

An Introduction to Public Key Infrastructure (PKI)

Judith A. Furlong

Product Architect

Annual Computer Security Applications
Conference

December 9, 1999

Conventional vs. Public Key Cryptography



**Conventional
(Symmetric)**

One Key

**Used for both
Encryption and Decryption**

Must be protected, kept private



**Public Key
(Asymmetric)**

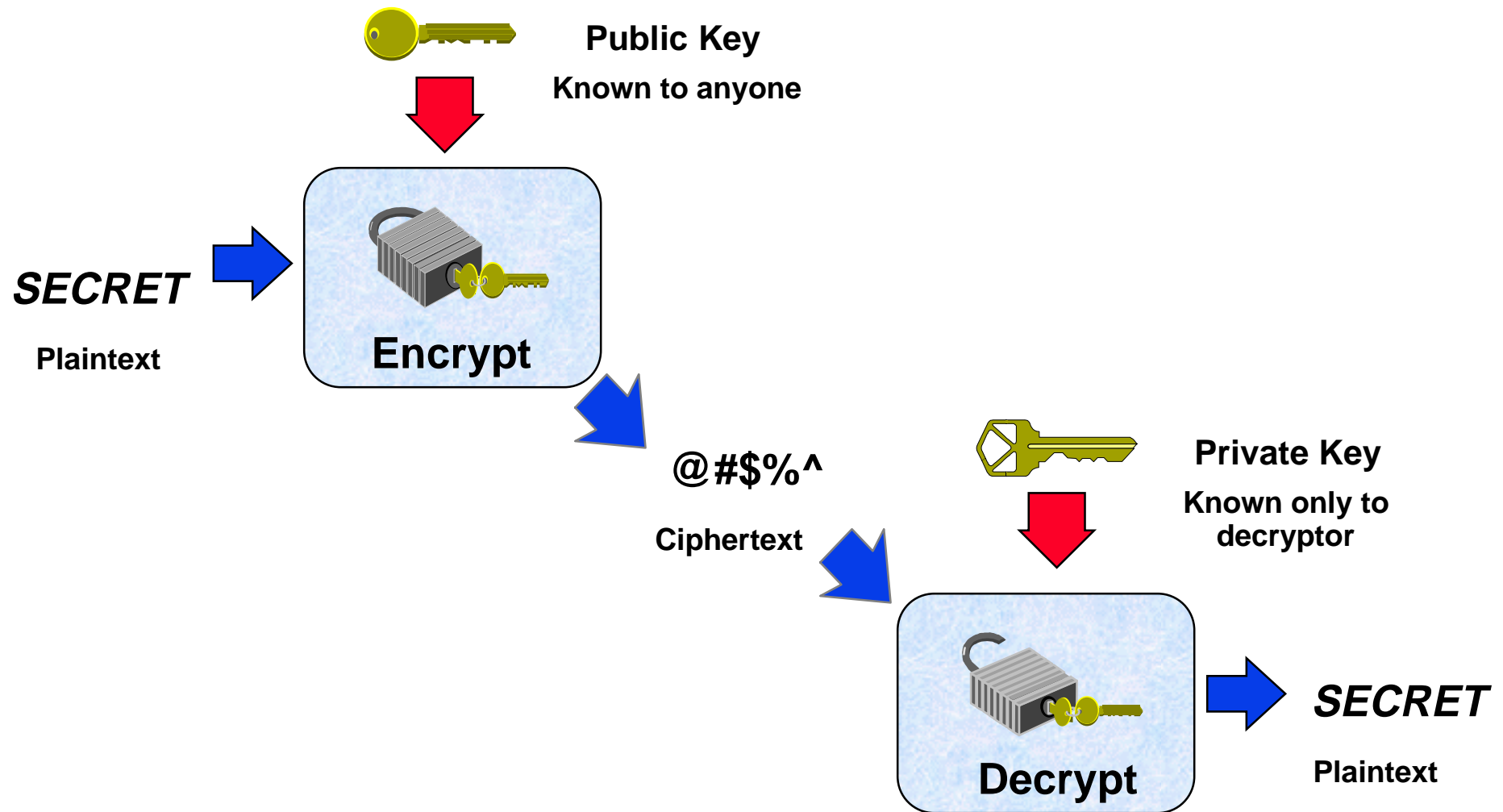
Two Keys

Mathematically related

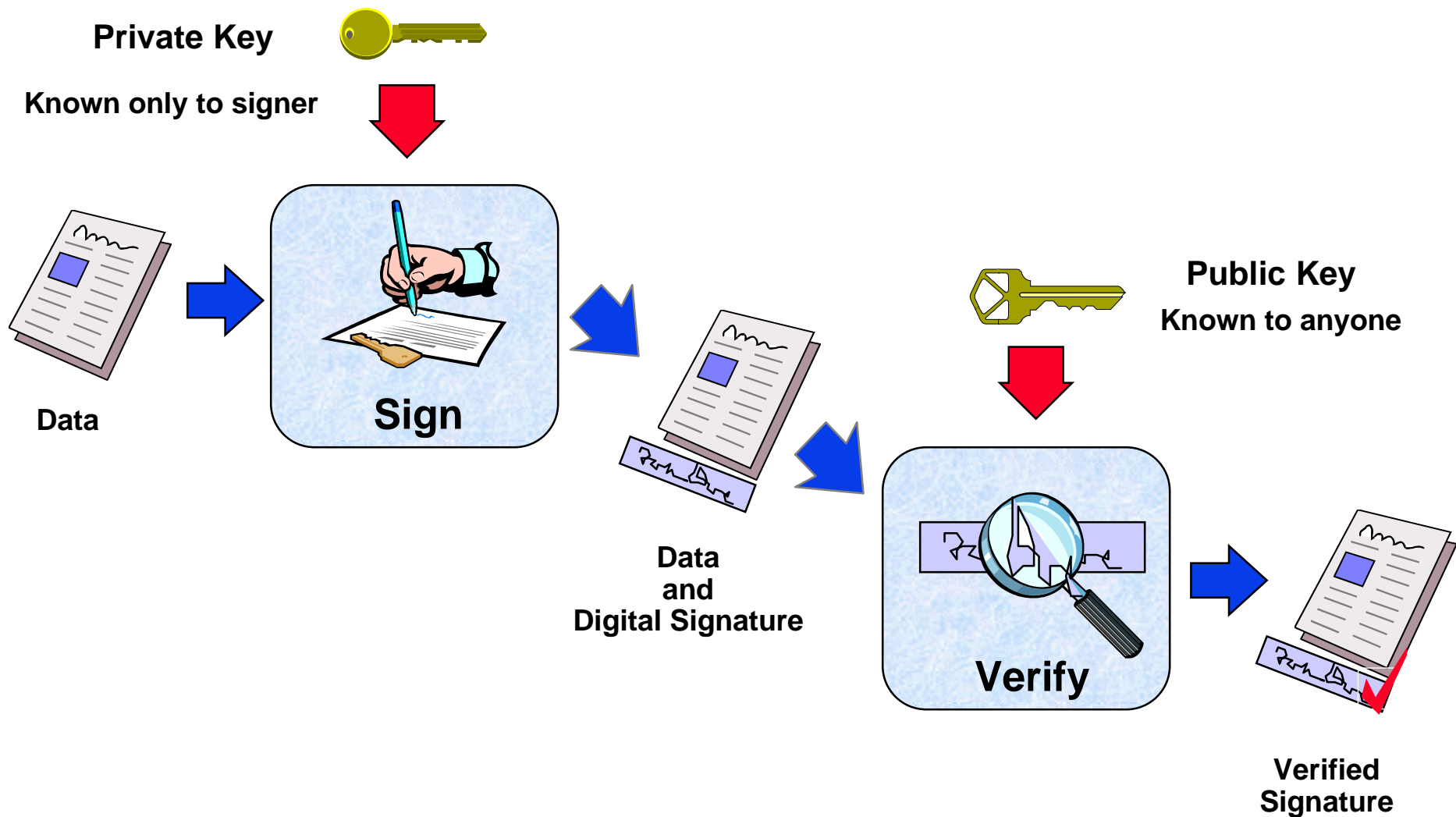
**One key used for encryption,
may be made public**

