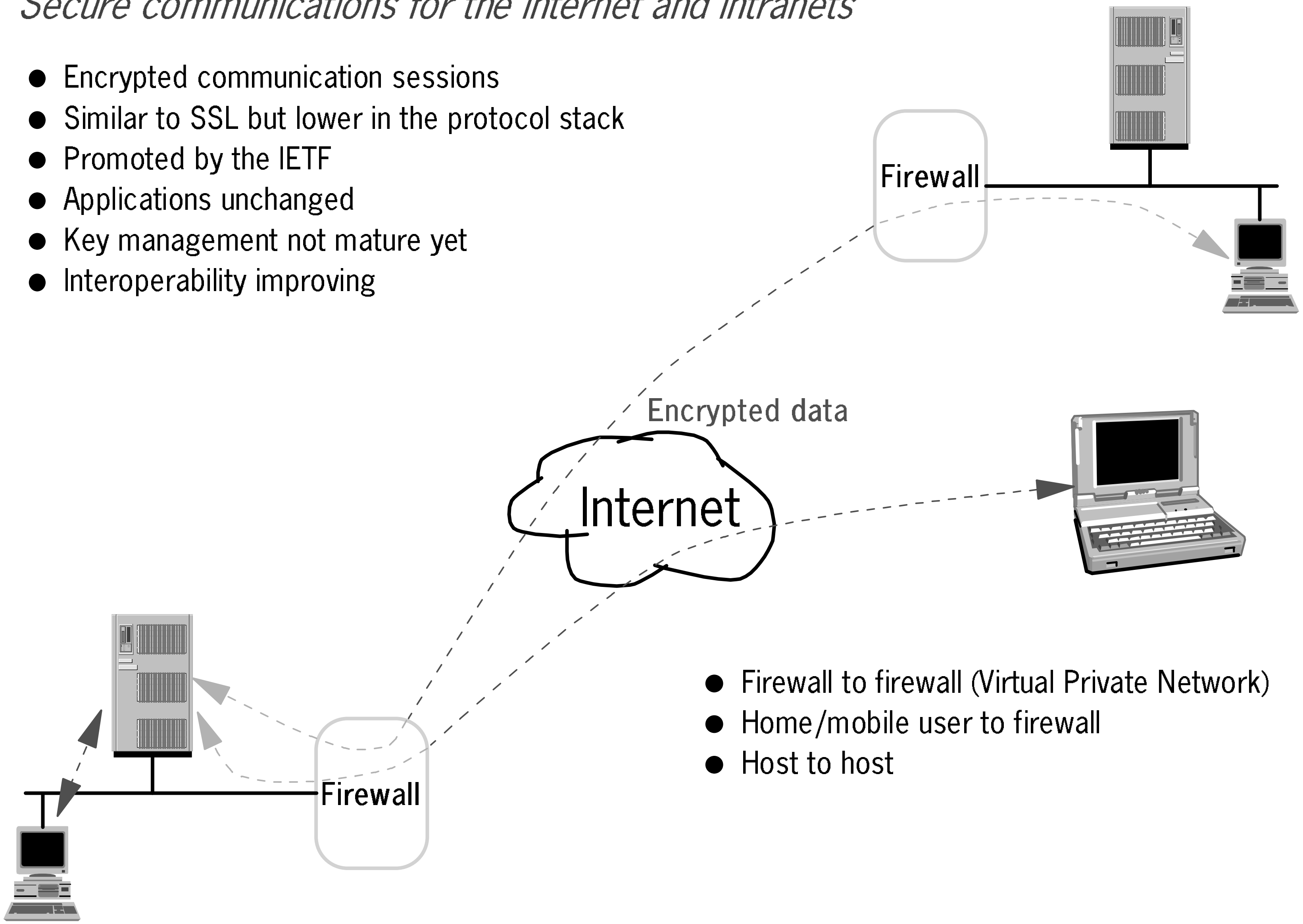
Client identity authenticated

Server identity authenticated

IP Security (IPSec)

