Controlling & Auditing
Information System

Magister SI UNIKOM

IT Security:

Protection of Information Assets

Basuki Rahmad, Dr, CISA, CISM

Chapter Overview

- Importance of Information Security Management
- Logical Access
- Network Infrastructure Security
- Auditing Information Security Management Framework
- Auditing Network Infrastructure Security
- Environmental Exposures and Controls
- Physical Access Exposures and Controls
- Mobile Computing

1. Importance of Information Security Management

Importance of Information Security Management

Security objectives to meet organization's business requirements include:

- Ensure the continued availability of their information systems
- Ensure the integrity of the information stored on their computer systems
- Ensure conformity to applicable laws, regulations and standards
- Ensure adherence to trust and obligation in relation to any information relating to an identified or identifiable individual
- Preserve the confidentiality of sensitive data in store and in transit

Key Elements

- Senior management commitment and support
- Policies and procedures
- Organization
- Security awareness and education
- Monitoring and compliance
- Incident handling and response

Roles and Responsibilities

- IS security steering committee
- Executive management
- Security advisory group
- Chief privacy officer (CPO)
- Chief security officer (CSO)
- Process owners
- Information assets owners and data owners
- Users
- External parties
- Security specialists/advisors
- IT developers
- IS auditors

Inventory and Classification of Information Asset

Inventory record should include:

- Clear identification of asset
- Relative value to organization
- Location
- Security/risk classification
- Asset group
- Owner
- Designated custodian

Inventory and Classification of Information Asset

Data classification should define:

- The owner of information asset
- Who has access rights and to what?
- What level of access should be granted?
- Who is responsible for determining the access rights and access levels?
- What approvals are needed for access?
- The extent and depth of security controls

System Access Permissions

- Logically or physically based
- Need-to-know basis
- Four IT layers of security provided for networks
- Access to information resources
- Access capabilities
- Reviews of access authorization

Mandatory and Discretionary Access Controls

- Mandatory
  - Enforces corporate security policy
  - Compares sensitivity of information resources
- Discretionary
  - Enforces data owner-defined sharing of information resources

Discretionary Access Control

- Access control is based on
  - User's identity and
  - Access control rules
- Most common administration: owner based
  - Users can protect what they own
  - Owner may grant access to others
  - Owner may define the type of access given to others

ACL v.s. Capabilities

- ACL:
  - Per object based
  - Good for file systems
- Capabilities:
  - Per subject based
  - Good for environment with dynamic, short-lived subjects

Access Control Conditions

- **Data-dependent conditions**: access constraints based on the value of the accessed data
- **Time-dependent**: access constraints based on the time of the data access
- **Context-dependent**: access constraints based on combinations on data which can be accessed
- **History-dependent**: access constraints based on previously accessed data

DAC Overview

- Advantages:
  - Intuitive
  - Easy to implement

- Disadvantages:
  - Inherent vulnerability (look TH example)
  - Maintenance of ACL or Capability lists
  - Maintenance of Grant/Revoke
  - Limited power of negative authorization

Privacy Management Issues and the Role of IS Auditors

The goals of a privacy impact assessment are:

- Pinpoint the nature of personally identifiable information associated with business processes
- Document the collection, use, disclosure and destruction of personally identifiable information
- Ensure that accountability for privacy issues exists
- Be the foundation for informed policy, operations and system design decisions based on an understanding of privacy risk and the options available for mitigating that risk

Critical Success Factors to Information Security Management

- Information security policy
- Senior management commitment and support on security training
- Security awareness training
- Professional risk-based approach

Information Security and External Parties

- Identification of risks related to external parties
- Addressing security when dealing with customers
- Addressing security in third-party agreements

Human Resources Security and Third Parties

- Screening
- Terms and conditions of employment
- During employment
- Termination or change of employment
- Removal of access rights

Computer Crime Issues and Exposures

Threats to business include the following:

- Financial loss
- Legal repercussions
- Loss of credibility or competitive edge
- Blackmail/industrial espionage
- Disclosure of confidential, sensitive or embarrassing information
- Sabotage

Computer Crime Issues and Exposures (continued)

Possible perpetrators include:

- Hackers
- Script kiddies
- Crackers
- Employees (authorized or unauthorized)
  - IS personnel
  - End users
- Former employees
- Interested or educated outsiders
- Part-time and temporary personnel
- Third parties
- Accidental ignorant

Security Incident Handling and Response

Phase of incident response:

- Planning and preparation;
- Detection;
- Initiation;
- Recording;
- Evaluation;
- Containment;
- Eradication;
- Escalation;
- Response;
- Recovery;
- Closure;
- Reporting;
- Postincident review;
- Lesson learned

2. Logical Access

Logical Access

Logical access controls are the primary means of managing and protecting resources to reduce risks to a level acceptable to an organization.

Logical Access Exposures

- Data leakage
- Wire-tapping
- Trojan horses or backdoors
- Viruses
- Worms
- Logic bombs
- Denial of service attack
- Computer shutdown
- War driving
- Piggybacking
- Trap doors
- Asynchronous attacks
- Rounding down
- Salami techniques

Paths of Logical Access

General Points of Entry

- Network connectivity
- Remote access
- Operator console
- Online workstations or terminals

Logical Access Control Software

Prevents unauthorized access and modification to an organization's sensitive data and use of system-critical functions.

Logical Access Control Software (continued)

General operating systems access control functions include:

- User identification and authentication mechanisms
- Assign user logon limitation rules
- Notification concerning proper use and access prior to initial login
- Create individual accountability and auditability
- Rules for access to specific information resources
- Create or change user profiles
- Log events
- Report capabilities

Logical Access Control Software (continued)

Database and/or application-level access control functions include:

- Create or change data files and database profiles
- Verify user authorization at the application and transaction levels
- Verify user authorization within the application
- Verify user authorization at the field level for changes within a database
- Verify subsystem authorization for the user at the file level
- Log database/data communications access activities for monitoring access violations

Identification and Authentication

- Logon-ids and passwords
  - Features of passwords
  - Password syntax (format) rules
- Token devices, one time passwords
- Biometric
  - Management of biometrics

Identification accuracy

- FAR = false acceptance rate
- FRR = false rejection rate
- EER = equal error rate
- TER = total error rate = FAR + FRR
- FER= false enrollment rate

Single Sign-on (SSO)

SSO is the process for consolidating all organization platform-based administration, authentication and authorization functions into a single centralized administrative function. A single sign-on product interfaces with:

- Client-server and distributed systems
- Mainframe systems
- Network security including remote access mechanisms

Identification and Authentication (continued)

Single Sign-on (SSO) advantages

- Multiple passwords are no longer required, therefore, whereby a user may be more inclined and motivated to select a stronger password
- It improves an administrator's ability to manage users' accounts and authorizations to all associates systems
- It reduces administrative overhead in resetting forgotten passwords over multiple platforms and applications
- It reduces the time taken by users to log into multiple applications and platforms

Identification and Authentication (continued)

Single Sign-on (SSO) disadvantages include:

- Support for all major operating system environments is difficult
- The costs associated with SSO development can be significant when considering the nature and extent of interface development and maintenance that may be necessary
- The centralized nature of SSO presents the possibility of a single point of failure and total compromise of an organization's information assets

Authorization Issues

Typical access restrictions at the file level include:

- Read, inquiry or copy only
- Write, create, update or delete only
- Execute only
- A combination of the above

Authorization Issues (continued)

Access control lists refer to:

- Users (including groups, machines, processes) who have been given permission to use a particular system resource
- The types of access permitted

Authorization Issues (continued)

Logical access security administration

- Centralized environment
- Decentralized environment

Authorization Issues (continued)

Advantages of conducting security in a decentralized environment

- The security administration is on-site at the distributed location
- Security issues are resolved in a more timely manner
- Security controls are monitored on a more frequent basis

Authorization Issues (continued)

Risks associated with distributed responsibility for security administration

- Local standards might be implemented rather than those required
- Levels of security management might be below chat can be maintained by central administration
- Unavailability of management checks and audits

Authorization Issues (continued)

Remote Access Security

- Today's organizations require remote access connectivity to their information resources for different types of users such as employees, vendors, consultants, business partners and customer representatives. In providing this capability, a variety of methods and procedures are available to satisfy an organization's business need for this level of access.

Authorization Issues (continued)

Remote access security risks include:

- Denial of service
- Malicious third parties
- Misconfigured communications software
- Misconfigured devices on the corporate computing infrastructure
- Host systems not secured appropriately
- Physical security issues over remote users' computers

Authorization Issues (continued)

Remote access security controls include:

- Policy and standards
- Proper authorizations
- Identification and authentication mechanisms
- Encryption tools and techniques, such as the use of VPN
- System and network management

Authorization Issues (continued)

Remote access using personal digital assistants (PDAs)

- Control issues to address include:
  - Compliance
  - Approval
  - Standard PDA applications
  - Due care
  - Awareness training
  - PDA applications
  - Synchronization
  - Encryption
  - Virus detection and control
  - Device registration
  - Camera use

Authorization Issues (continued)

Access issues with mobile technology

- These devices should be strictly controlled both by policy and by denial of use. Possible actions include:

  - Banning all use of transportable drives in the security policy
  - Where no authorized used of USB ports exists, disabling use with a logon script which removes them form the system directory
  - If they are considered necessary for business use, encrypting
  - all data transported or saved by these devices

Authorization Issues (continued)

Audit logging in monitoring system access

- Provides management an audit trail to monitor activities of a suspicious nature, such as a hacker attempting brute force attacks on a privileged logon ID

Authorization Issues (continued)

Audit logging in monitoring system access (continued)

- Access rights to system logs
  - A periodic review of system-generated logs can detect security problems, including attempts to exceed access authority or gain system access during unusual hours

Authorization Issues (continued)

Audit logging in monitoring system access (continued)

- Tools for audit trails (logs) analysis
  - Audit reduction tools
  - Trends/variance-detection tools
  - Attack signature-detection tools

Authorization Issues (continued)

Audit logging in monitoring system access (continued)

- Cost consideration
- Audit concerns
  - Patterns or trends that indicate abuse of access privileges, such as concentration on a sensitive application
  - Violations (such as attempting computer file access that is not authorized) and/or use of incorrect passwords
  - Effectiveness of IDs and IPs and management of detected and prevented intrusion

Authorization Issues (continued)

Restrict and monitor access to computer features that bypass cost consideration

- Generally, only system software programmers should have access to:
  - Bypass label processing (BLP)
  - System exits
  - Special system logon IDs

Authorization Issues (continued)

Naming conventions for logical access controls

- Structures used to govern user access to the system and user authority to access/use computer resources, such as files, programs and terminals

Storing, Retrieving, Transporting and Disposing of Confidential Information

Management should define and implement procedures to prevent access to, or loss of, sensitive information and software from computers, disks, and other equipment or media when they are stored, disposed of or transferred to another user.

The Data Protection Rules

1. Fair obtaining & processing
   - Consent
2. Specified purpose
3. No disclosure
   - unless “compatible”
4. Safe and secure
5. Accurate, up-to-date
6. Relevant, not excessive
7. Retention period
8. Right of access

3. Network Infrastructure Security

LAN Security

Local area networks facilitate the storage and retrieval of programs and data used by a group of people. LAN software and practices also need to provide for the security of these programs and data.