**One key used for decryption,
must be protected, kept private**

Public Key Cryptography: Encryption



Public Key Cryptography: Digital Signature

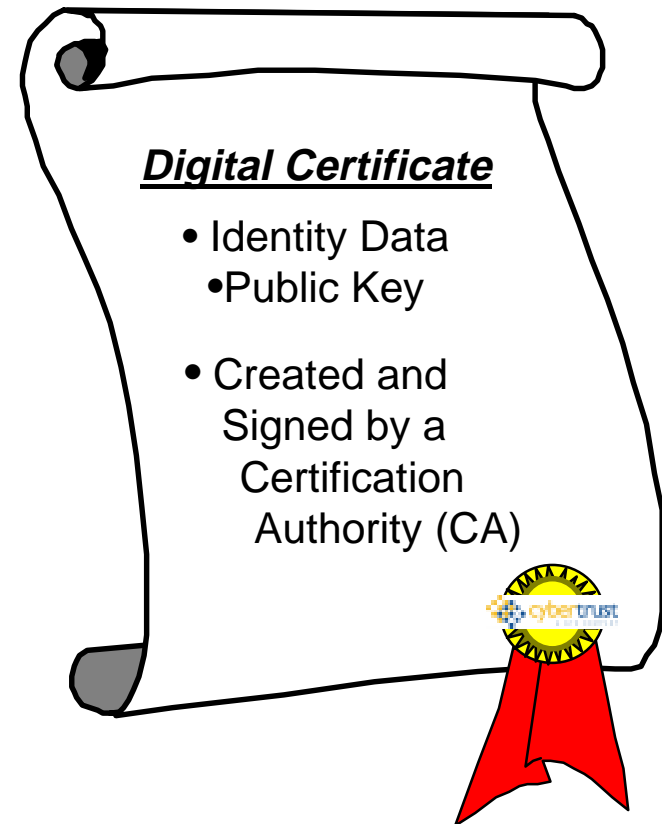


Digital Certificate

- A digitally signed binding between your identity and your public key
- Used as an electronic passport to prove your identity and authenticate you in the electronic world

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



Certification Authority (CA)



- A trusted entity which issues, manages and distributes digital certificates
- CAs are responsible for authenticating the identity of an entity prior to binding a public key to that identity



Physical World

- ATM Card

- Driver's license

- Employee badge

Issued by

Banks

States

Employer

Electronic World

A Certificate for Internet banking

A Certificate for online registration

A Certificate to gain facility and computer resource access

What is a Public Key Infrastructure (PKI)?



- A PKI is the set of components, people, policies and procedures which provide the foundation for the management of keys and certificates used by public key-based security services
- A PKI assures the trustworthiness of public key-based security mechanisms
 - Confidentiality of the private key
 - Integrity of the public key
- PKI functions can include
 - Key Generation and Distribution
 - Certificate Issuance and Distribution
 - Certificate Validation
 - Key Expiry and Revocation
 - Key Update
 - Key Escrow and Recovery

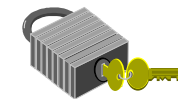
What Does PKI Enable?

