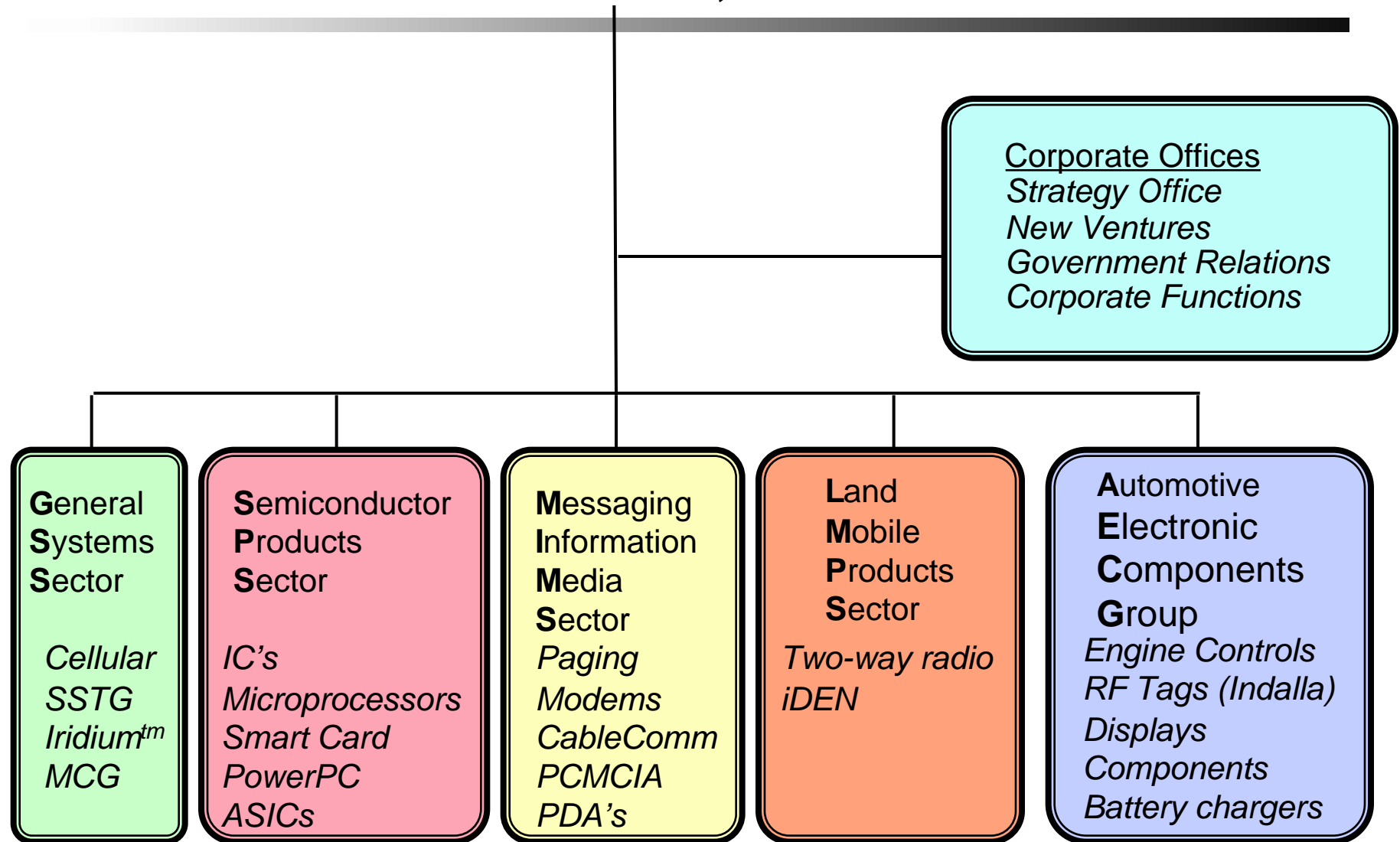


---

# **Flexibility and Confidence in Information Sharing**



# Motorola, Inc.

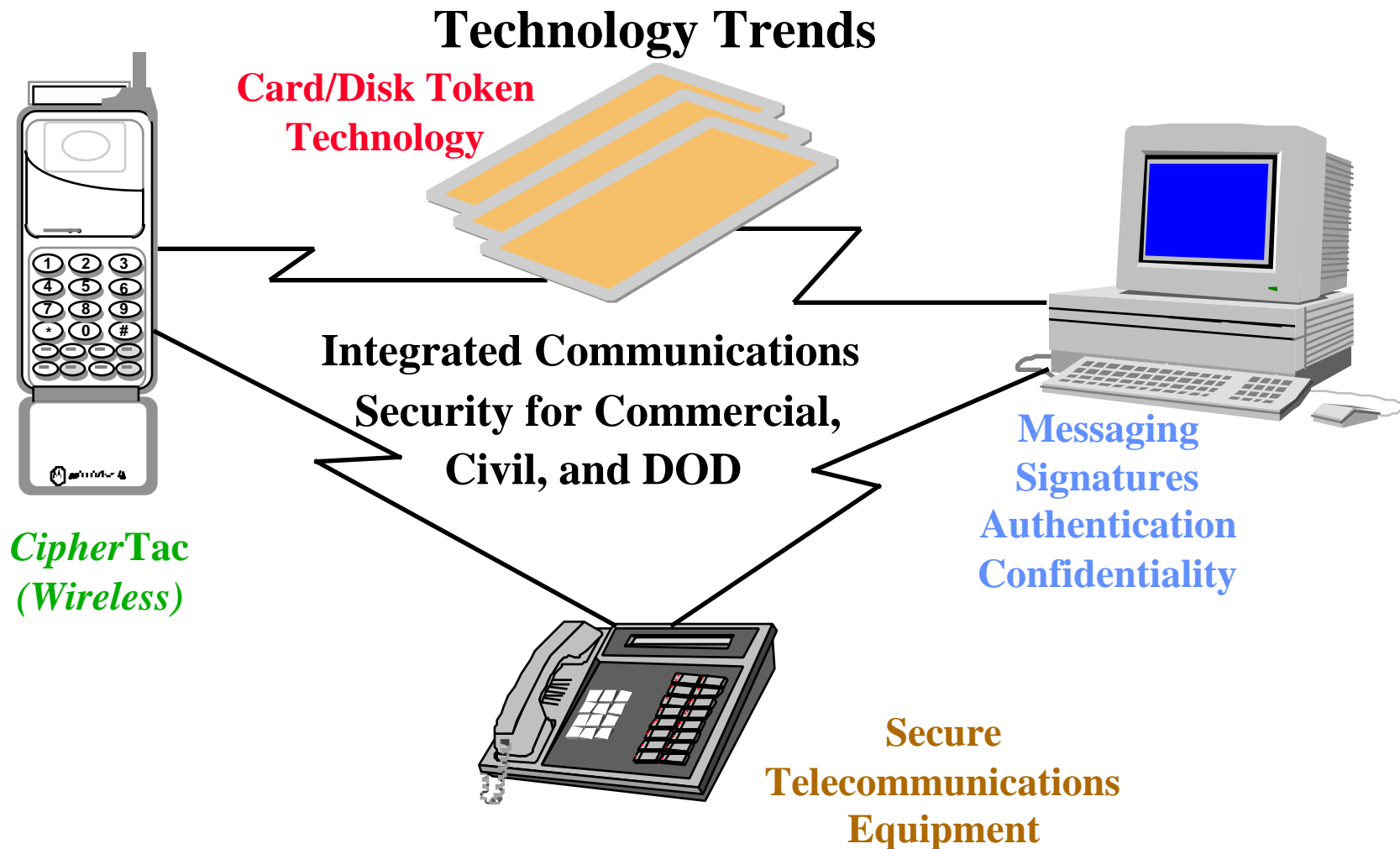