- LAN risk and issues
- Dial-up access controls

Client-Server Security

Control techniques in place

- Securing access to data or application
- Use of network monitoring devices
- Data encryption techniques
- Authentication systems
- Use of application level access control programs

Threats Categorization

- Errors and omissions
- Fraud and theft committed by authorized or unauthorized users of the system
- Employee sabotage
- Loss of physical and infrastructure support
- Malicious hackers
- Industrial espionage
- Malicious code
- Foreign government espionage
- Threats to personal privacy

Wireless Security Threats and Risk Mitigation (continued)

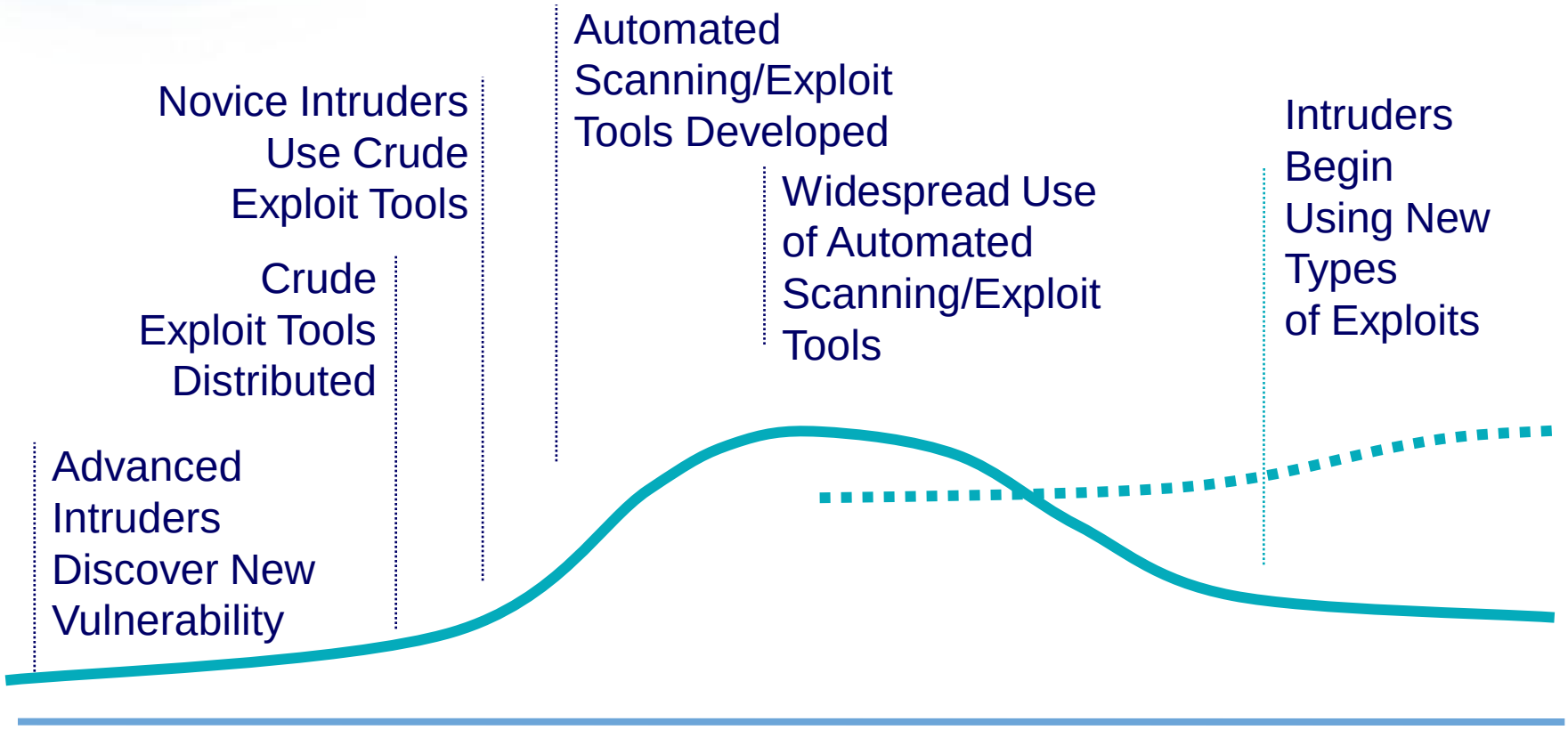
Security Requirements

- Authenticity
- Nonrepudiation
- Accountability
- Network availability

Network Security Threats

- Passive attacks
  - Network analysis
  - Eavesdropping
  - Traffic analysis
- Active attacks
  - Brute-force attack
  - Masquerading
  - Packet replay
  - Phishing
  - Message modification
  - Unauthorized access through the Internet or web-based services
  - Denial of service
  - Dial-in penetration attacks
  - E-mail bombing and spamming
  - E-mail spoofing

Vulnerability Exploit Cycle

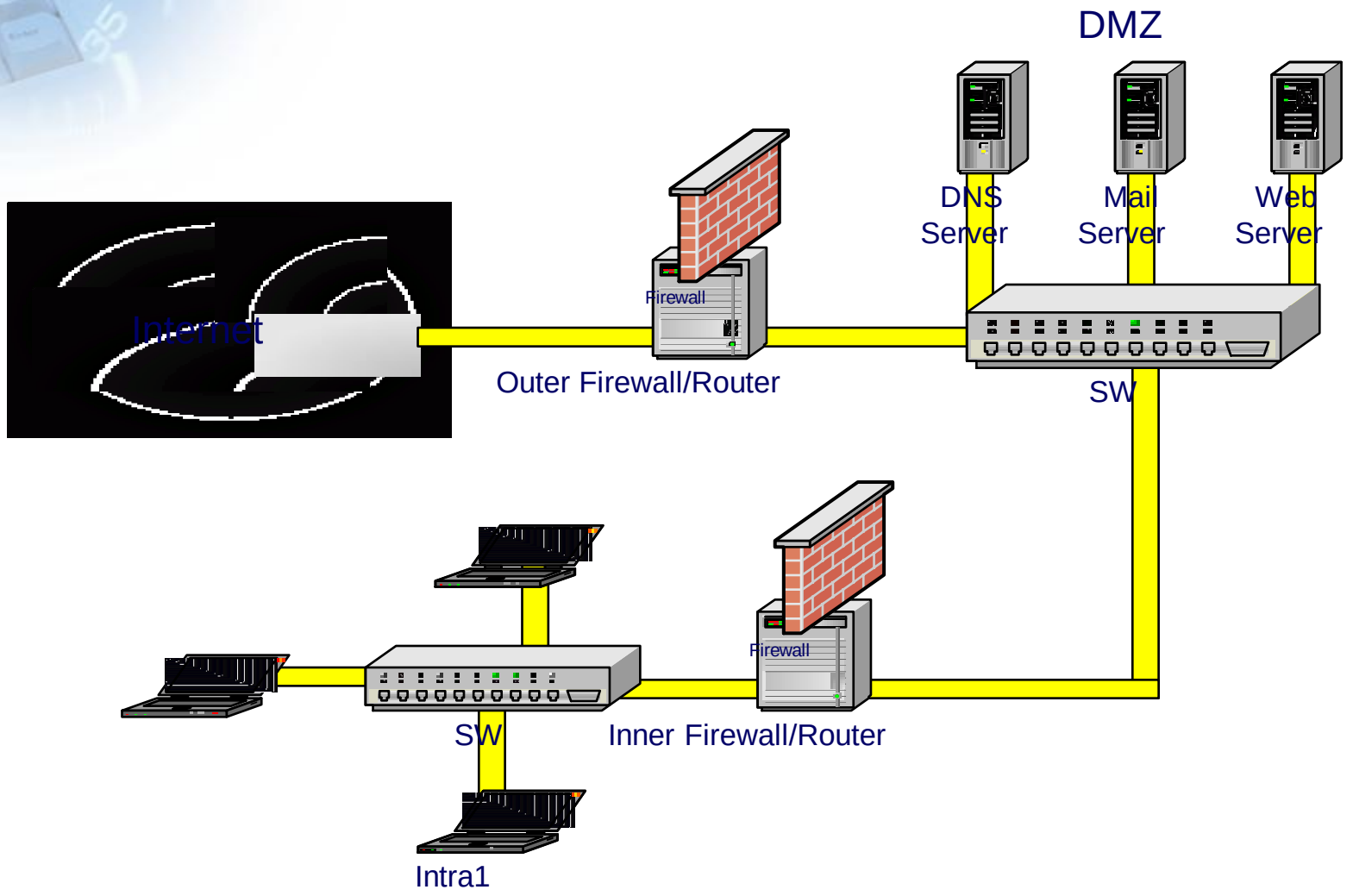


Internet Threats and Security (continued)

- Causal factors for internet attacks
  - Availability of tools and techniques on the Internet
  - Lack of security awareness and training
  - Exploitation of security vulnerabilities
  - Inadequate security over firewalls

- Internet security controls

Internet Threats and Security (continued)



Internet Threats and Security (continued)

Firewall Security Systems

- Firewall general features
- Firewall types
  - Router packet filtering
  - Application firewall systems
  - Stateful inspection

Firewall Security Systems (continued)

- Examples of firewall implementations
  - Screened-host firewall
  - Dual-homed firewall
  - Demilitarized zone (DMZ)

Firewall Basic Design : Examples

- Address filtering
  - Based on source and/or destination address in IP packets
  - Allowing packets with certain IP addresses to go through
  - Blocking packets with certain IP addresses
- Traffic type filtering
  - Based on the type of traffic in IP header (TCP/UDP port numbers)
  - Allowing certain types to go through. E.g http (port# 80)
- Content filtering
  - Based on the content of packets. Blocking packets with some patterns in the content.
- Specific filtering: ICMP message type, TCP SYN and ACK bits

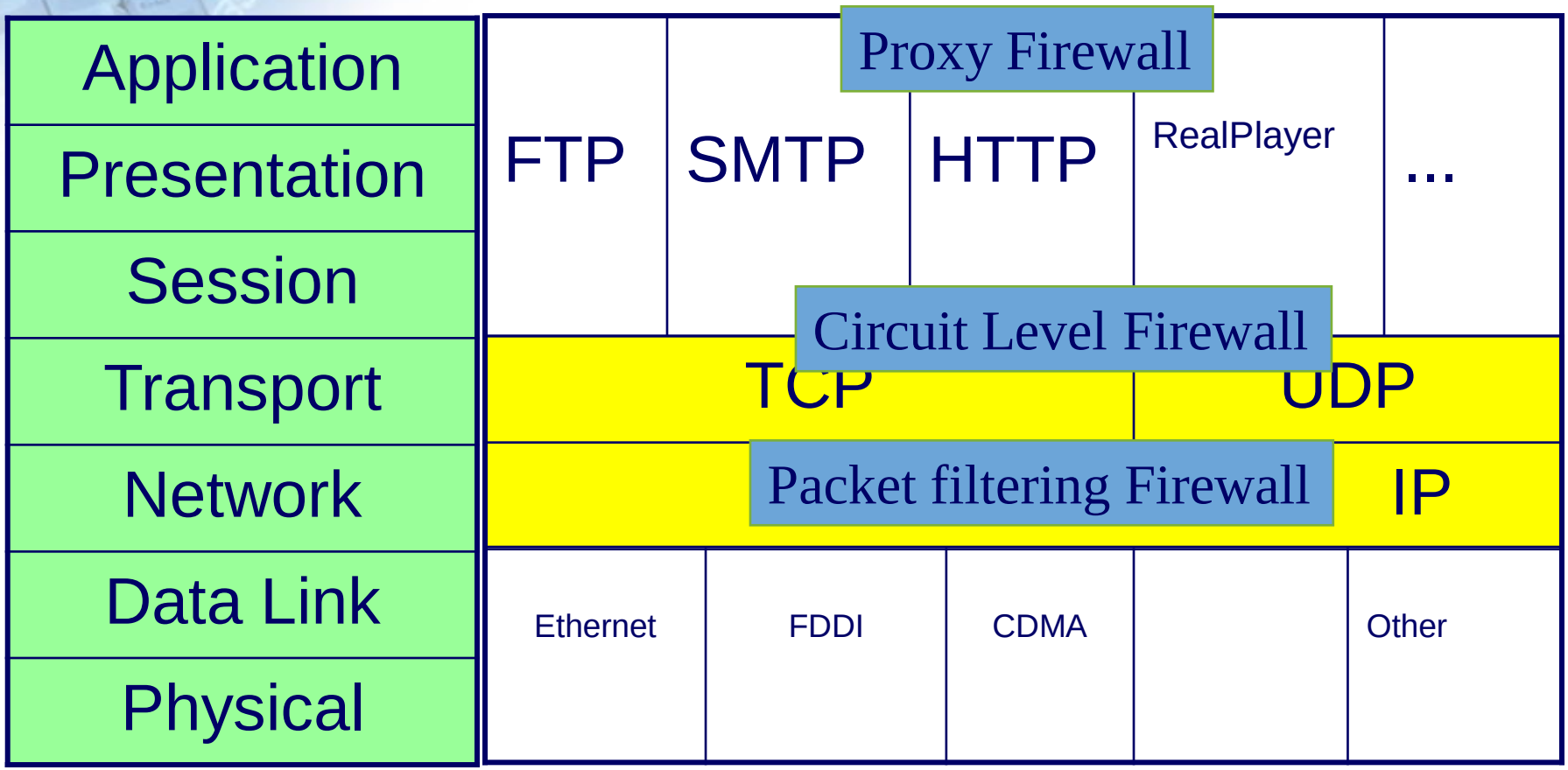
Firewall Security Systems (continued)

- Firewall issues
  - A false sense of security
  - The circumvention of firewall
  - Misconfigured firewalls
  - What constitutes a firewall
  - Monitoring activities may not occur on a regular basis
  - Firewall policies

Internet Threats and Security (continued)

- Firewall security systems
- Firewall platforms
  - Using hardware or software
  - Appliances versus normal servers

Firewalls at Different Layers



Intrusion Detection Systems (IDS)

An IDS works in conjunction with routers and firewalls by monitoring network usage anomalies.

