

**Security Technology and Architecture**  
**Implications of HIPAA**  
**October 12,1999**

**Morton D. Hoffman**

**Senior Technologist**

**[mort.hoffman@cybertrust.gte.com](mailto:mort.hoffman@cybertrust.gte.com)**

# The Challenge

---

- **Comply with HIPAA security standards and regulations**
- **Provide cost effective and user friendly systems for managing patient records**

# HIPPA

---

- Health Insurance Portability and Accountability Act of 1996, *Kennedy-Kassebaum law*
- Section 45 CFR Part 142 introduced August, 1998
  - Requirements for securing electronic health information
  - Rule focuses on Security and Electronic Signature Standards
  - Specifically (from Background)
    - Confidentiality and privacy
    - Identify signatory
    - Non-repudiation

# Application of Standards

---

- Applicable to:
  - Health plan
  - Health care clearinghouse
  - Health care provider
- Covering
  - Information in electronic form
  - Electronic transactions using all media
  - Data that identifies individuals
- *Except* voice and fax

# HIPPA Users

---

- Department of Health and Human Services
- Health Care Financing Administration
- State Medicaid Agencies
- Health Plans / Health Insurers
- Healthcare Providers
- Hospitals, Clinics, Physician Practices
- Healthcare Clearinghouses
- Healthcare Web Site Designers and Hosts

# HIPPA Transactions

---

- Health claims and encounter forms
- Health claim attachments
- Enrollment/dis-enrollment in a health plan
- Eligibility for a health plan
- Health care payment and remittance advice
- Health plan premium payments
- First report of injury
- Health claim status
- Referral certification and authorization

# Policies, Practices, and Procedures

---

- Policies and procedures
  - Security and confidentiality policies
  - Information security officers
  - Education and training programs
  - Sanctions
- Technical Practices
  - Authentication
  - Access control
  - Audit trails
  - Physical security and disaster recovery
  - ...
  - System assessment

# Public Key Cryptography (PKI)

---

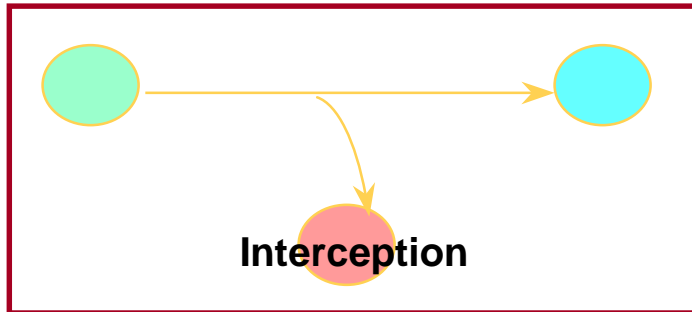
- **PKI meets HIPAA requirements**
- **PKI provides the only mature electronic signature capability**
  - **Electronic vs. Digital Signature**
- **PKI is dominant security technology for Internet-oriented networking**

# Core Security Services

## (excerpt from HIPAA)

---

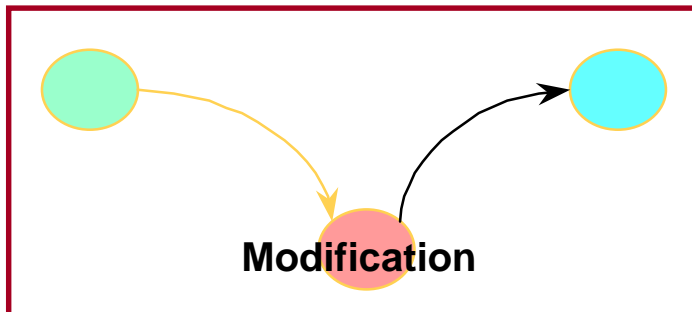
### Confidentiality



Is my communication private?

“The property that information is not made available or disclosed to unauthorized individuals, entities or processes.” p. 43272

### Integrity



Has my communication been altered?