Integrated Security Solutions  
12/23/96



**MOTOROLA**

# Information Security



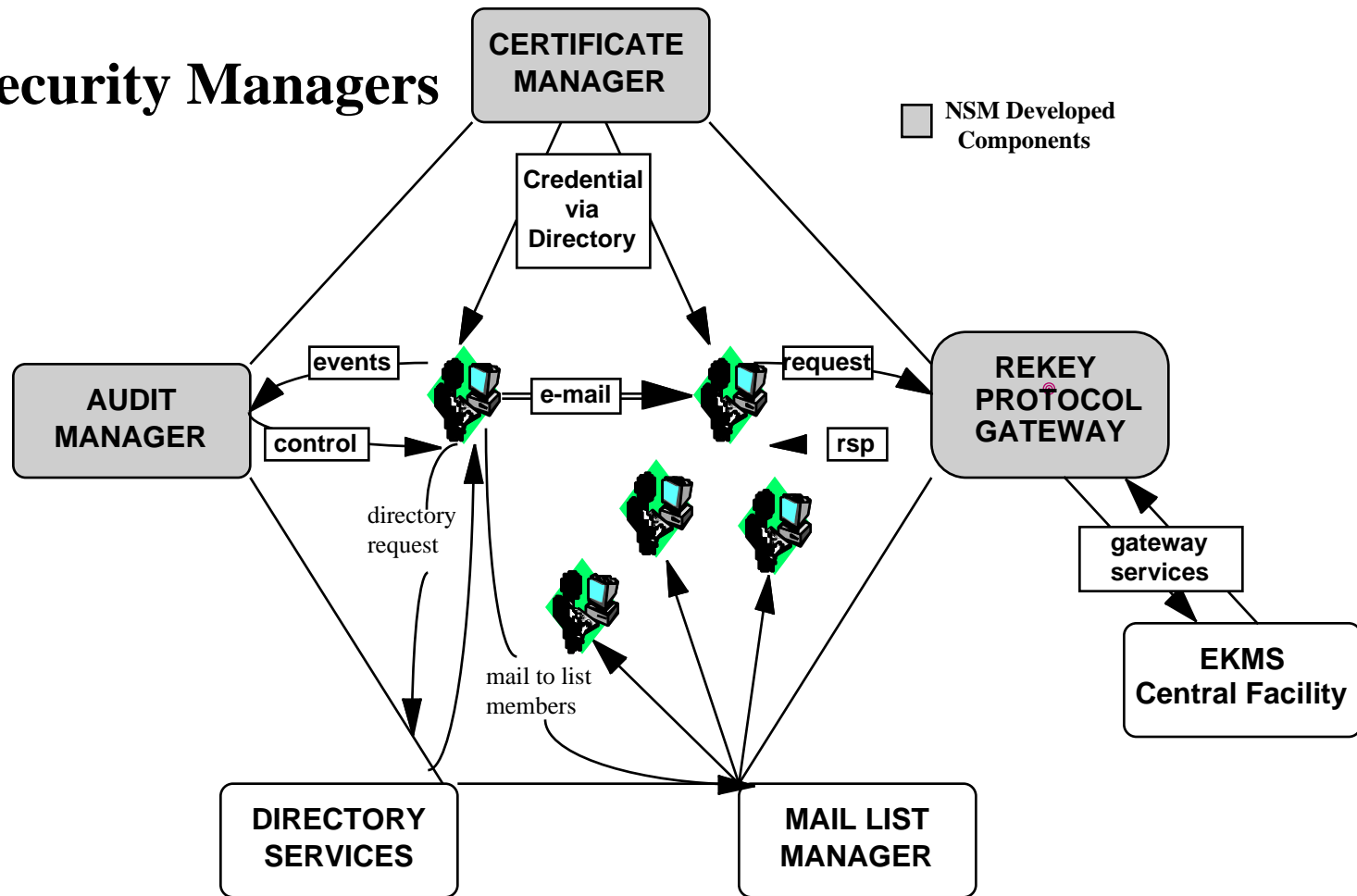
Integrated Security Solutions  
12/23/96