- Network-based IDSs
- Host-based IDSs

Intrusion Detection Systems (IDS) (continued)

Components:

- Sensors that are responsible for collecting data
- Analyzers that receive inputo from sensors and determine intrusive activity
- An administration console
- A user interface

Intrusion Detection Systems (IDS) (continued)

Types include:

- Signature-based
- Statistical-based
- Neural networks

Intrusion Detection Systems (IDS) (continued)

Features:

- Intrusion detection
- Gathering evidence on intrusive activity
- Automated response
- Security monitoring
- Interface with system tolls
- Security policy management

Intrusion Detection Systems (IDS) (continued)

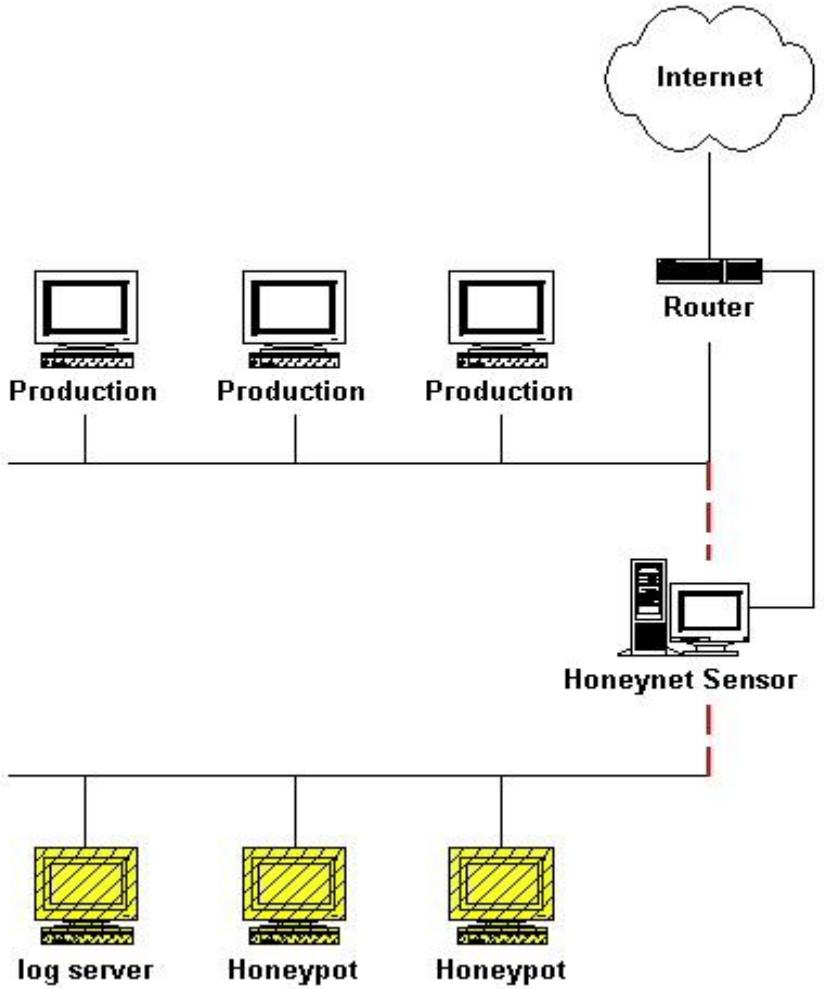
Limitations:

- Weaknesses in the policy definition
- Application-level vulnerabilities
- Backdoors into applications
- Weaknesses in identification and authentification schemes

Honeypots and Honeynets

- High interaction – Give hackers a real environment to attack
- Low interaction – Emulate production environments

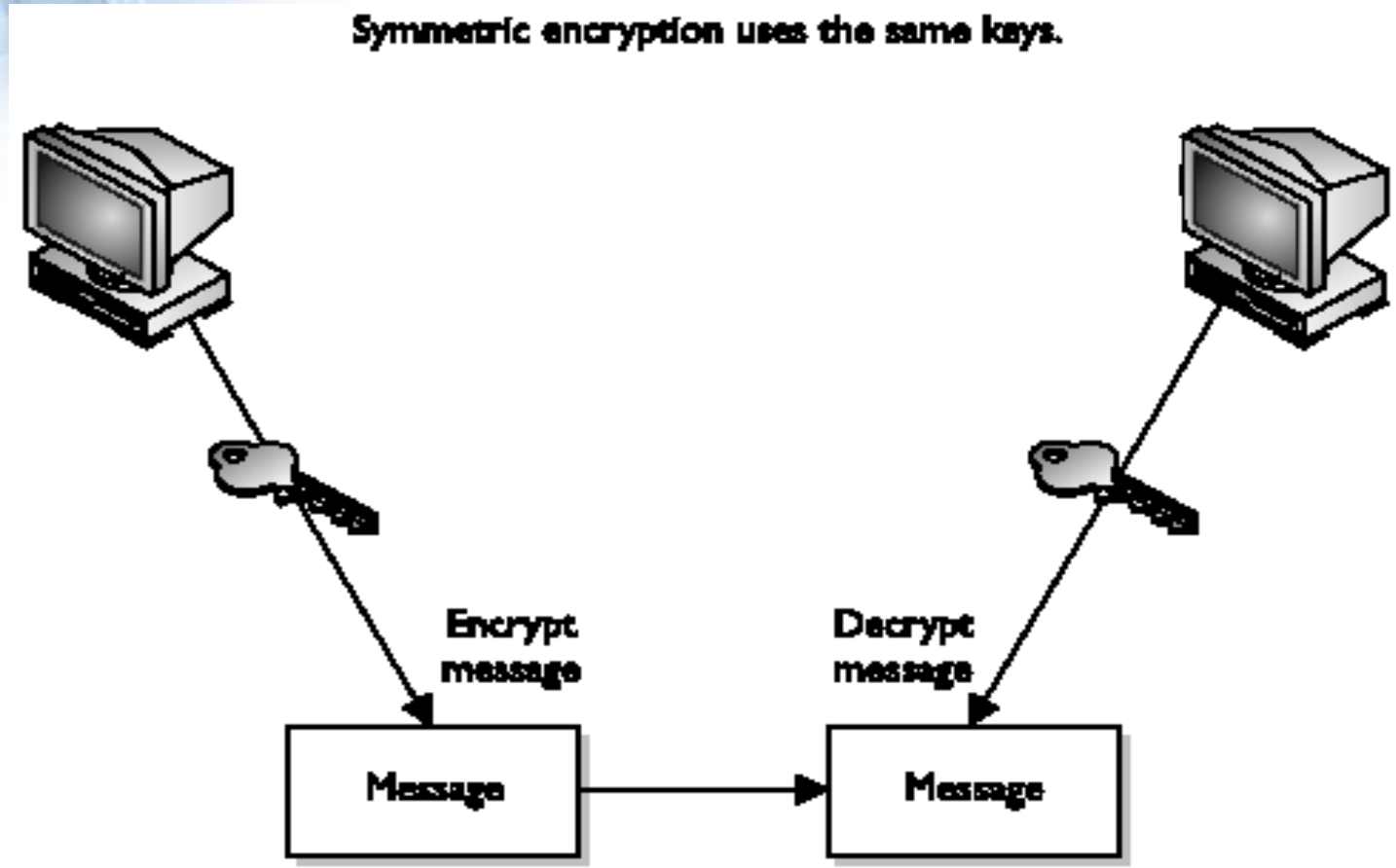
Internet Threats and Security (continued)



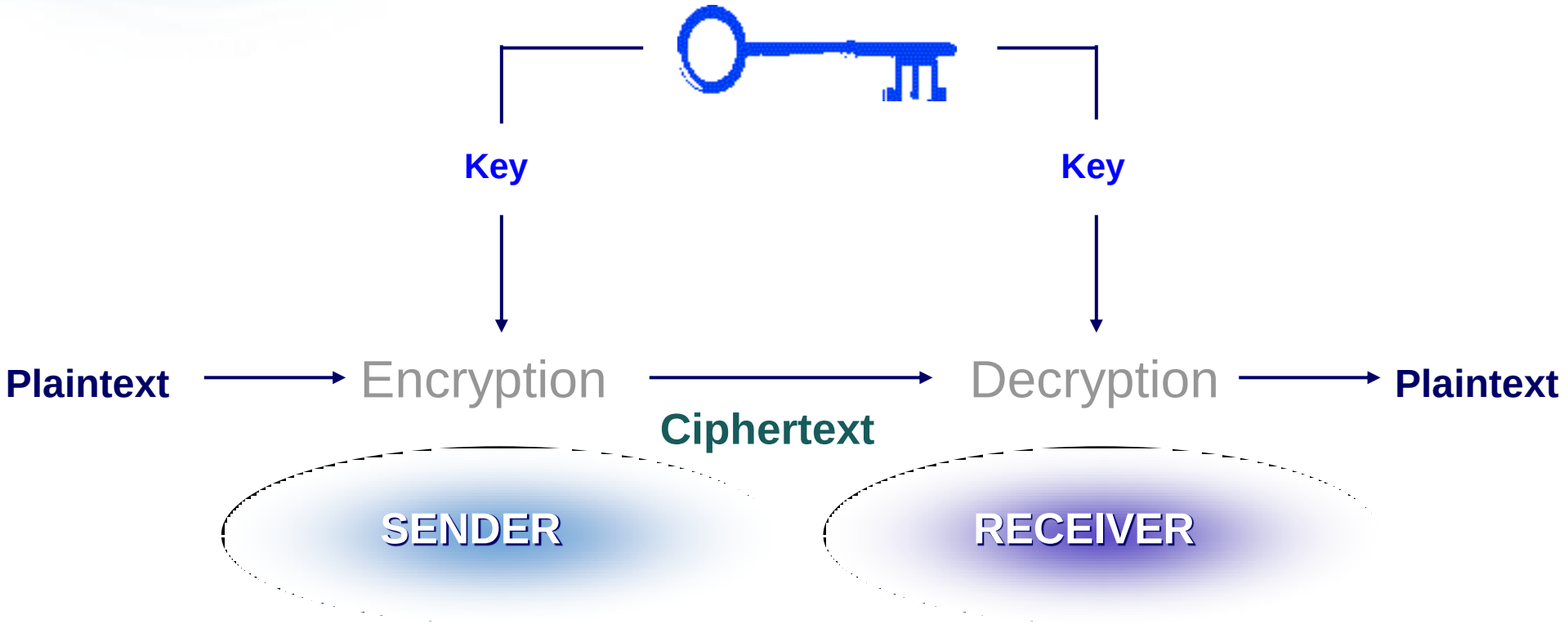
Encryption

- Key elements of encryption systems
  - Encryption algorithm
  - Encryption key
  - Key length
- Private key cryptographic systems
- Public key cryptographic systems