“Ensuring, typically with a message authentication code, that a message received matches the message sent”  
p. 43274

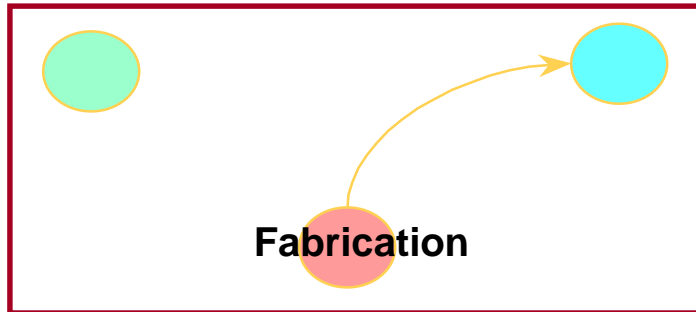
Source: Federal Register / Vol. 63, No. 155

# Core Security Services

## (excerpt from HIPAA)

---

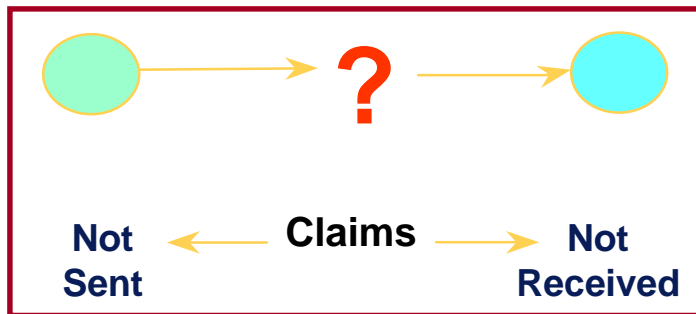
### Authentication



Who am I dealing with?

“The corroboration that an entity is the one claimed” p. 43273

### Non-repudiation



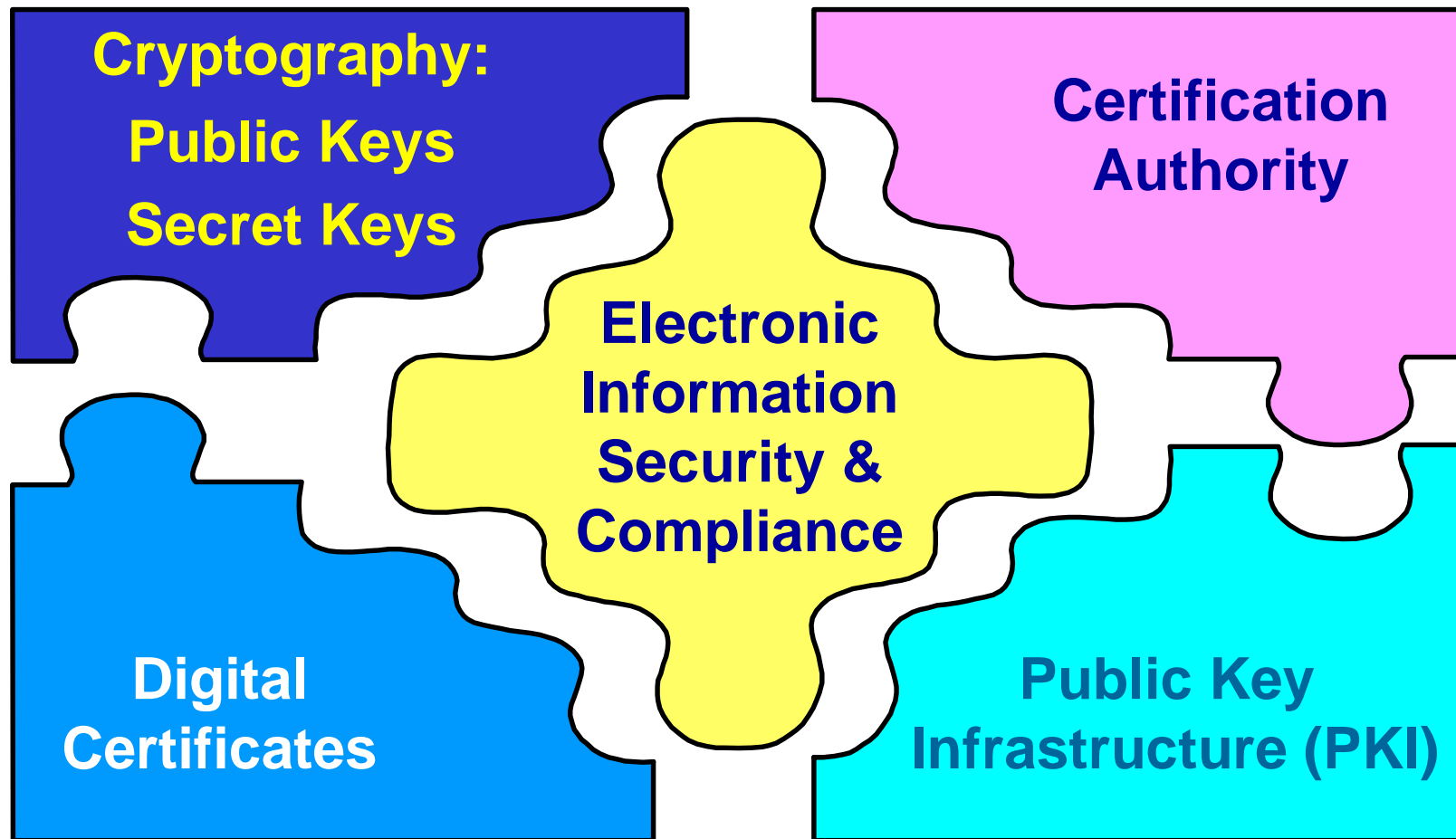
Who sent/received it and when?