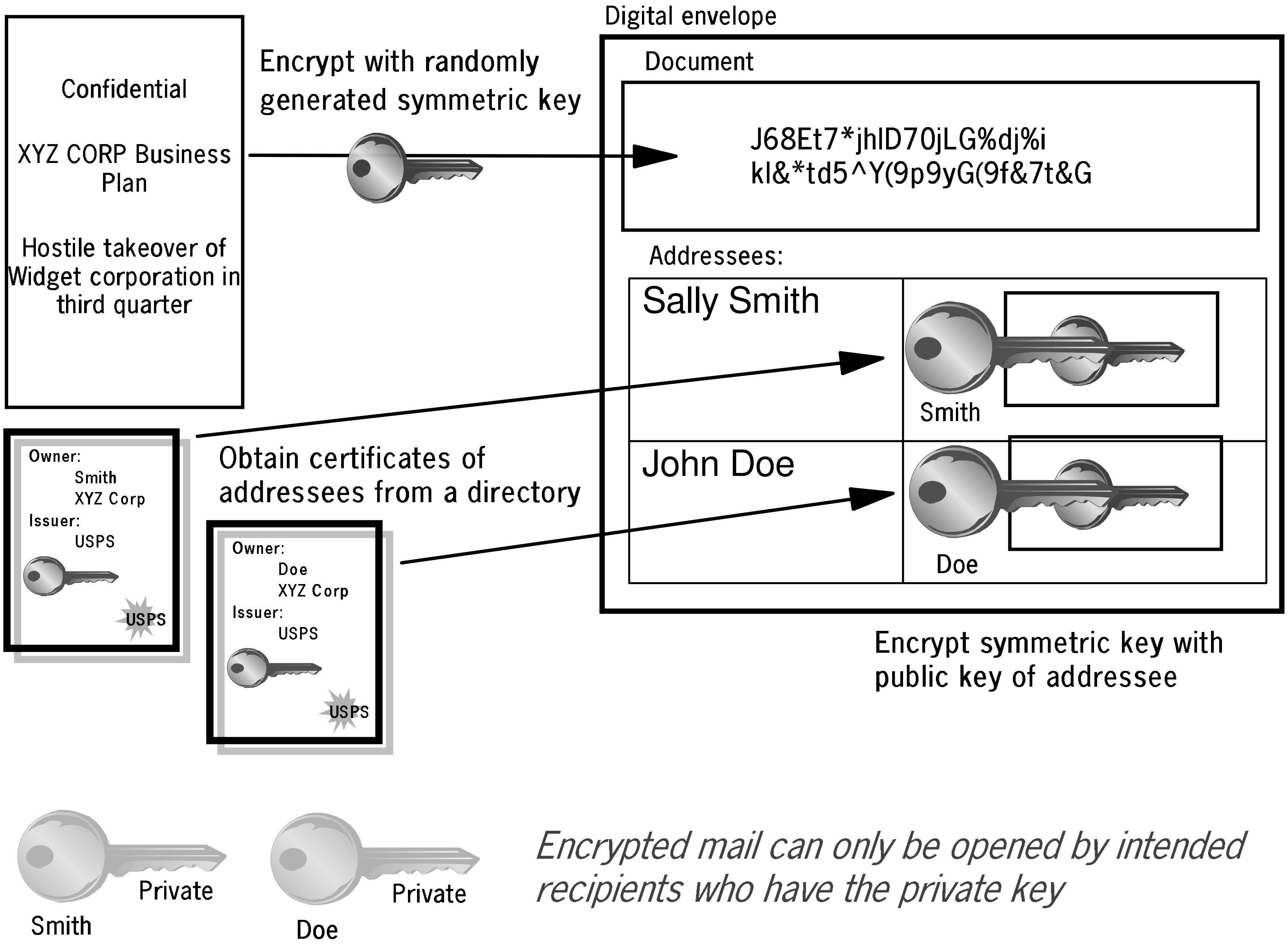
Secure communications for the Internet and intranets

- Encrypted communication sessions
- Similar to SSL but lower in the protocol stack
- Promoted by the IETF
- Applications unchanged
- Key management not mature yet
- Interoperability improving



- Firewall to firewall (Virtual Private Network)
- Home/mobile user to firewall
- Host to host

Secure Mail (S/MIME)