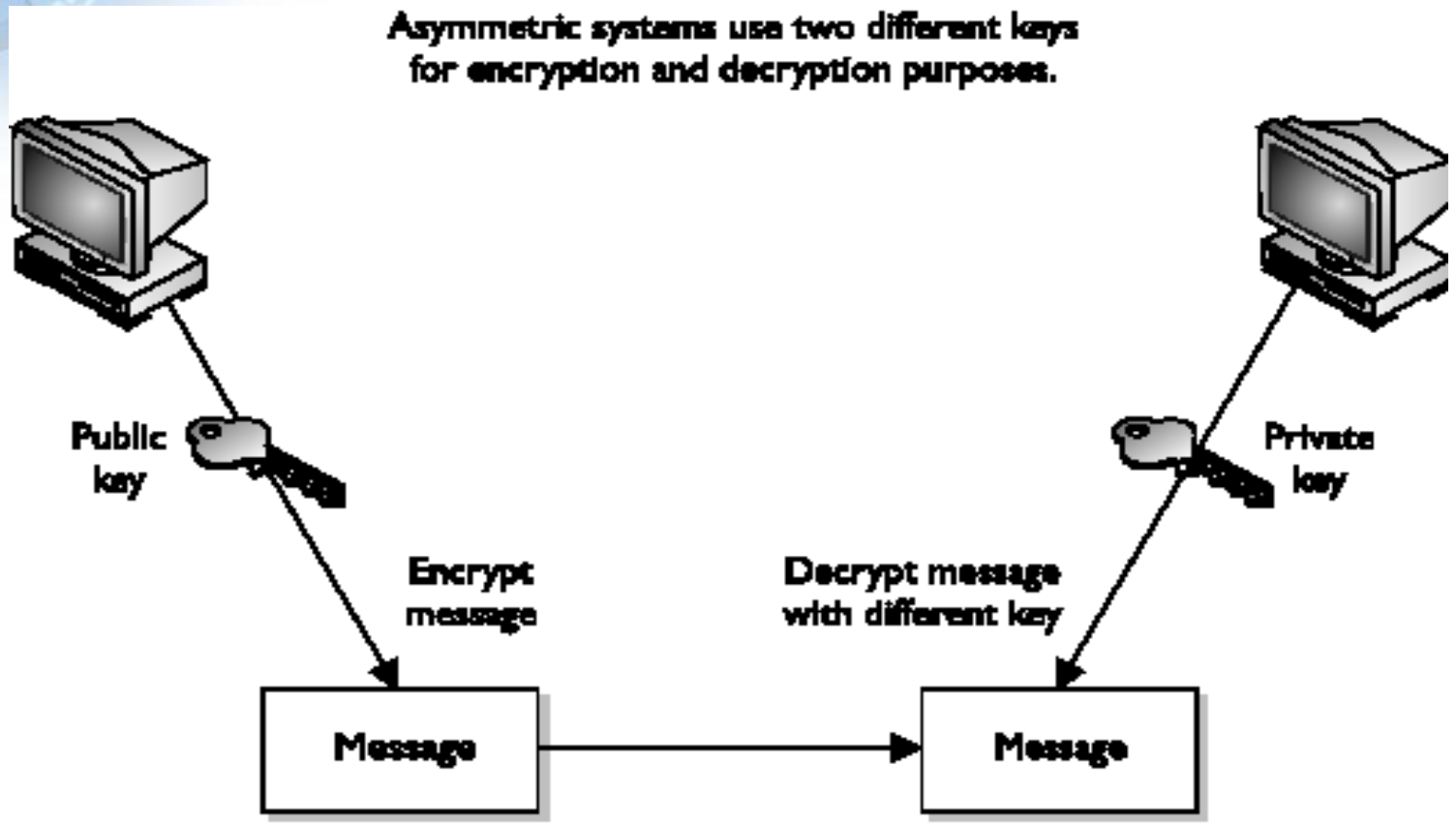
Encryption Private key cryptographic systems



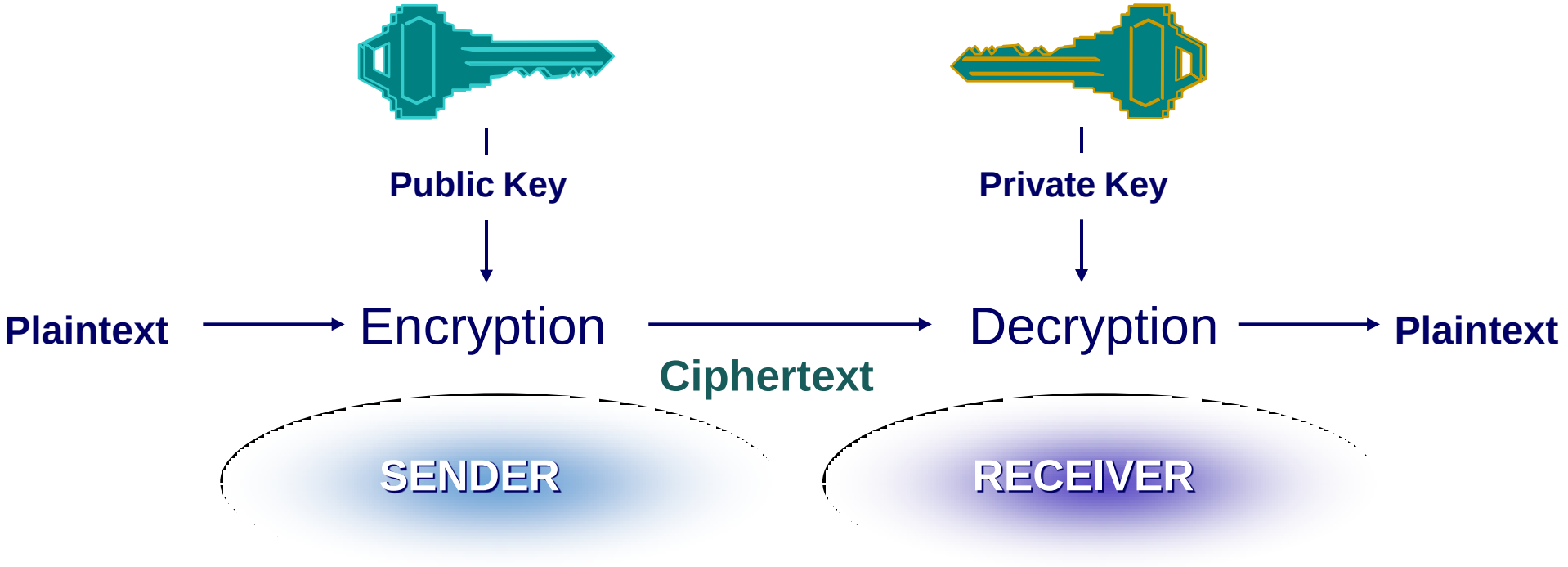
Symmetric Key Encryption



Encryption Public key cryptographic systems



Asymmetric Key Encryption



Encryption (continued)

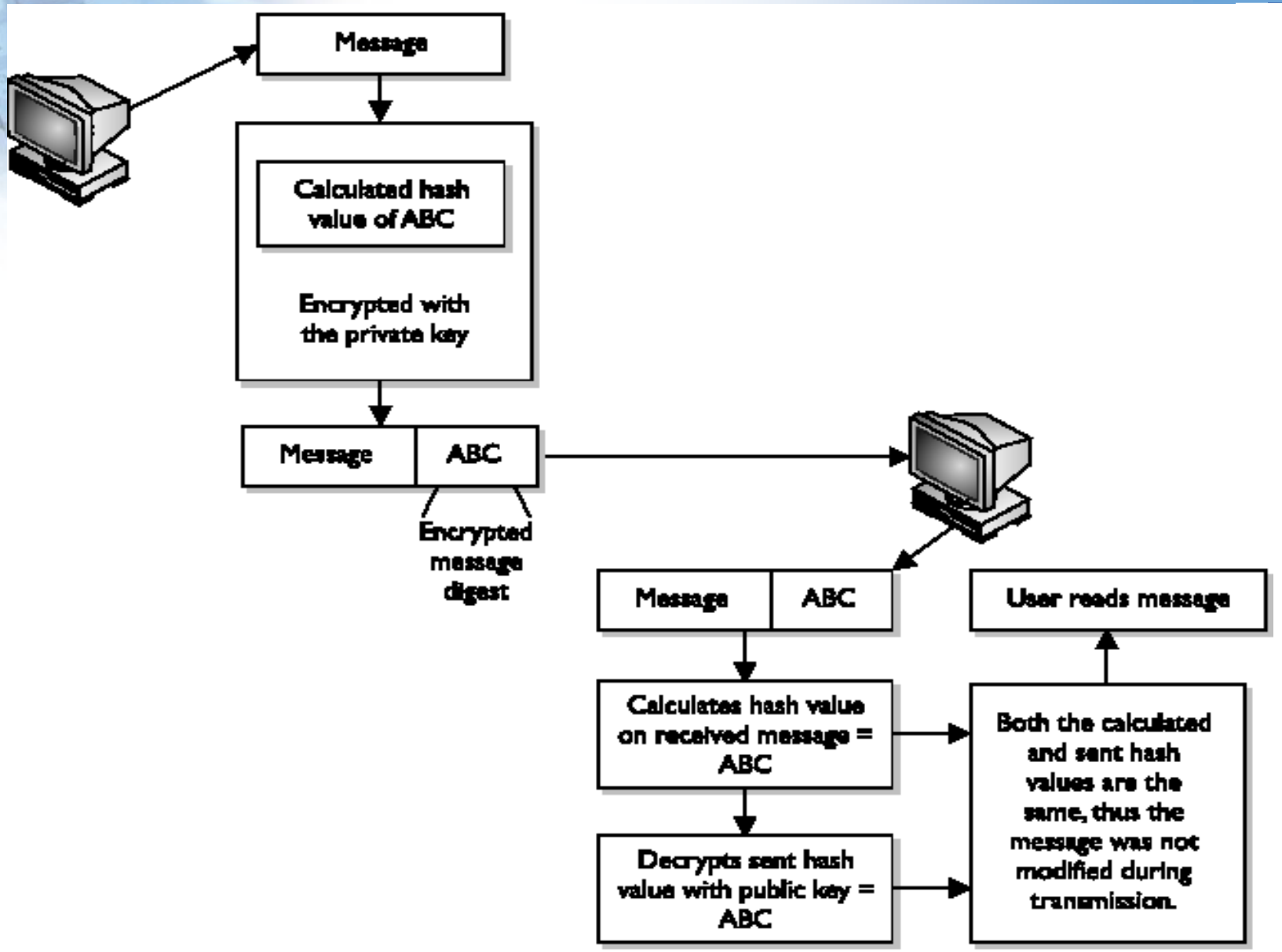
- Elliptical curve cryptosystem (ECC)
- Quantum cryptography
- Advanced Encryption Standard (AES)
- RSA
- Digital signatures

Encryption (continued)