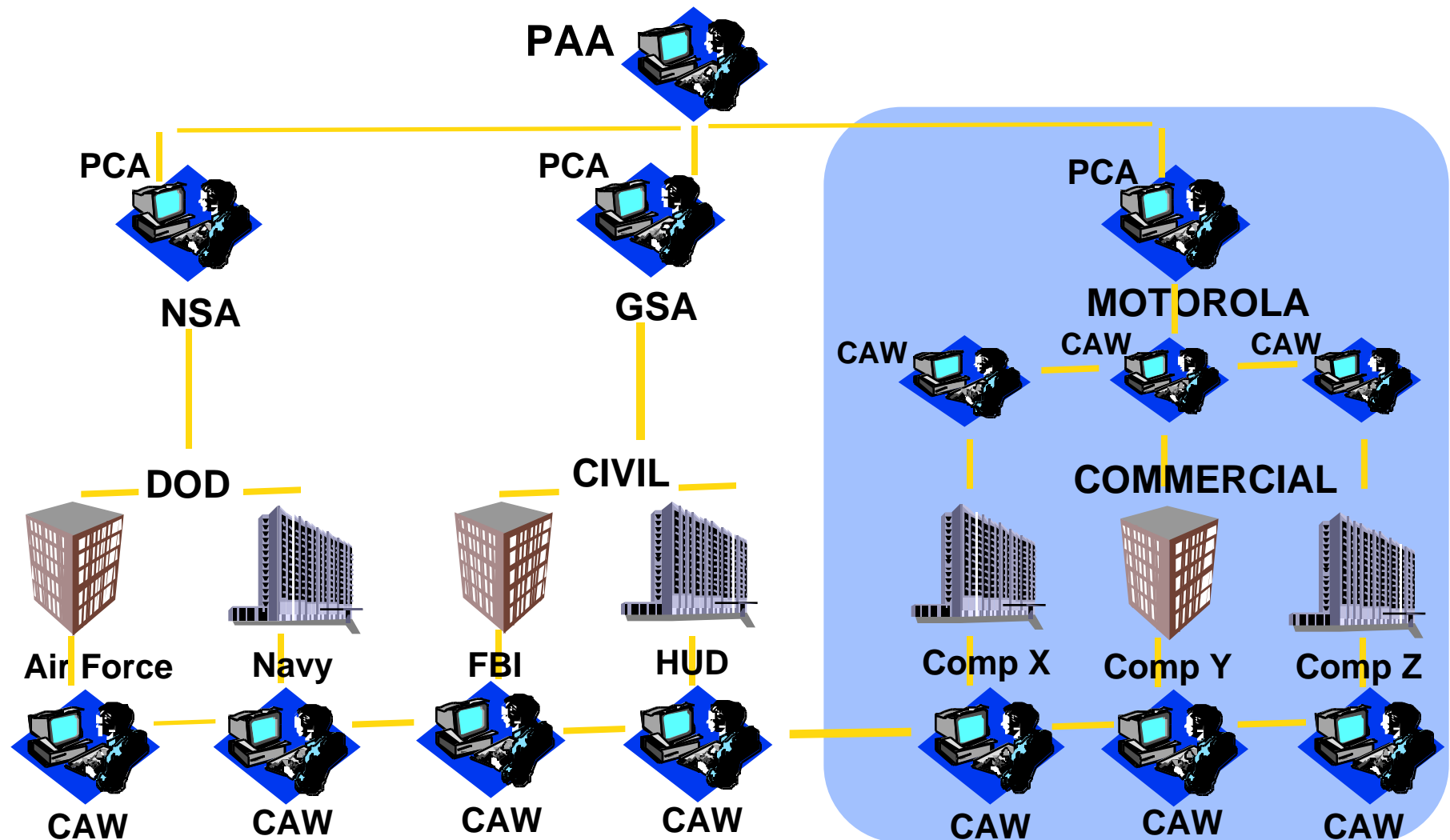
**MOTOROLA**

# *THE* US Government System

## Network Security Managers



# Commercial FORTEZZA™ Cards



Integrated Security Solutions  
12/23/96

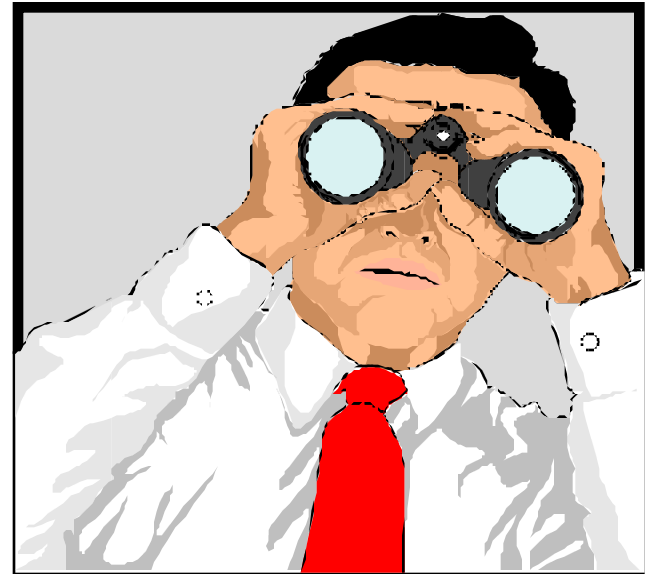


**MOTOROLA**

# Potential Security Threats

---

- **Eavesdropping, tampering, fraud**
- **Computer hackers, industrial spies, other unauthorized users**
- **Information theft, damage, destruction**
- **Wireless interception**
- **Carelessness, inadvertent mistakes**
- **Inadequate awareness of “need-to-know”**