“Strong and substantial evidence of the identity of the signer of a message and of message integrity, sufficient to prevent a party from successfully denying the origin, submission or delivery of the message and the integrity of its contents ” p. 43274

Source: Federal Register / Vol. 63, No. 155

# The Elements of the Solution

---



# Cryptography

---

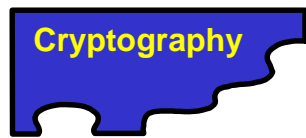
- **Secret Key (Symmetric)**

- Data are encrypted & decrypted using the same key
- Does not scale well
- Ex: DES

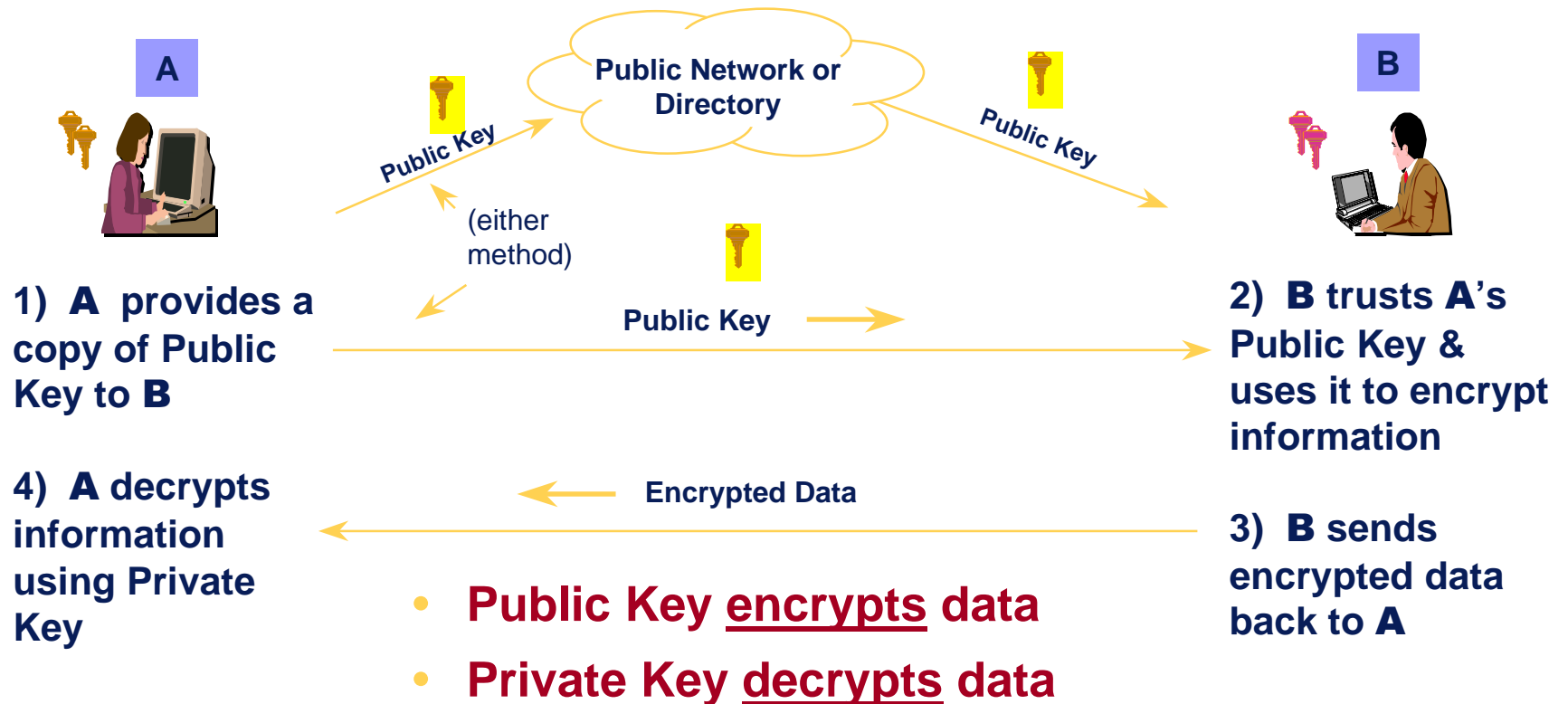
- **Public key (Asymmetric)**