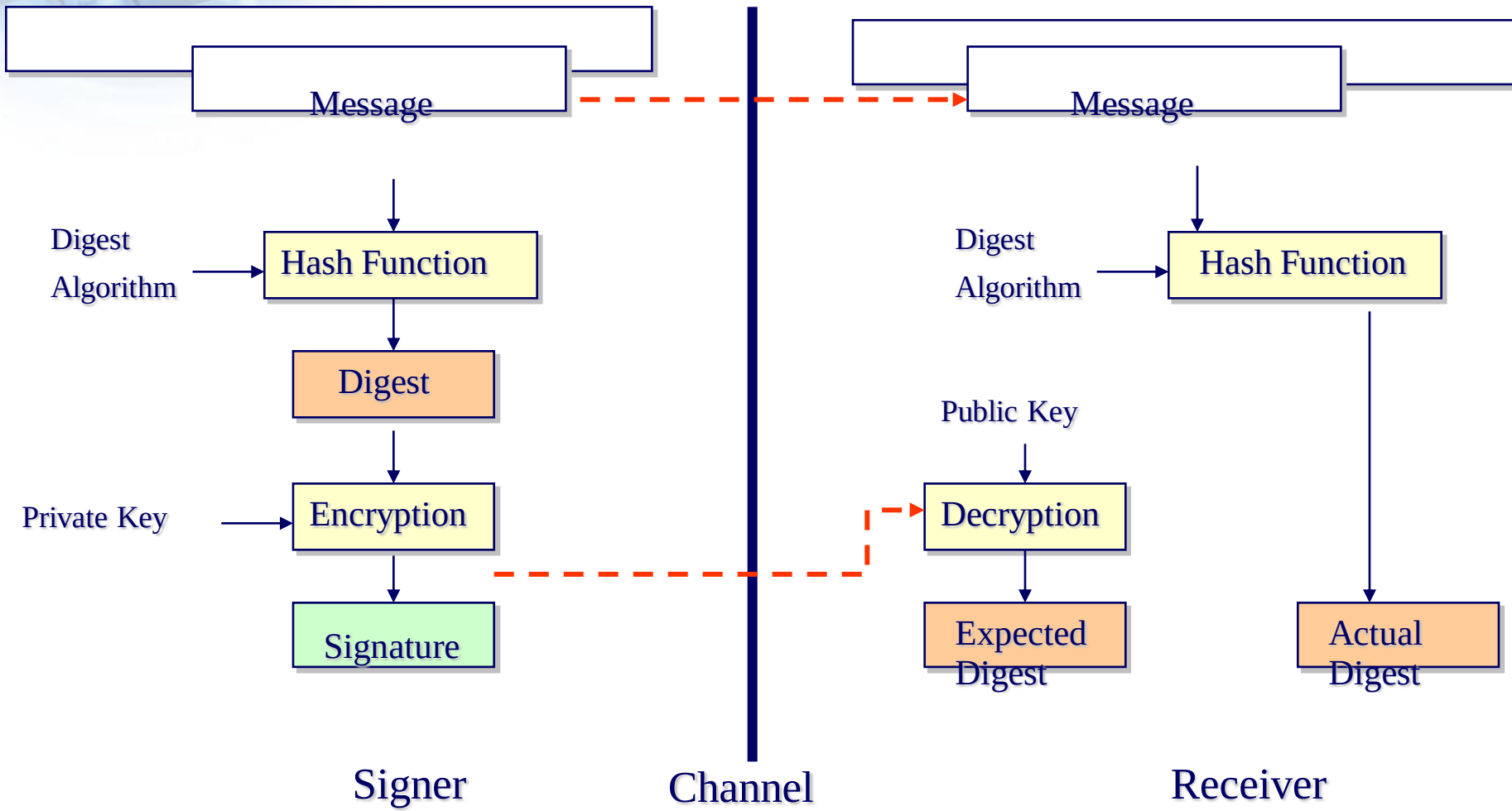
Digital Signatures

- Data integrity
- Authentication
- Nonrepudiation
- Replay protection

Digital Signatures



Digital Signature

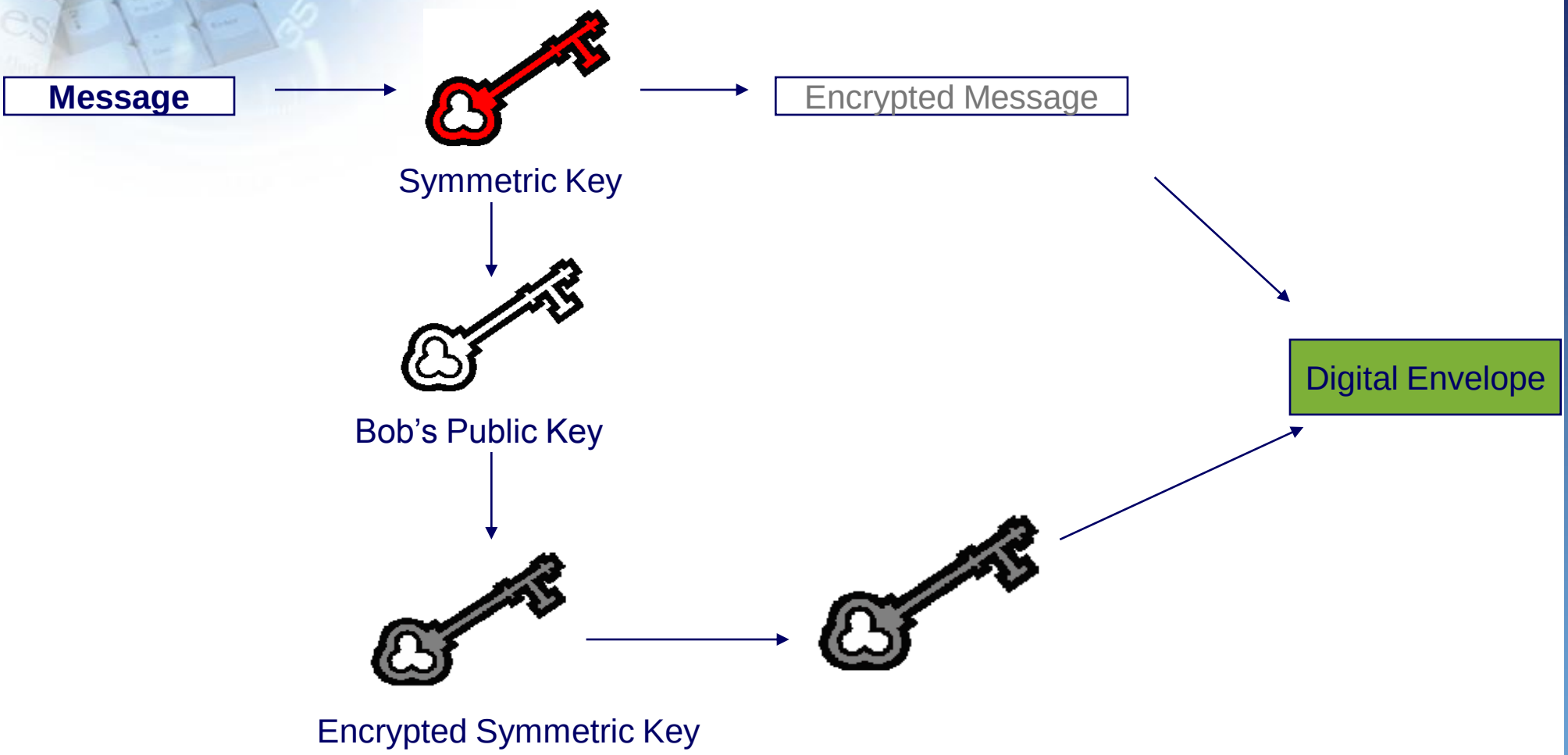


Encryption (continued)

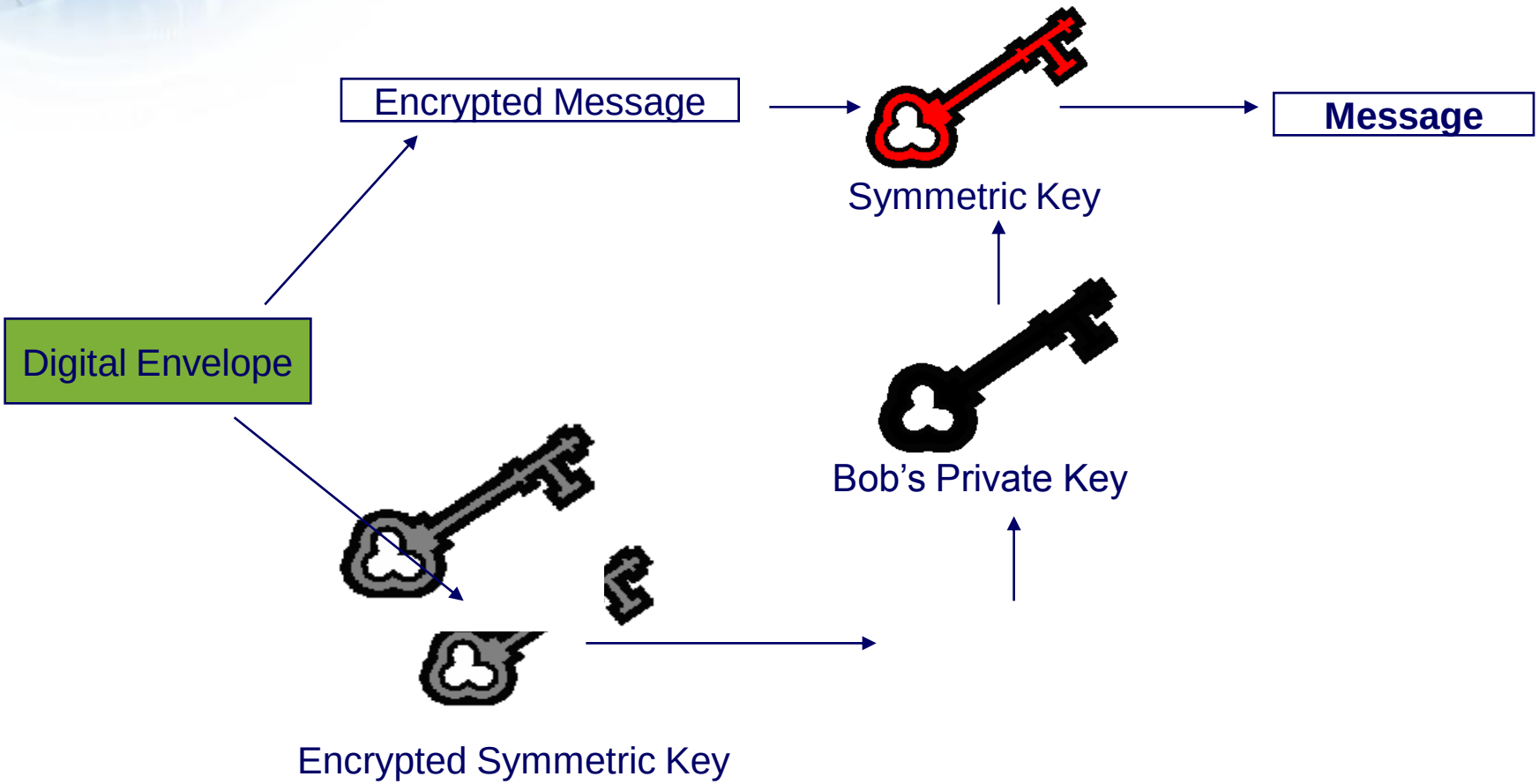
Digital Envelope

- Used to send encrypted information and the relevant key along with it
- The message to be sent, can be encrypted by using either:
  - Asymmetric key
  - Symmetric key