- Strong authentication
- Authenticity and integrity of data
- Nonrepudiation of transactions



Digital
Signature

- Confidentiality of data in transit or storage



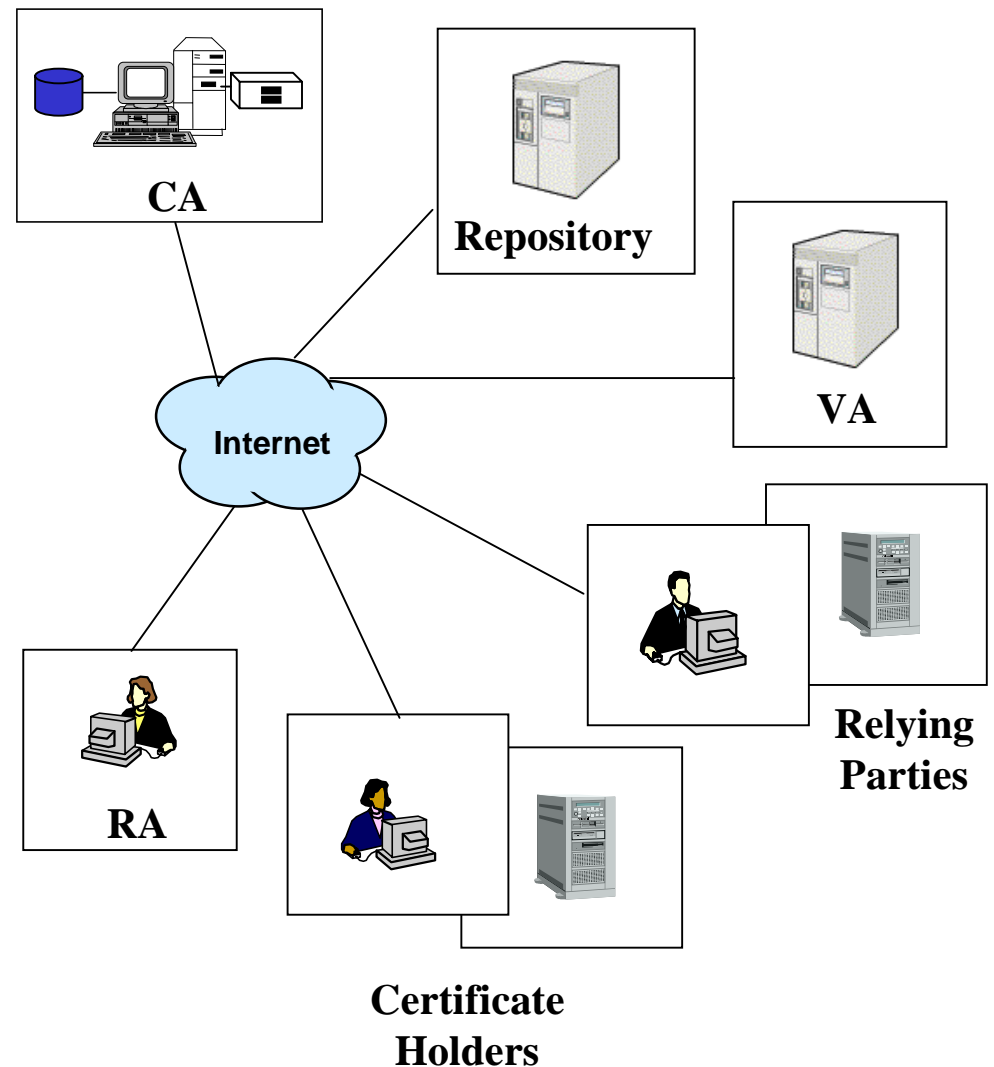
Encryption