- Data are encrypted with one key & decrypted with the other key of the pair
- Keep your private key secret
- Ex: RSA

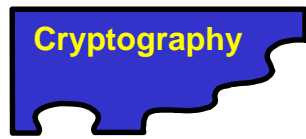
# Public Key Cryptography



Everyone has a Key Pair: Public Key & Private Key

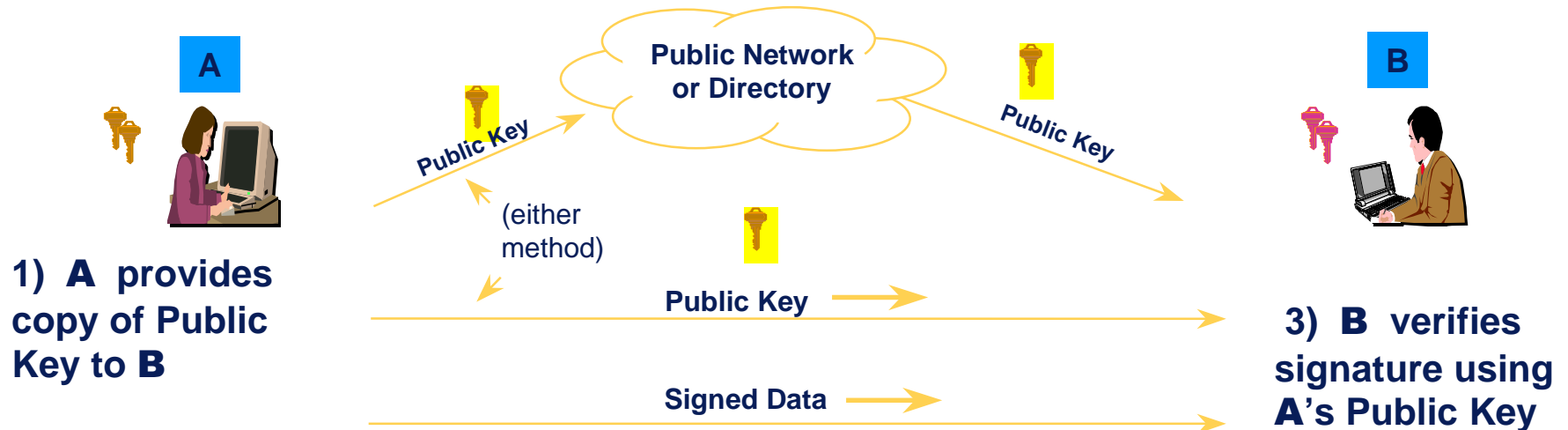


# Digital Signature



Everyone has a *Signature Key Pair*

- May be different from the *Encryption Key Pair*



1) **A** provides copy of Public Key to **B**

2) **A** signs information using Private Key

3) **B** verifies signature using **A's** Public Key

- **Private Key signs (encrypts) data**
- **Public Key verifies (decrypts) signature on data**