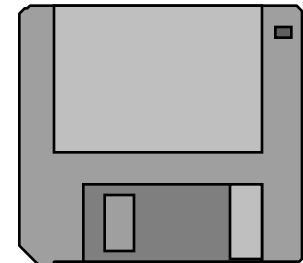
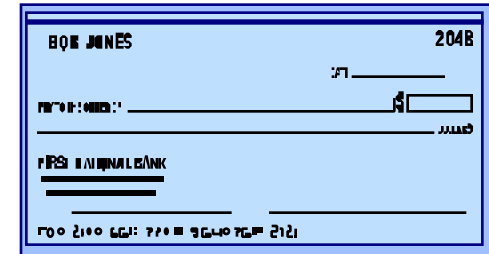
# Pushing Limits of Security Technology

- Dispersed work groups
- Portable computing
- Need flexible security systems
- Needs to be part of business process



# Security = Competitive Advantage

- Confidence in privacy of transactions
- Conduct more business electronically
- Increase productivity
- Increase profits
- Expand business
- Pursue unexplored electronic opportunities



Integrated Security Solutions  
12/23/96



**MOTOROLA**



# The *CipherNet*<sup>TM</sup> System

---

## **Digital Signature and Encryption System for Information Transfer**



# Capabilities of the *CipherNet*<sup>TM</sup> System

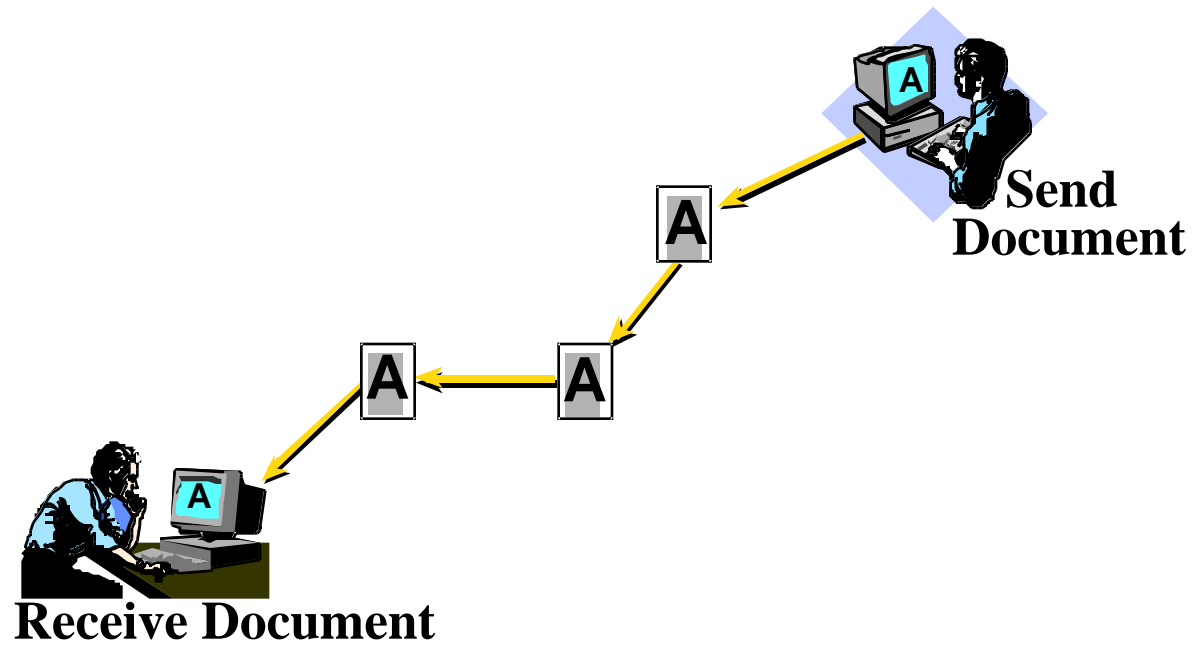
---

- Allows companies to **confidentially** exchange data and files within and between organizations using lower cost, nonsecure networks (e.g. Internet).
- Allows individuals to verify the **authenticity** and **accuracy** of information received from others.
- Provides a **scaleable management system** which will support the deployment across large organizations.