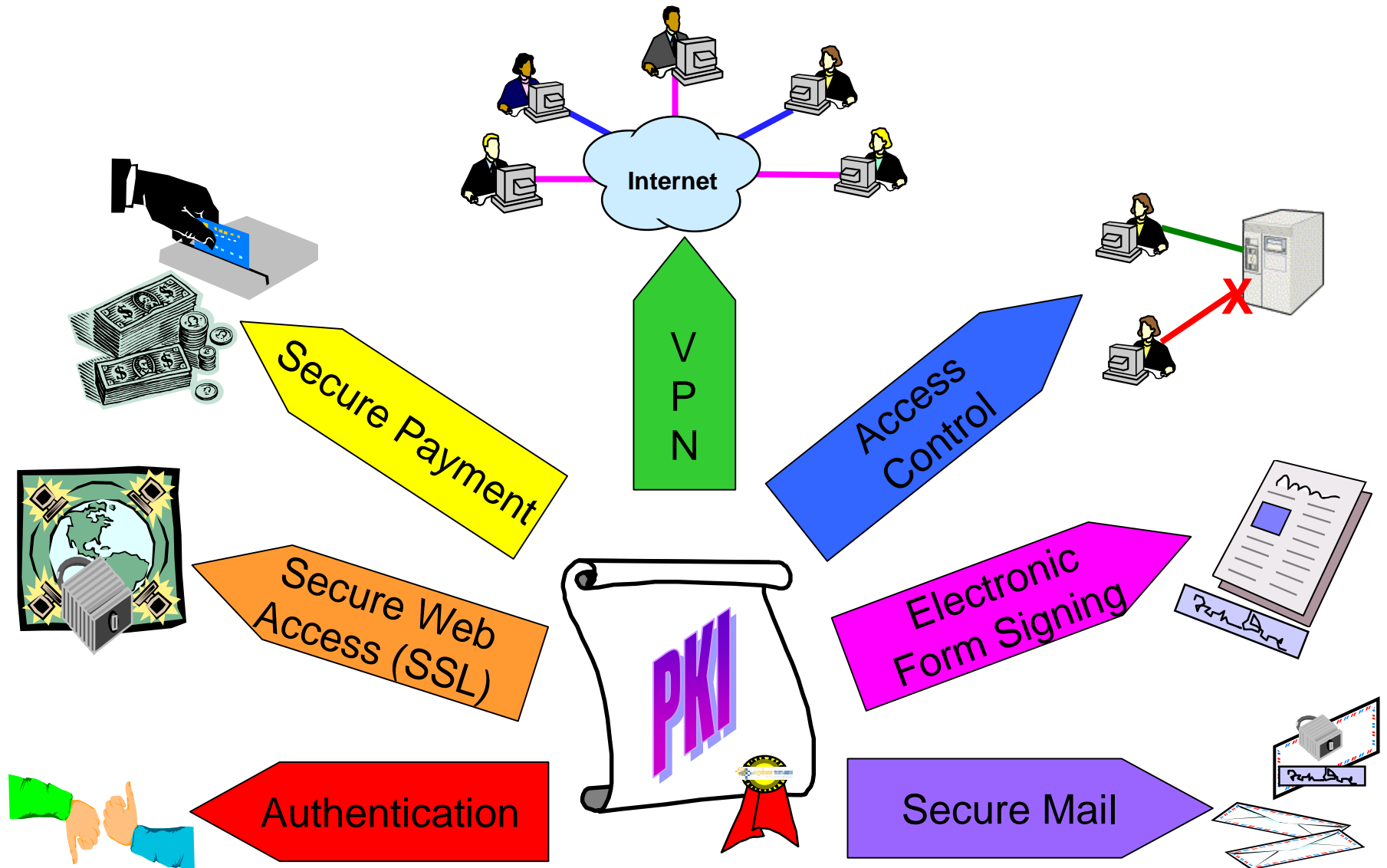
- Ability to process more sensitive data in shared networks
- Automation of sensitive functions previously kept off-line
- Enhanced security services
- Improved security interoperability