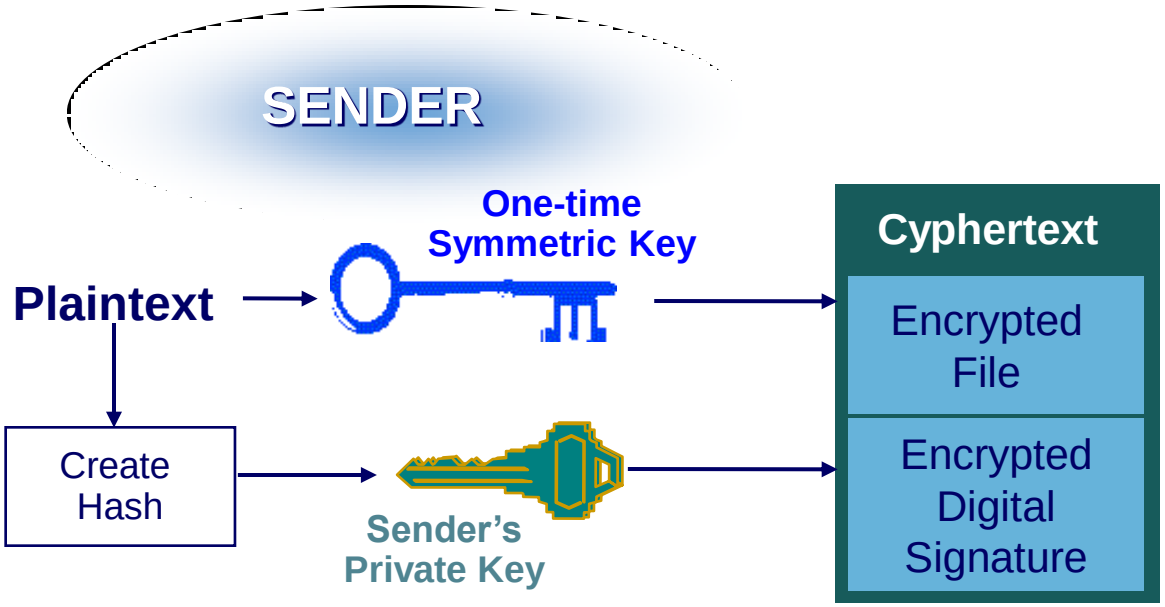
Putting it All Together



Putting it All Together

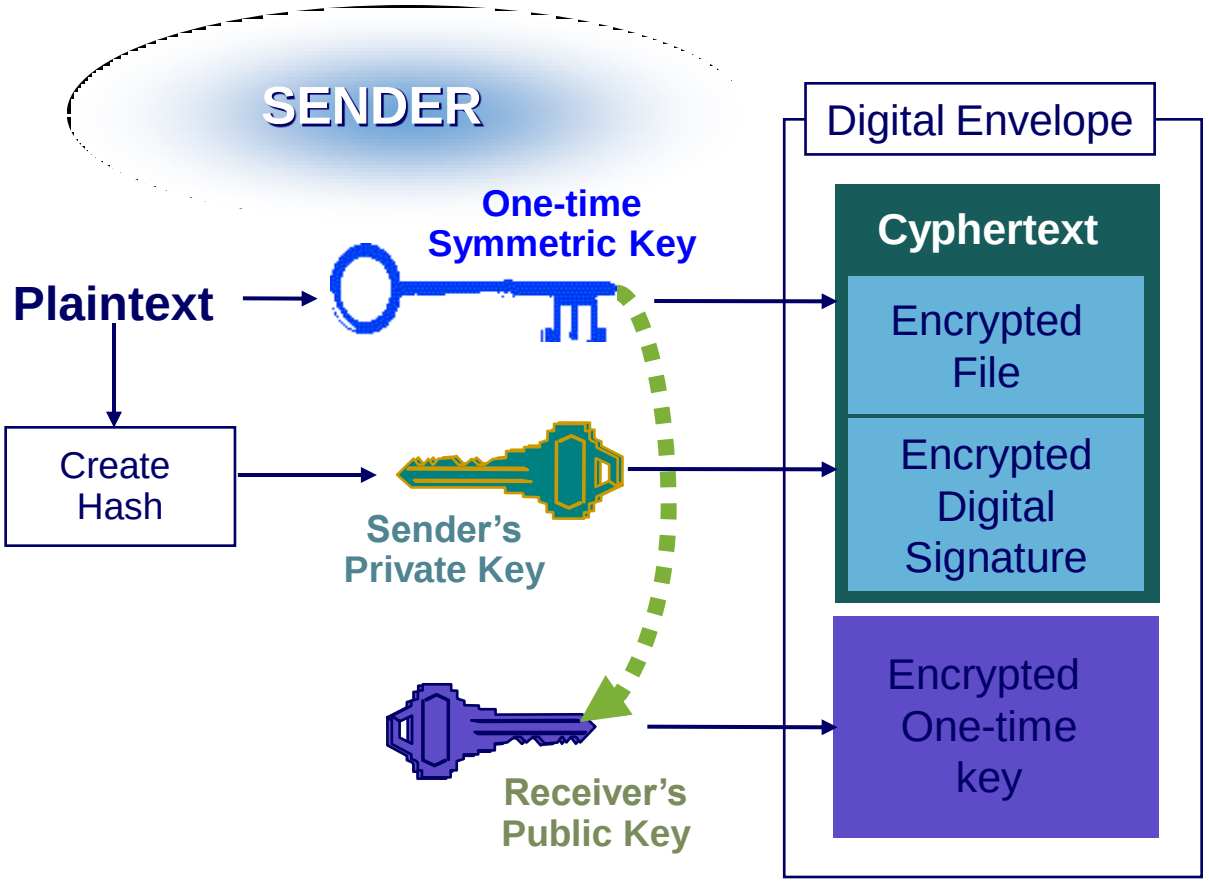


Security Overview



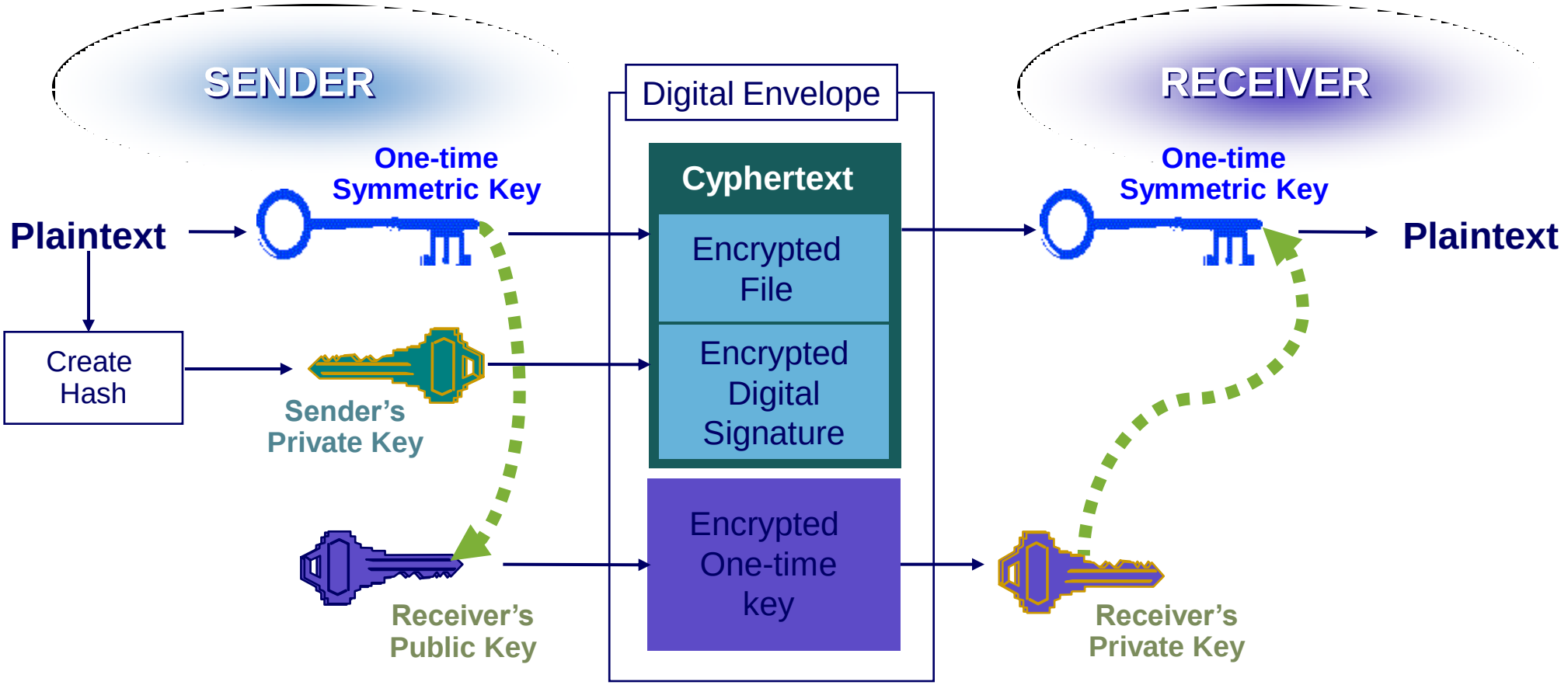
Encryption

Security Overview

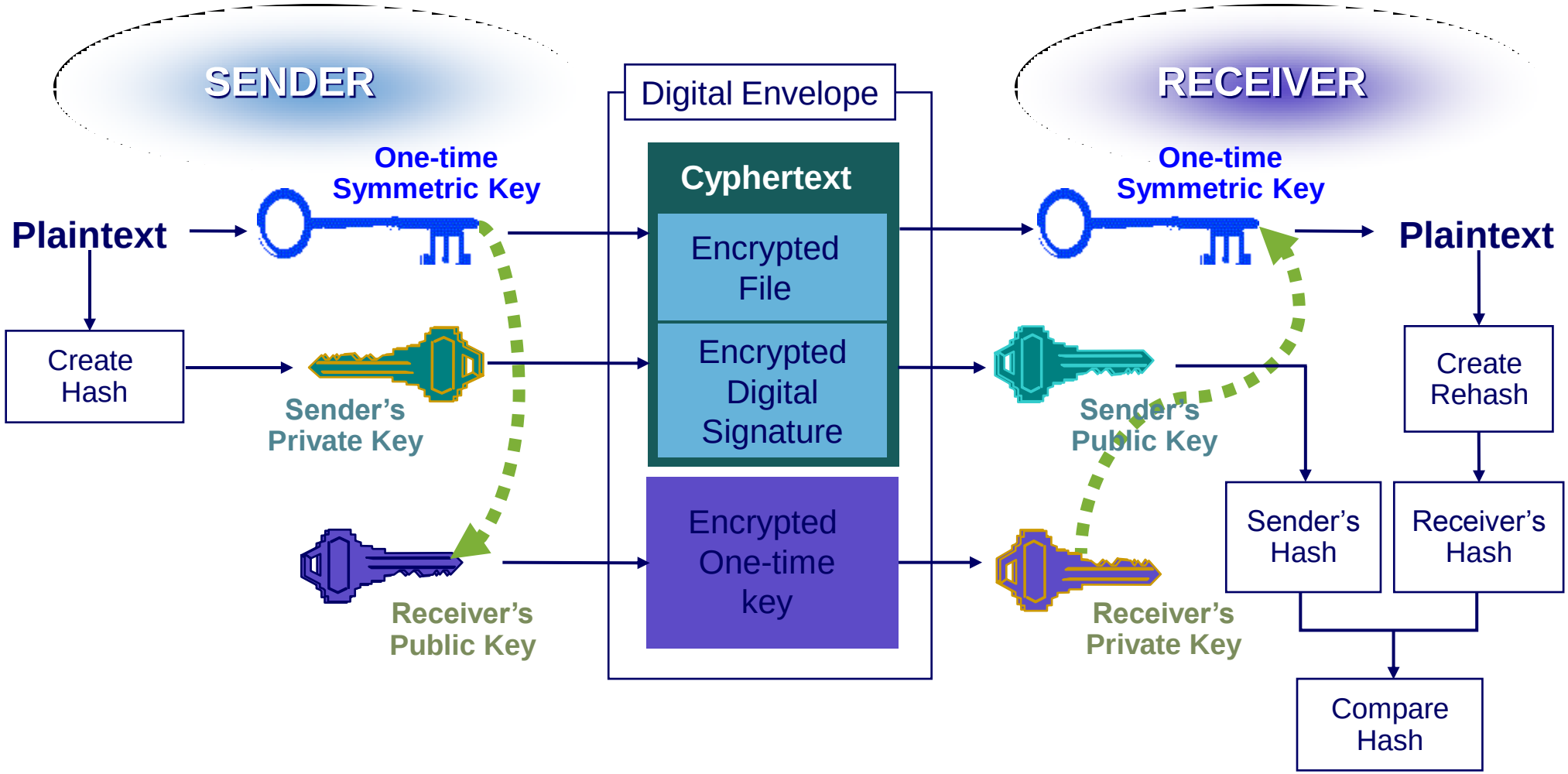


Encryption

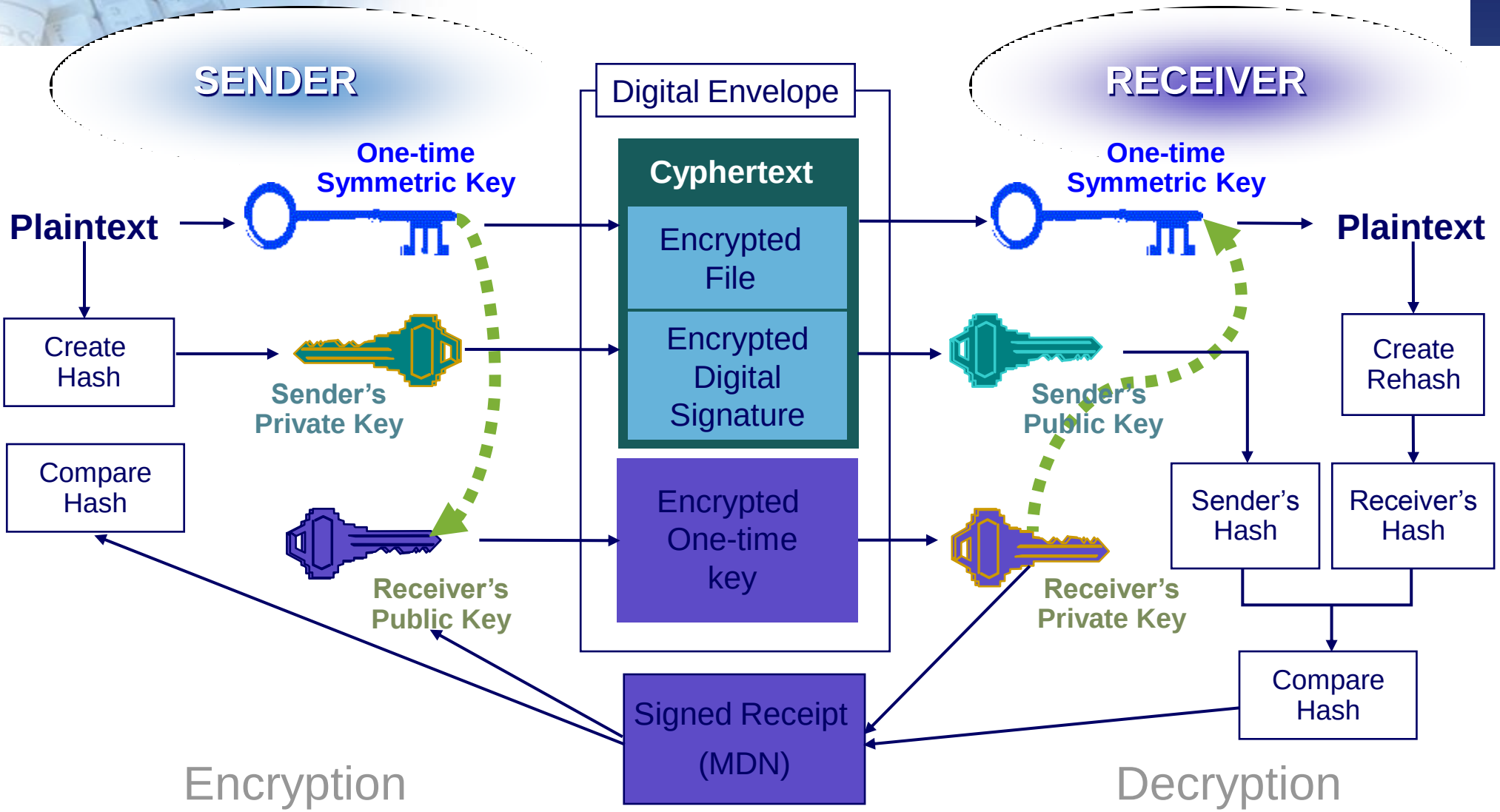
Security Overview



Security Overview



Security Overview



Encryption (continued)

Public Key Infrastructure

- Digital certificates
- Certificate authority (CA)
- Registration authority (RA)
- Certificate revocation list (CRL)
- Certification practice statement (CPS)

Digital Signature

There is still a problem linked to the *"Real Identity"* of the Signer.

Why should I trust what the Sender claims to be?



Moving towards PKI ...

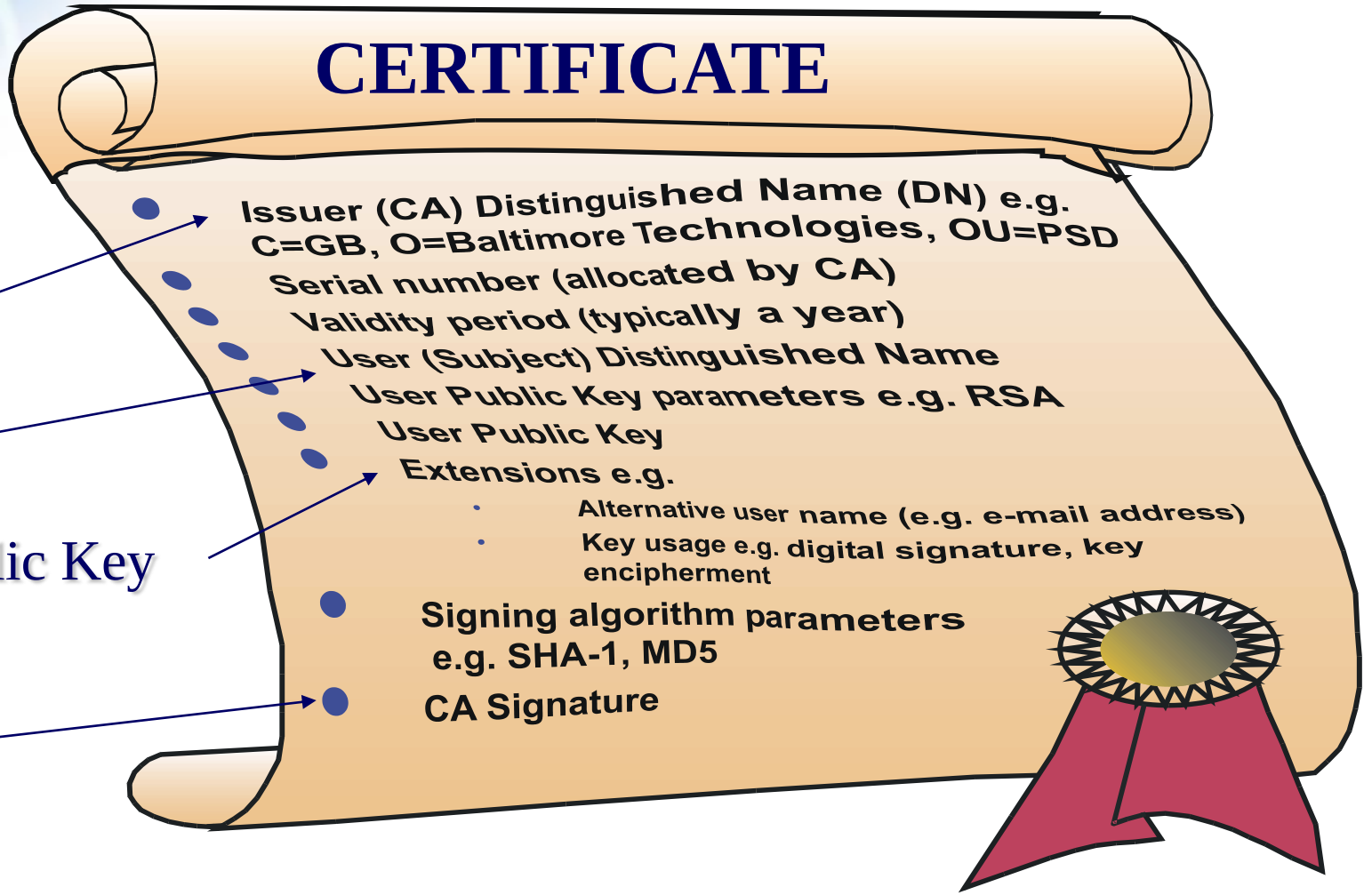
Digital Certificate

Digital Certificate

A Digital Certificate is a binding between an entity's Public Key and one or more Attributes relating its Identity.

- The entity can be a Person, an Hardware Component, a Service, etc.
- A Digital Certificate is issued (and signed) by someone
  - Usually the issuer is a Trusted Third Party
- A self-signed certificate usually is not very trustworthy

Digital Certificate



Digital Certificate

Problems

- How are Digital Certificates Issued?
- Who is issuing them?
- Why should I Trust the Certificate Issuer?
- How can I check if a Certificate is valid?
- How can I revoke a Certificate?
- Who is revoking Certificates?



Moving towards PKI ...

Public Key Infrastructure (PKI)

A Public Key Infrastructure is an Infrastructure to support and manage Public Key-based Digital Certificates

Public Key Infrastructure (PKI)

"A PKI is a set of agreed-upon standards, Certification Authorities (CA), structure between multiple CAs, methods to discover and validate Certification Paths, Operational Protocols, Management Protocols, Interoperable Tools and supporting Legislation"

"Digital Certificates" book – Jalal Feghhi, Jalil Feghhi, Peter Williams

Public Key Infrastructure (PKI)

Focus on:

- X509 PKI
- X509 Digital Certificates

➔ Standards defined by IETF, PKIX WG:

http://www.ietf.org/

... even if X509 is not the only approach (e.g. SPKI)