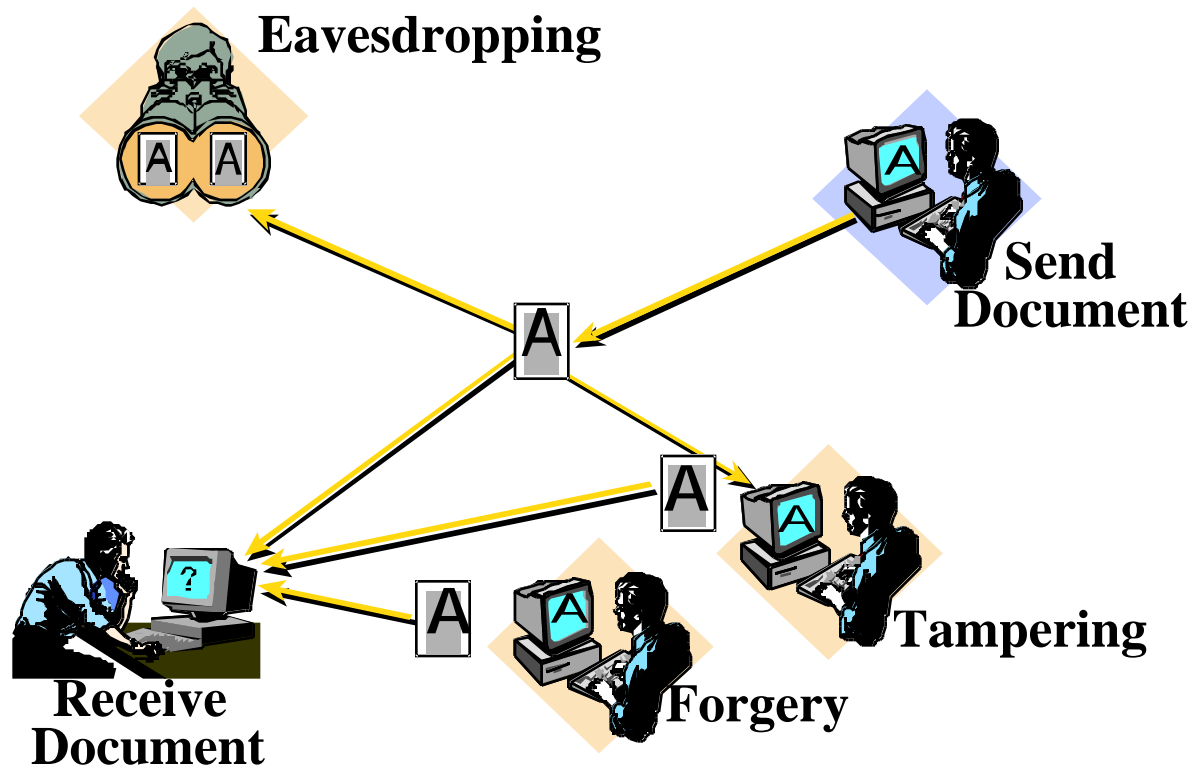


# What You Trust is Happening

---

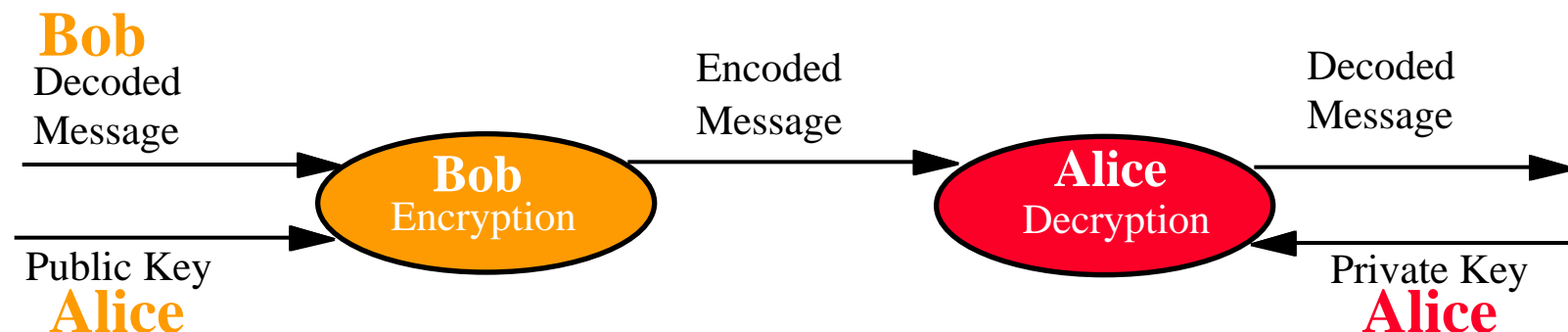


# What Can Be Happening



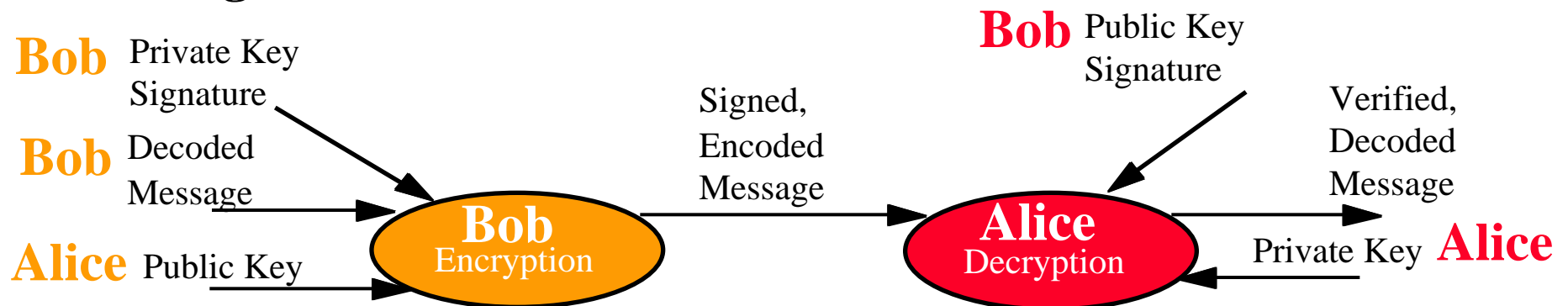
# Public and Private Keys

- Each authorized user is issued two encryption keys, called the public key and the private key, which are mathematically linked to each other.
- The public key is made available to everyone. Any authorized user can encrypt information prior to sending it to the owner of the public key.
- The private key is used only by its owner. As the recipient of an encrypted message, the private key owner uses it to decrypt incoming information.



# Digital Signatures

- The receiver of a message can authenticate that the sender is who they say they are.
- The private key is used only by it's owner. As the sender, the private key owner uses it to digitally sign information.
- The public key is made available to everyone and is used by the recipient of a signed file to verify the identity of the sender.
- Digital signatures may or may not be used with encrypted messages.