# Digital Certificate

*An electronic passport that proves your identity and authenticates you*

- Who you are
- What your public key is
- Who issued your certificate



## **Physical World Analogies**

ATM Card - a Certificate to conduct electronic banking

Driver's license - a Certificate to operate a vehicle

Employee badge - a Certificate to gain facility access

U.S. Passport - a Certificate telling who you are

# Certification Authority

---

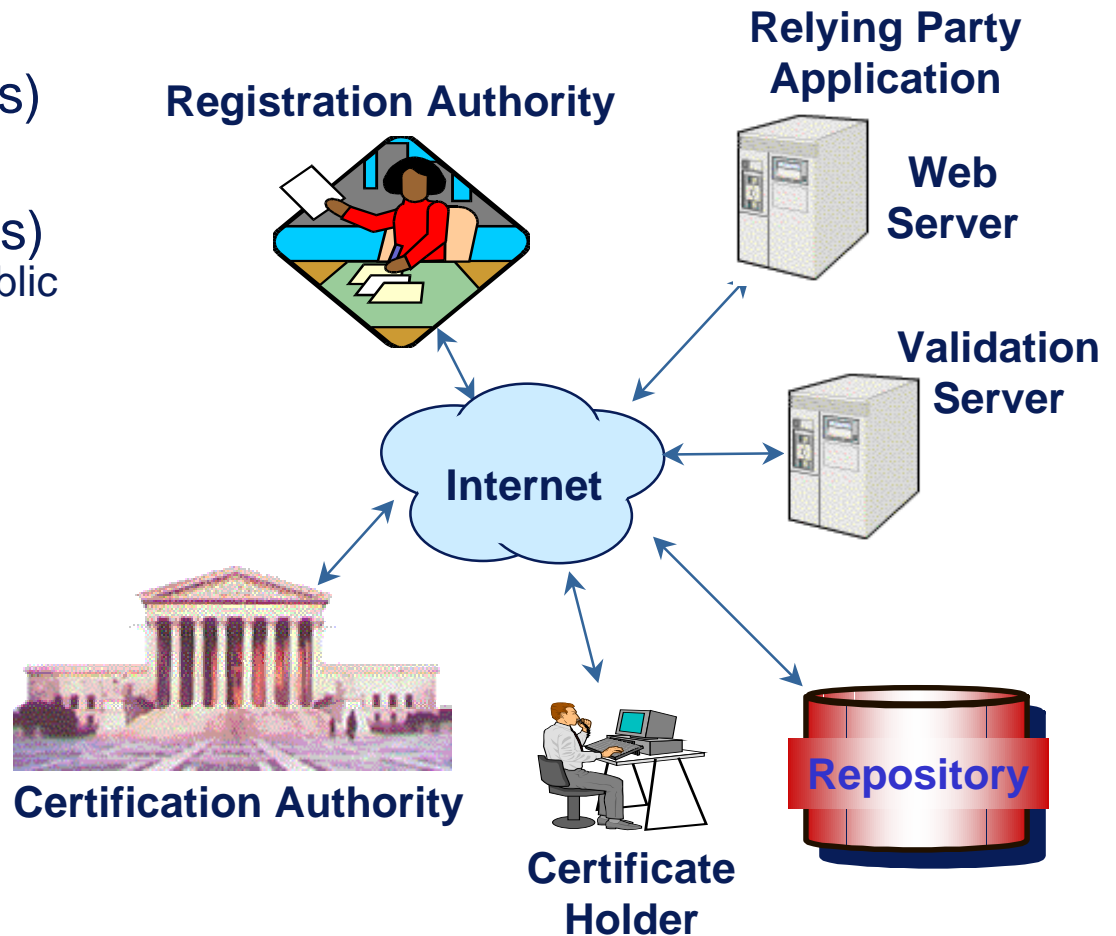


- A CA verifies and vouches for the identity information in a Certificate
  - like a Government for passports
  - like a bank for ATM cards
- CA verification techniques:
  - Check existing records - employee databases
  - Examine typical identification - passport, license
  - Background check - government database, personal interview, references, etc.