X509 PKI – Technical View

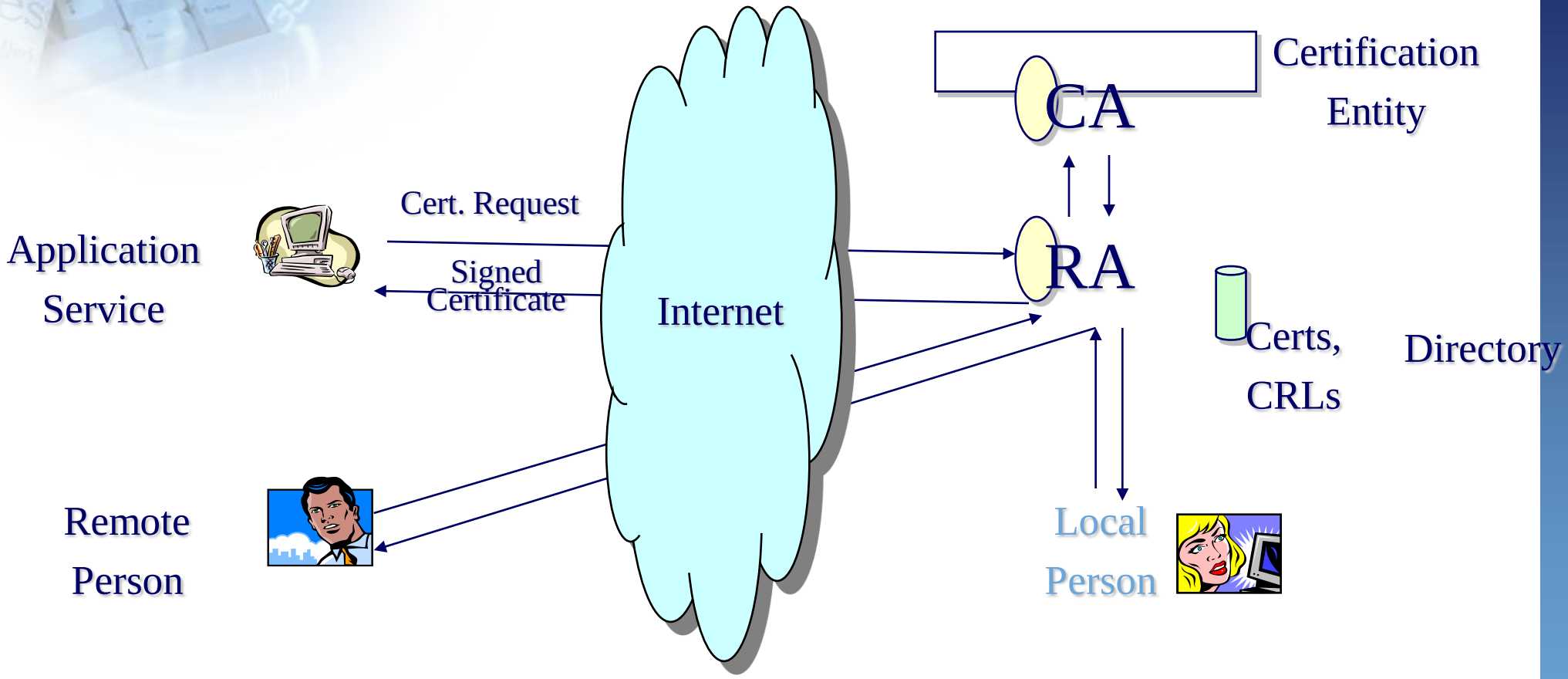
Basic Components:

- Certificate Authority (CA)
- Registration Authority (RA)
- Certificate Distribution System

} **"Provider" Side**

- PKI enabled applications → **"Consumer" Side**

X509 PKI – Simple Model



X509 PKI
Certificate Authority (CA)

Basic Tasks:

- Key Generation
- Digital Certificate Generation
- Certificate Issuance and Distribution
- Revocation
- Key Backup and Recovery System
- Cross-Certification

X509 PKI
Registration Authority (RA)

Basic Tasks:

- Registration of Certificate Information
- Face-to-Face Registration
- Remote Registration
- Automatic Registration
- Revocation

X509 PKI
Certificate Distribution System

Provide Repository for:

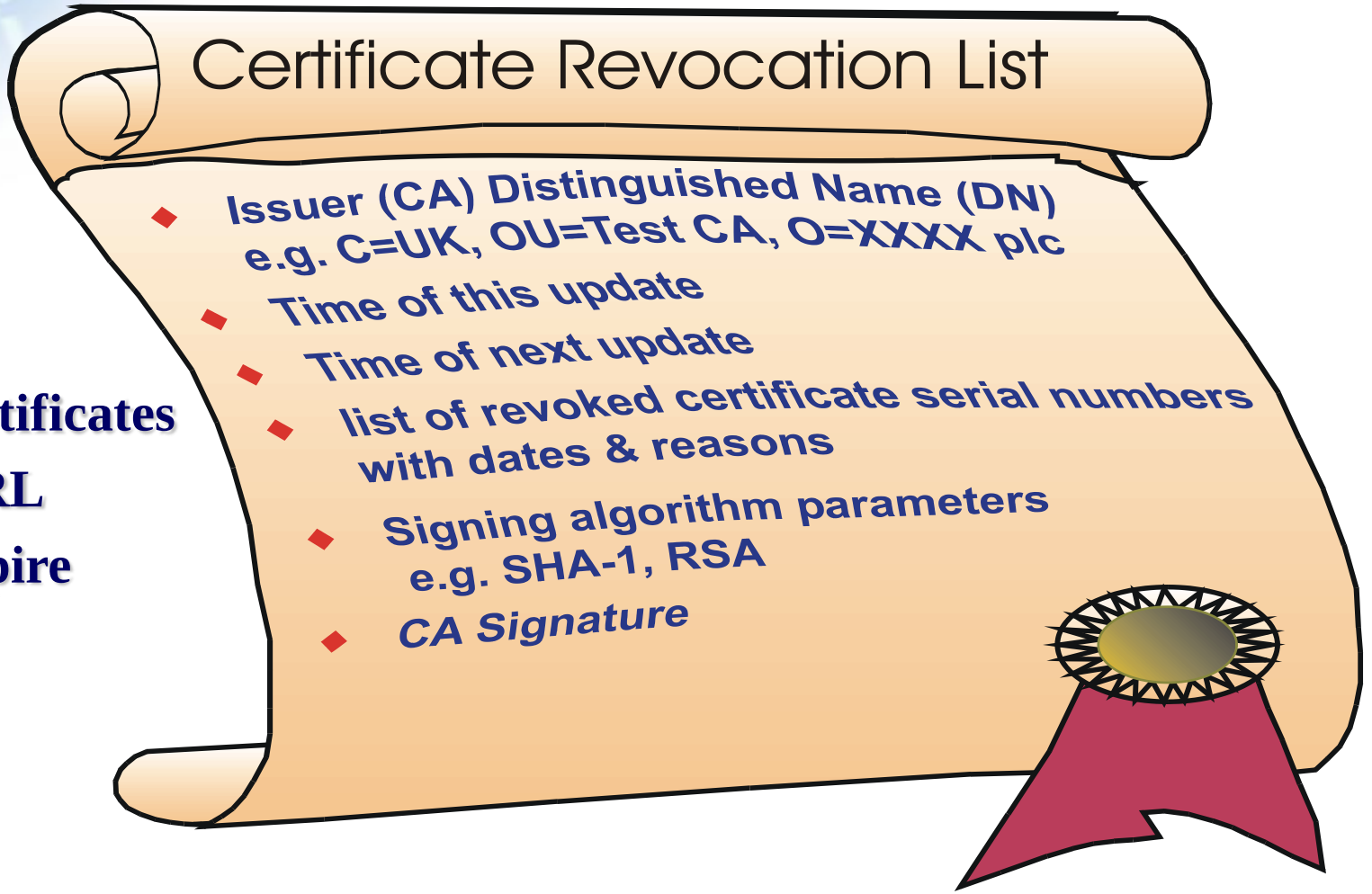
- Digital Certificates
- Certificate Revocation Lists (CRLs)

Typically:

- Special Purposes Databases
- LDAP directories

Certificate Revocation List

Revoked Certificates remain in CRL until they expire



Encryption (continued)

Use of encryption in OSI protocols

- Secure sockets layer (SSL)
- Secure Hypertext Transfer Protocol (S/HTTP)
- IP security
- SSH
- Secure multipurpose Internet mail extensions (S/MIME)
- Secure electronic transactions (SET)
- Encryption risks and password protection

Viruses

- Virus and worm controls
- Technical controls
- Anti-virus software implementation strategies Virus and worm controls
- Management procedural controls
- Technical controls
- Anti-virus software implementation strategies

Voice-Over IP

Advantages

- Unlike traditional telephony VoIP innovation progresses at market rates
- Lower costs per call, or even free calls, especially for long-distance calls
- Lower infrastructure costs. Once IP infrastructure is installed, no or little additional telephony infrastructure is needed.

Voice-Over IP (continued)

VoIP Security Issues

- Inherent poor security
  - The current Internet architecture does not provide the same physical wire security as the phone lines
- The key to securing VoIP
  - Security mechanisms such as those deployed in data networks (e.g., firewalls, encryption) to emulate the security level currently used by PSTN network users

4. Auditing Information Security Management Framework

Auditing Information Security Management Framework

- Review written policies, procedures and standards
- Logical access security policies
- Formal security awareness and training
- Data ownership (data classification scheme)
- Data owners

Auditing Information Security Management Framework (continued)

- Data custodians
- Security administrator
- New IT users
- Data users
- Documented authorizations
- Terminated employee access
- Access standards
- Security baselines
- Access standards

Auditing Logical Access

- Familiarization with the organization's IT environment
- Documenting the access paths
- Interviewing systems personnel
- Reviewing reports from access control software
- Reviewing application systems operations manual

Techniques for Testing Security

- Use of terminal cards and keys
- Terminal identification
- Logon-ids and passwords
- Controls over production resources
- Logging and reporting of computer access violations

Techniques for Testing Security (continued)

- Follow-up access violations
- Investigation of computer crime
- Protection of evidence
- Identification of methods of bypassing security and compensating controls
- Review access controls and password administration



5. Auditing Network Infrastructure Security

Auditing Remote Access

- Auditing Internet “points of presence”
- Network penetration tests
- Full network assessment reviews
- LAN networks assessments
- Development and authorization of network changes
- Unauthorized changes

Auditing Remote Access

Computer Forensics

- The process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in any legal proceedings.

6. Environmental Exposures and Controls

Environmental Issues and Exposures

Environmental exposures are due primarily to naturally occurring events, such as lightning storms, earthquakes, volcanic eruptions, hurricanes, tornados and other types of extreme weather conditions.

Environmental Issues and Exposures (continued)

Power failures can be grouped into distinct categories

- Total failure (blackout)
- Severely reduced voltage (brownout)
- Sags, spikes and surges
- Electromagnetic interference (EMI)

Controls for Environmental Exposures

- Alarm control panels
- Water detectors
- Handheld fire extinguishers
- Manual fire alarms
- Smoke detectors
- Fire suppression systems
- Strategically locating the computer room

Controls for Environmental Exposures (continued)

- Regular inspection by fire department
- Fireproof walls, floors and ceilings surrounding the computer room
- Electrical surge protectors
- Uninterruptible power supply/generator
- Emergency power-off switch
- Power leads from two substations

Controls for Environmental Exposures (continued)

- Wiring placed in electrical panels and conduit
- Prohibiting against eating, drinking and smoking within the information processing facility
- Fire resistant office materials
- Documented and tested emergency evacuation plans

Auditing Environmental Controls

- Water and smoke detectors
- Handheld fire extinguishers
- Fire suppression systems
- Regular inspection by fire department
- Fireproof walls, floors and ceilings surrounding the computer room
- Electrical surge protectors
- Power leads from two substations
- Fully documented and tested business continuity plan
- Wiring placed in electrical panels and conduit
- UPS/generator
- Documented and tested emergency evacuation plans
- Humidity/temperature control

7. Physical Access Exposures and Controls

Physical Access Issues and Exposures

Physical Access Exposures

- Unauthorized entry
- Damage, vandalism or theft to equipment or documents
- Copying or viewing of sensitive or copyrighted information
- Alteration of sensitive equipment and information
- Public disclosure of sensitive information
- Abuse of data processing resources
- Blackmail
- Embezzlement

Physical Access Controls

- Bolting door locks
- Combination door locks (cipher locks)
- Electronic door locks
- Biometric door locks
- Manual logging
- Electronic logging
- Identification badges (photo IDs)
- Video cameras
- Security guards
- Controlled visitor access
- Bonded personnel
- Deadman doors

Physical Access Controls

- Not advertising the location of sensitive facilities
- Computer workstation locks
- Controlled single entry point
- Alarm system
- Secured report/document distribution cart

Auditing Physical Access

- Touring the information processing facility (IPF)
- Testing of physical safeguards

Mobile Computing

Control reduce risk of disclosure of sensitive data stored on laptop:

- Engrave or brand serial number and company name and logo on laptop with electric engraver or tamper resistant tags;
- Use cable locking system or locking system with motion detector that sound audible alarm;
- Back-up business critical or sensitive data on regular basis at work and when traveling;
- Encrypt data using well-known encryption software;
- Allocate password to individual files to prevent them from being opened by unauthorized person;
- Establish a theft response team and develop procedure to follow when laptop is stolen.

Thank You !