Components of a PKI

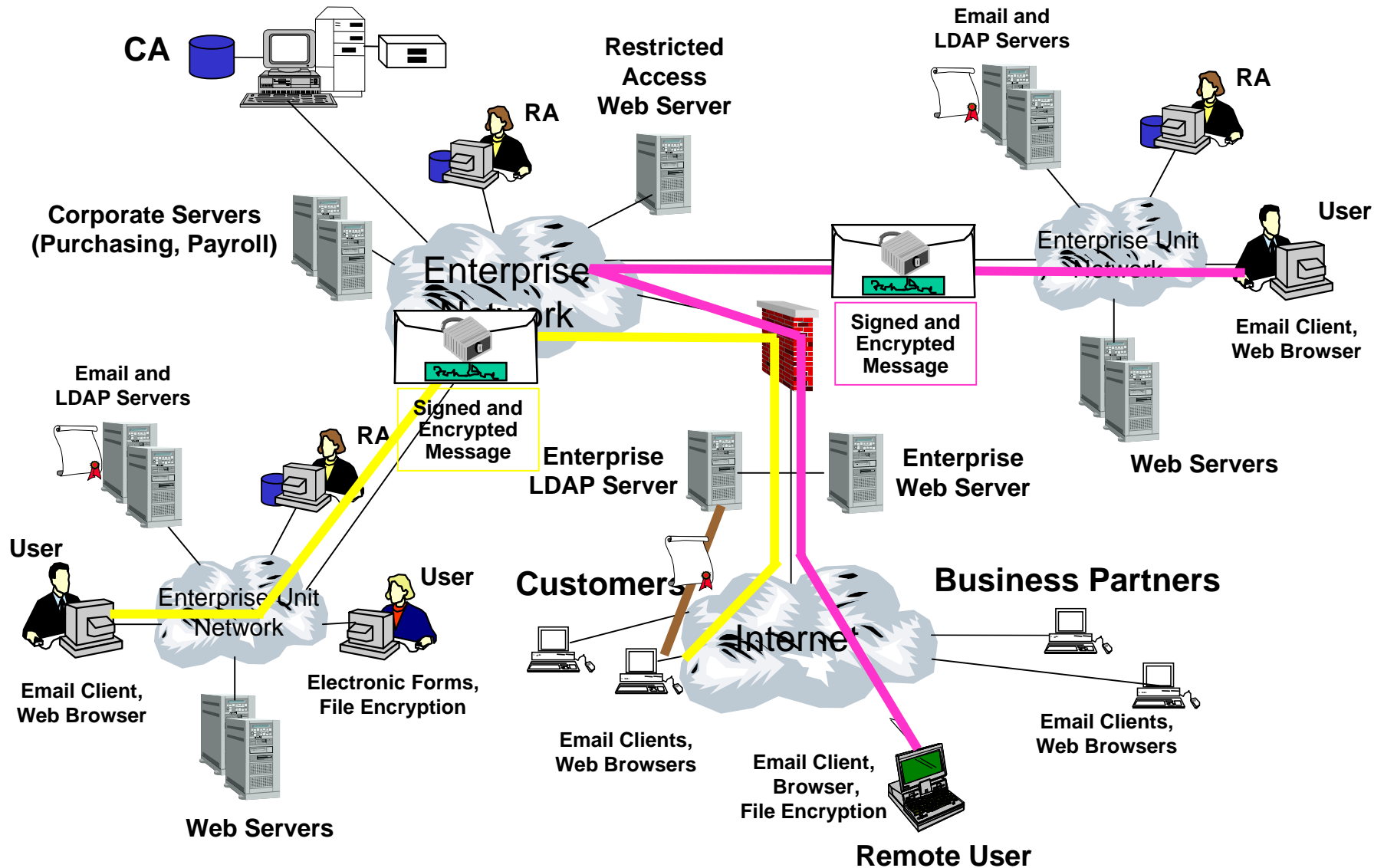
- **Certification Authorities (CA)**
(Issues and manages certificates)
- **Registration Authorities (RAs)**
(Performs Certificate Holder authentication on behalf of CA)
- **Repository**
(Stores and Distributes Certificates, CRLs)
- **Validation Authority (VA)**
(Provides Certificate Status)
- **Certificate Holders**
(Certificate subjects)
- **Relying Parties**
(Verifies signatures and certificate paths)