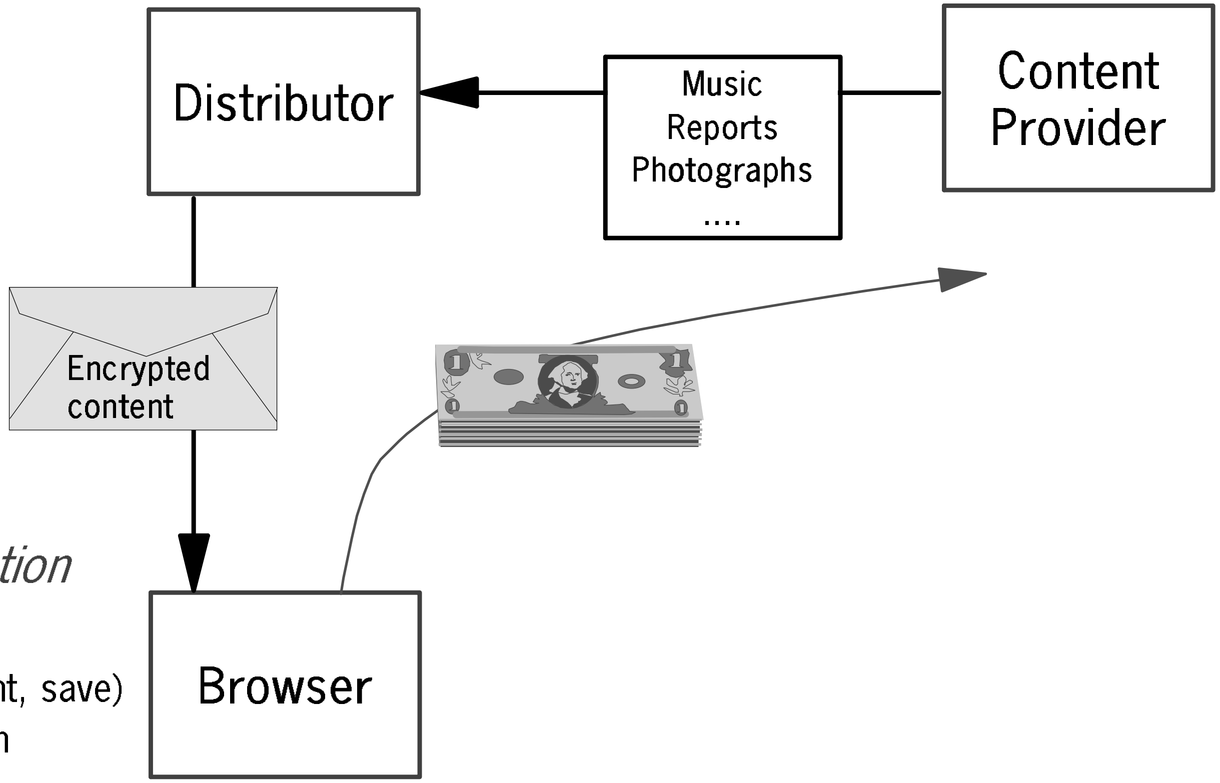


Encrypted mail can only be opened by intended recipients who have the private key

Cryptolope

An IBM Secure Packaging Technology

- Enable new distribution channels (Internet)
- Protect against unauthorized distribution
- Receive payment for use

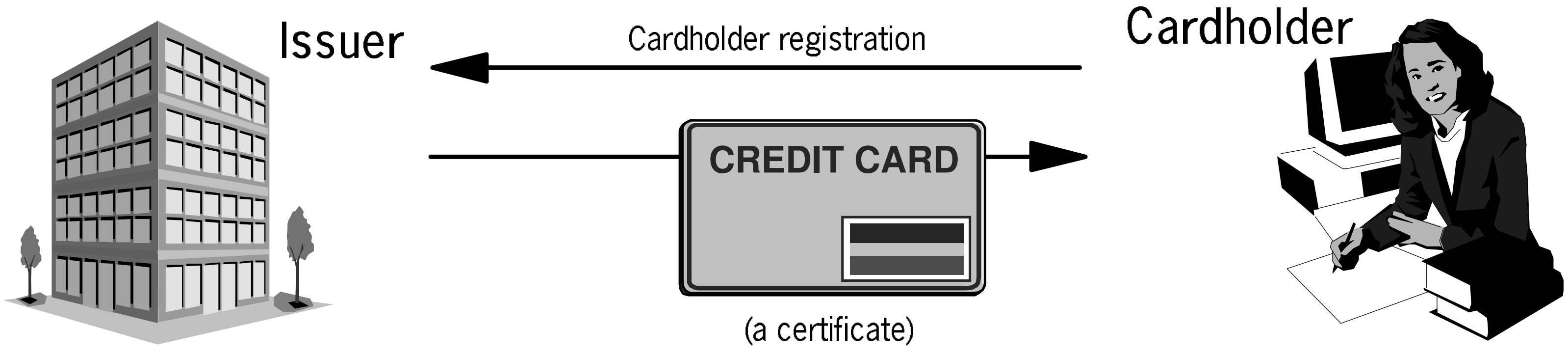


Browser Helper Application

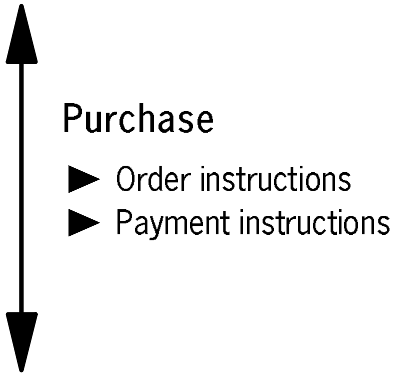
- View abstract
- Purchase rights (view, print, save)
- Receive key for decryption
- Track actions