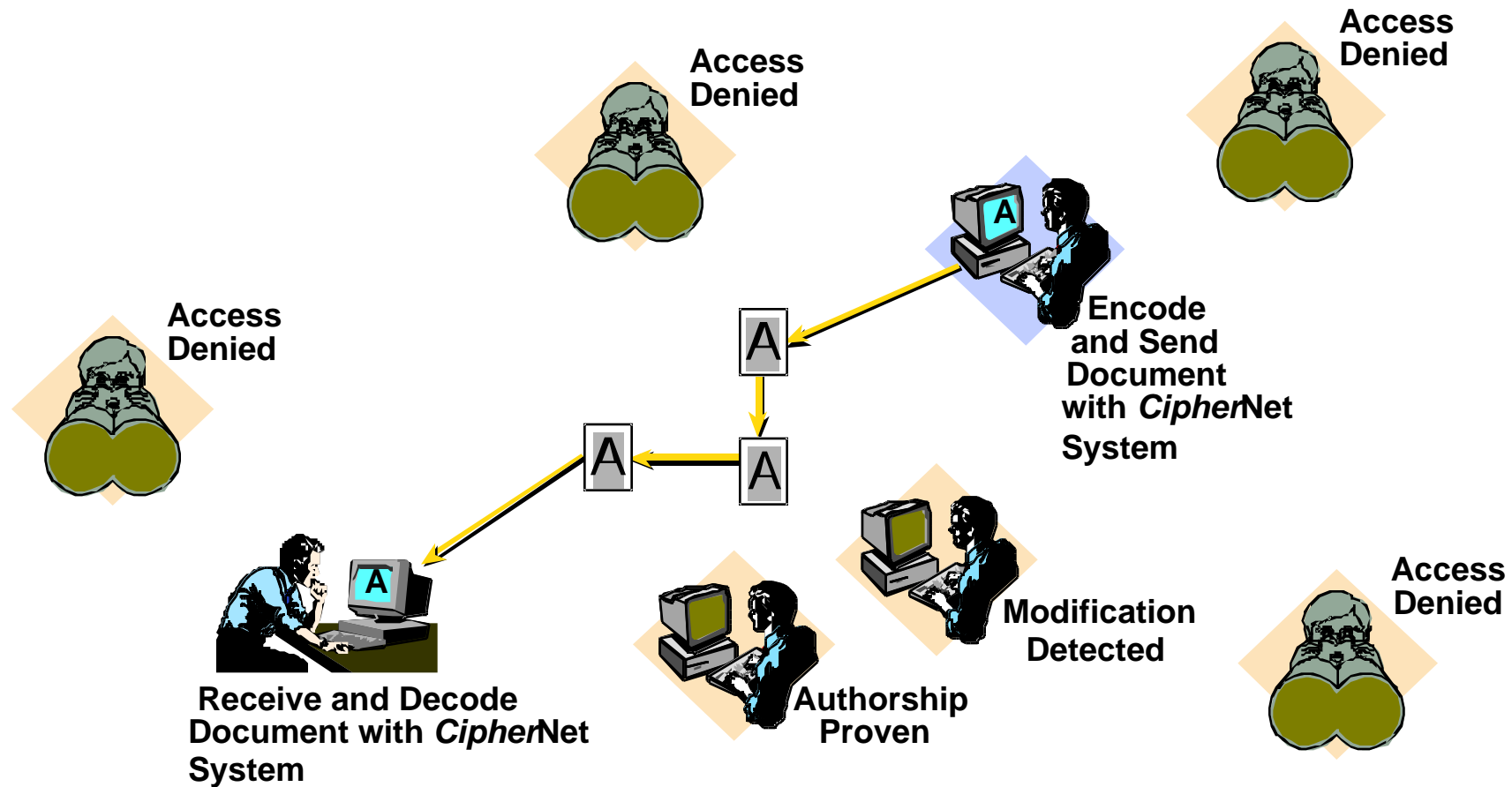
# Certificate Management

---

- **A trustworthy authority creates certificates which bind an individual to security privileges.**
  - ④ **Personal identification attributes**
  - ④ **Security privileges which include access rights or encryption rights**
  - ④ **Public key which is used for authentication and encryption**
- **Certificates are used to thwart attempts to substitute one key for another.**