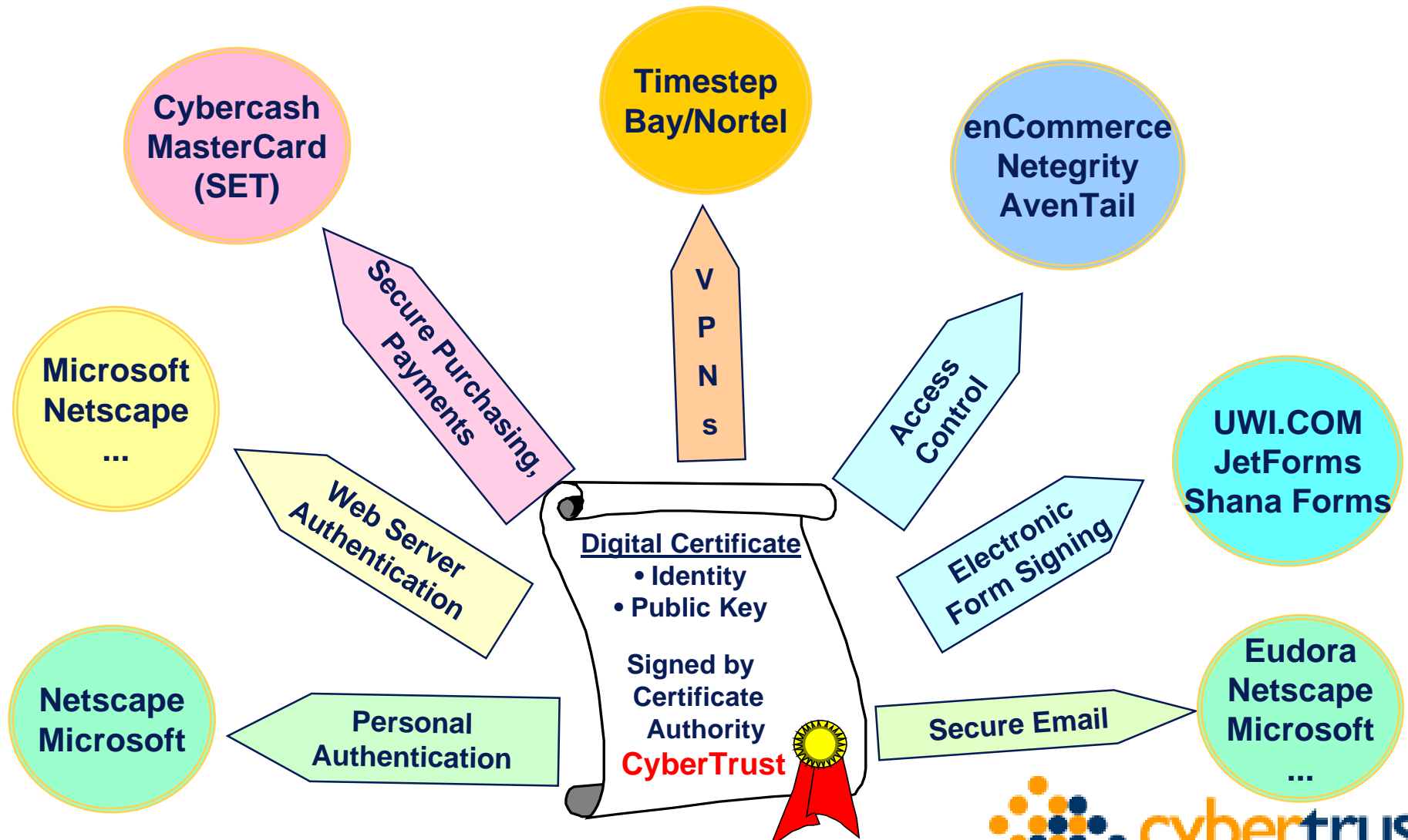
# Components of a PKI



- Certification Authorities (CAs)  
(Issuers)
- Registration Authorities (RAs)  
(Authorize the binding between Public Key & Certificate Holder)
- Certificate Holders  
(Subjects)
- Relying Parties  
(Validate signatures & certificate paths)
- Repository  
(Store & distribute certificates)
- Validation Server  
(Provide certificate status: expired, revoked, etc.)