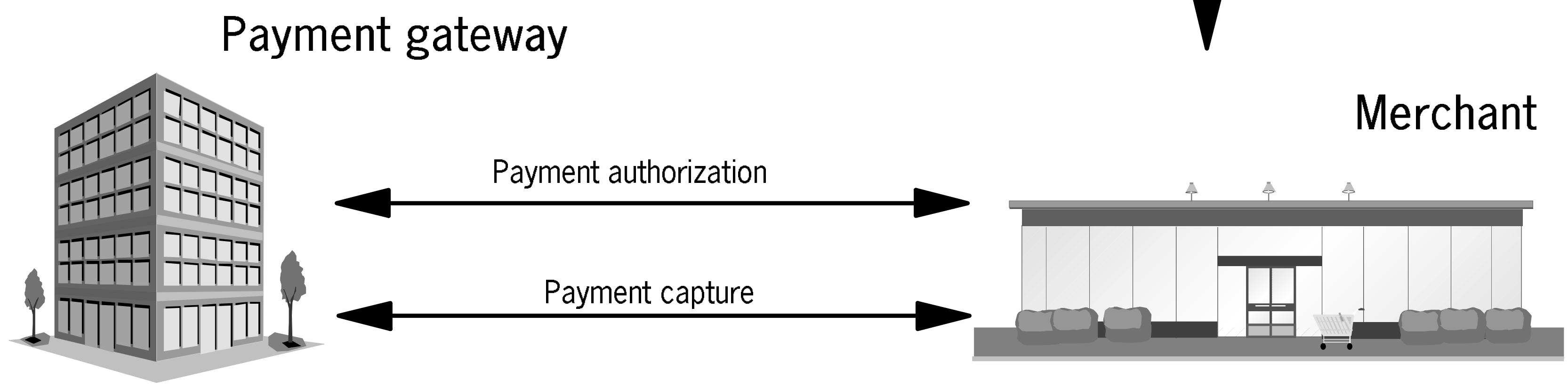
Secure Electronic Transactions (SET)

A secure electronic payment system



- Encryption provides confidentiality, integrity and authentication
- Certificate is electronic representation of branded payment card
- Merchant cannot see payment instructions (e.g. credit card)
- Payment gateway cannot see order instruction (e.g. items ordered)

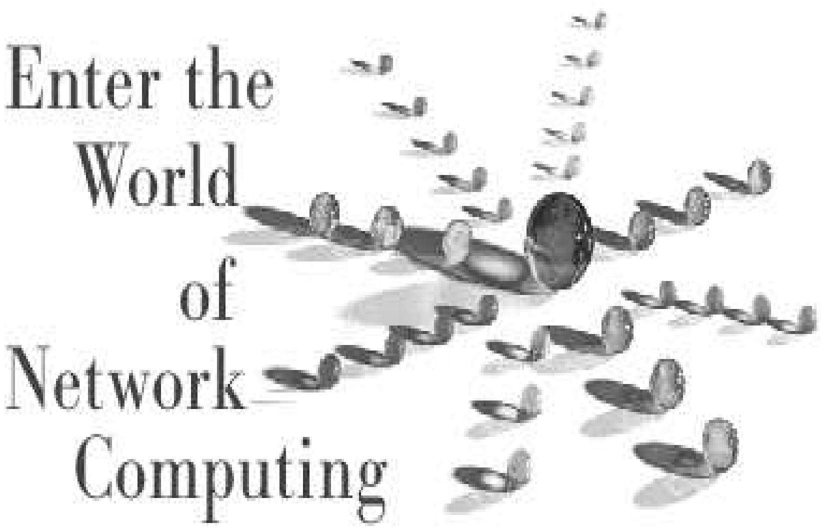




Internet Security 101 Summary

The Internet can be a reasonably safe place to do business

- Caution is advised, poor planning or mistakes could be disastrous
- Internet security is rapidly changing, everything is not mature yet
- Many security products and services from many vendors
- Cryptography plays a major role
- Ultimately should be more secure than paper solutions we use every day



Trademarks

AS/400, IBM, OS/400 and Cryptolope are trademarks of the IBM Corporation in the United States or other countries or both.

Java is a registered trademark of Sun Microsystems Inc.

Other company, product, and service names may be trademarks and service marks of others.