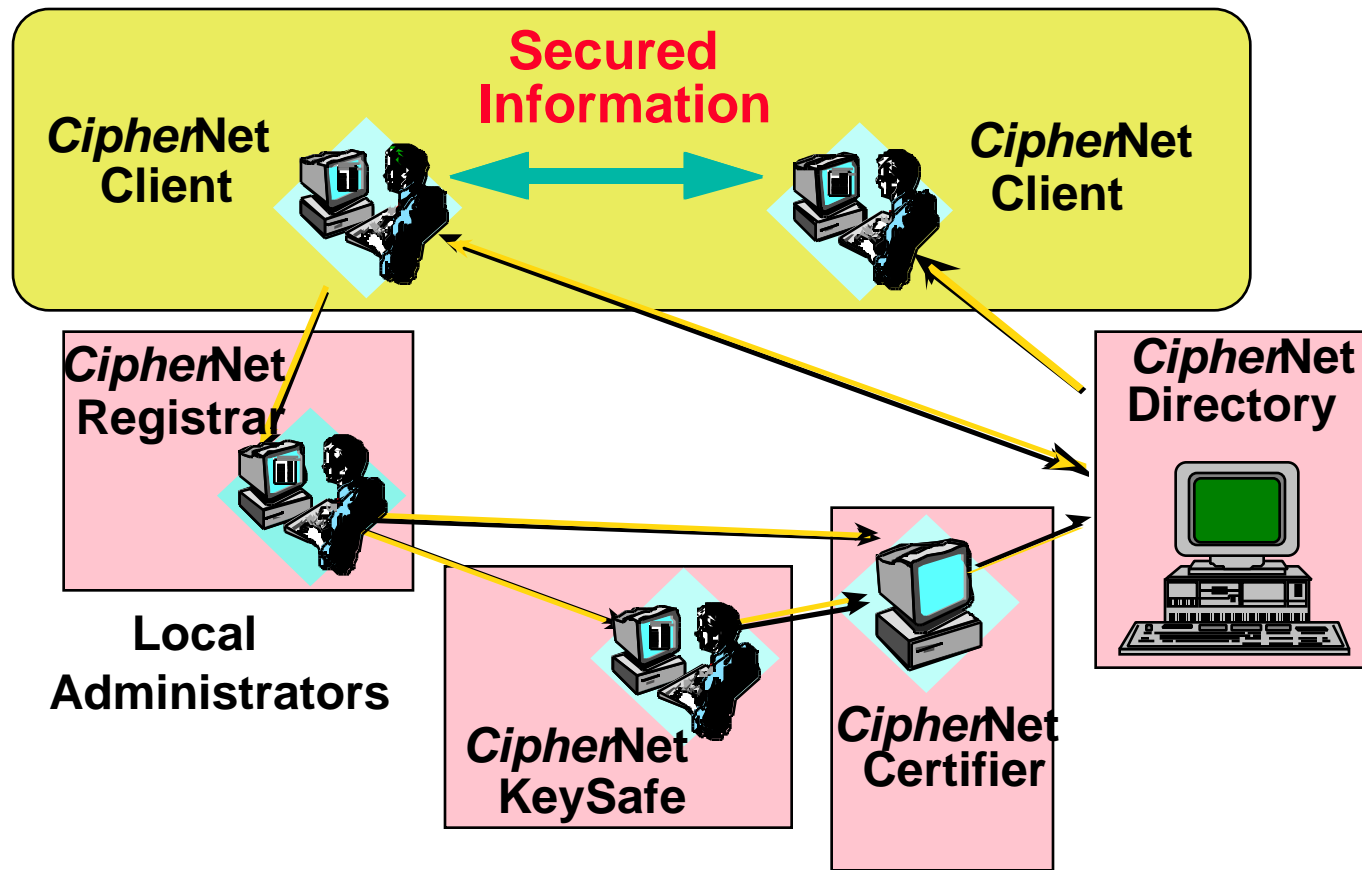


# The *CipherNet*<sup>TM</sup> System Protects





# The *CipherNet*<sup>TM</sup> System Environment



# *Cipher*Net Client

---

- **File encryption and digital signatures based on proven encryption technologies (RSA, MD2/MD5, and DES)**
- **E-mail enabled software can transmit secured information**
- **Integrated with many e-mail agents**
- **Simple point-and-click interface**
- **Drag-and-drop file security**
- **Built-in text editor for sending brief, secured messages**
- **Available for Windows<sup>™</sup>, Macintosh<sup>®</sup>, and UNIX<sup>®</sup> platforms**



# *CipherNet*<sup>TM</sup> Client Configuration

---

## ■ *CipherNet* Client for Windows

- ④ IBM-compatible 386 or later
- ④ Microsoft Windows 3.1 or later
- ④ 5 MB RAM minimum, 8 MB recommended
- ④ 5 MB hard disk minimum, 8 MB recommended
- ④ 3.5" (1.44 MB) disk drive
- ④ MS-DOS 3.3 or later

## ■ *CipherNet* Client for Macintosh

- ④ Macintosh System 7 OS or later
- ④ 2 MB RAM minimum, 4 MB recommended
- ④ 2 MB hard disk minimum, 3 MB recommended



# *CipherNet*<sup>TM</sup> Certificate Management

---

- Provides local administration for a person's enrollment and registration.
- Supports scaling solutions for large and small companies.
- System places a user's private key in a secure escrow.
- Supports automated processing of requests from *CipherNet* Registrar systems.
- Serves as a central certification authority.
- Allows users to look up and retrieve the public keys of others.
- Enables global distributed access to public keys.
- Supports key lengths from 512 to 1024 bits.
- Uses X.509 certificate standard.