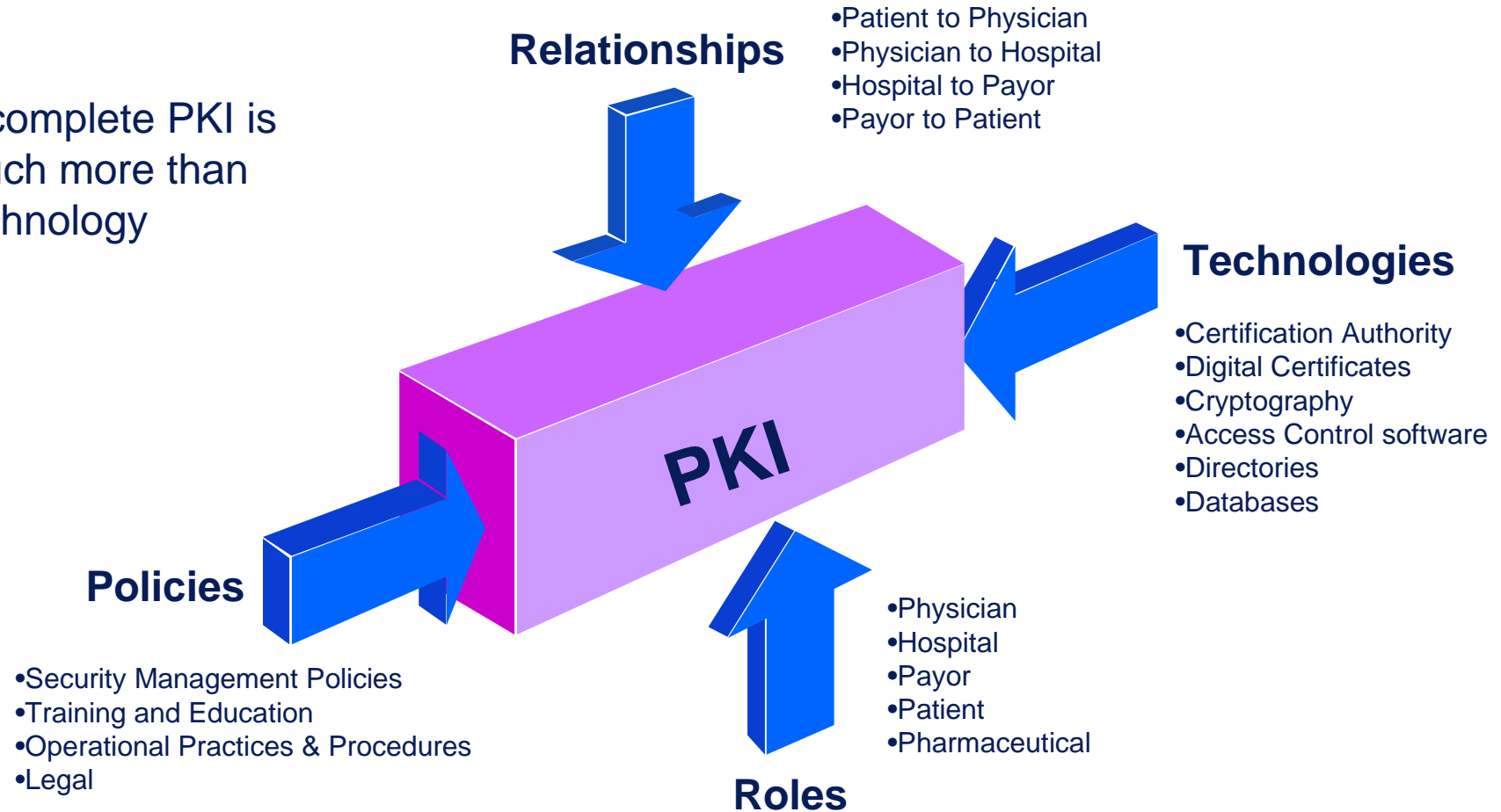
# Ways to Use PKI and Digital Certificates



# Public Key Infrastructure



A complete PKI is much more than technology



# Questions & Discussion

---

Phone: 1 800 362 7304

[HTTP://WWW.CYBERTRUST.COM](http://www.cybertrust.com)