# *CipherNet*<sup>TM</sup> Certifier Configuration

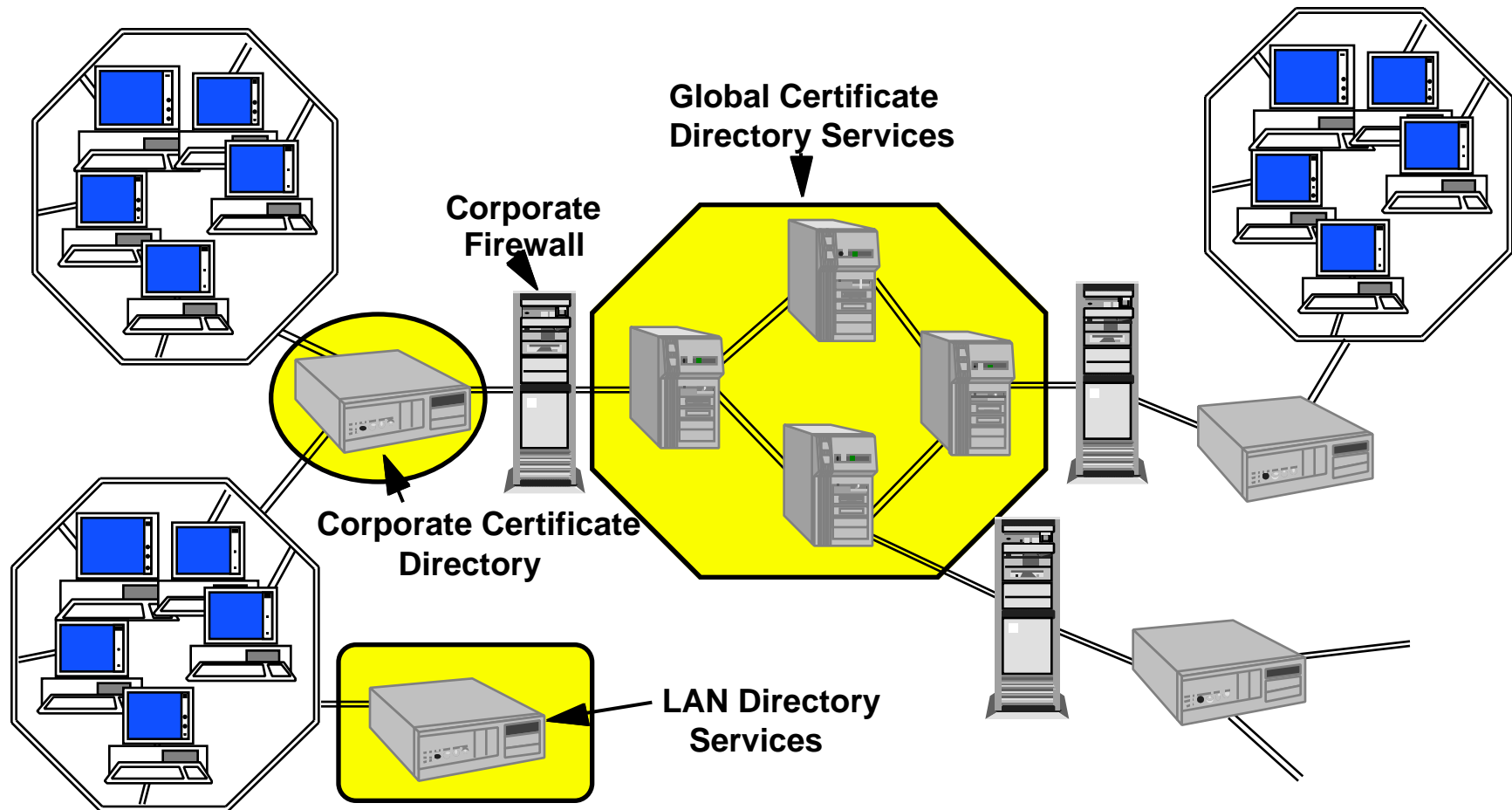
---

## ■ *CipherNet* Certifier

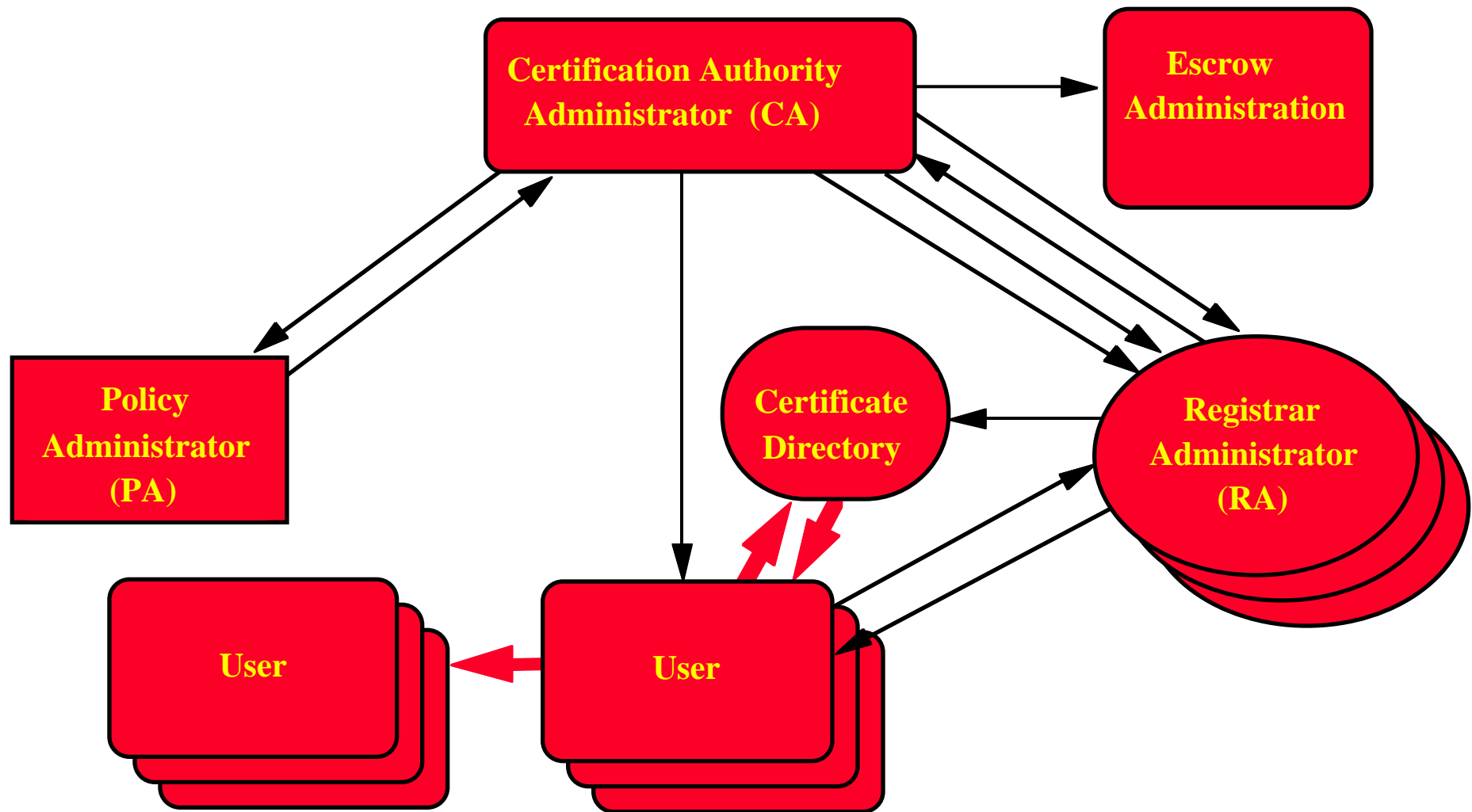
- ④ IBM-compatible 486 or later
- ④ Microsoft Windows NT 3.51 or later
- ④ 12 MB RAM minimum, 16 MB recommended
- ④ 5 MB hard disk minimum, 8 MB recommended
- ④ 3.5" (1.44 MB) disk drive



# Directory Service Options



# Certificate Management



# CipherNet Deployment