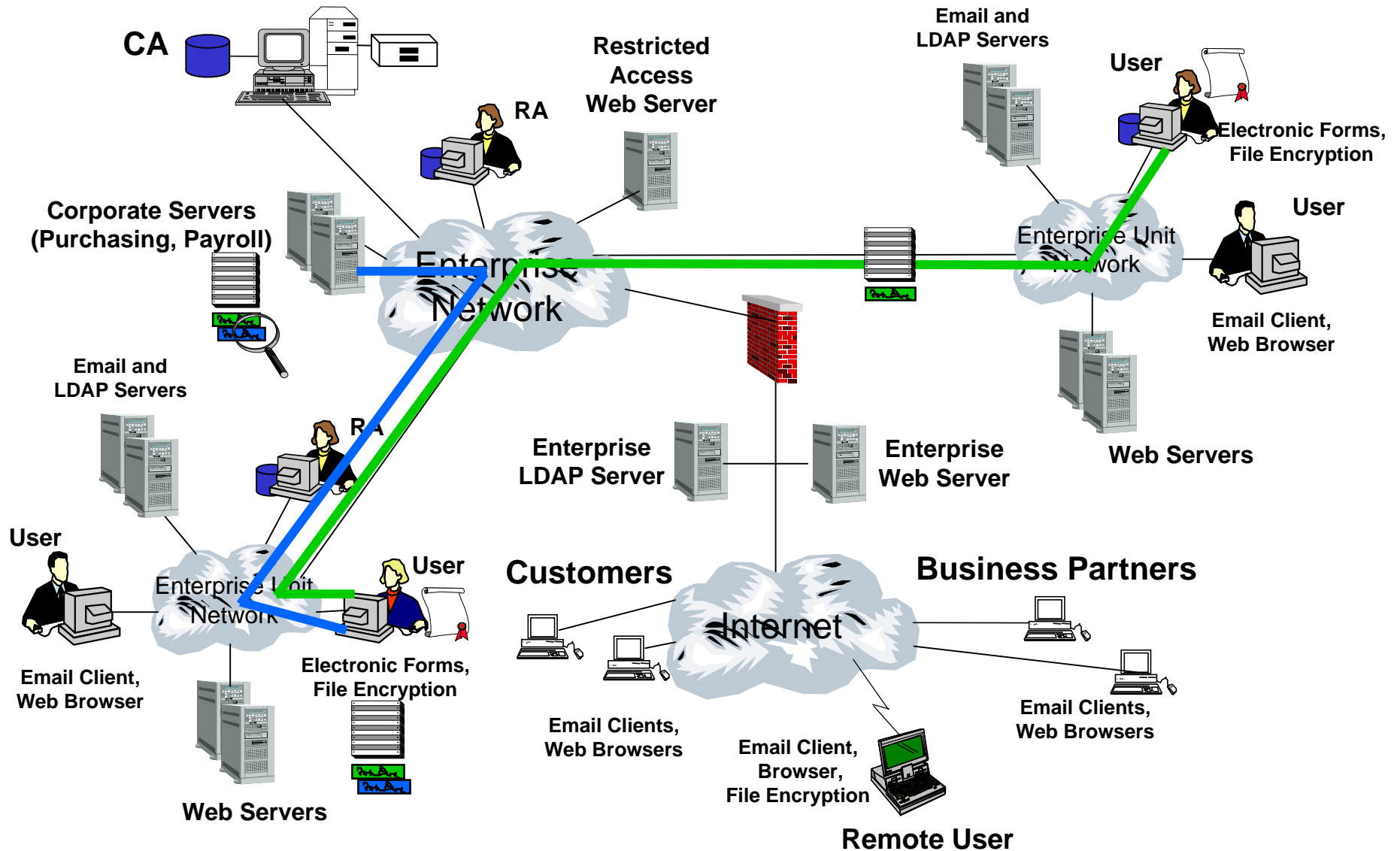
Where is PKI Used Today?



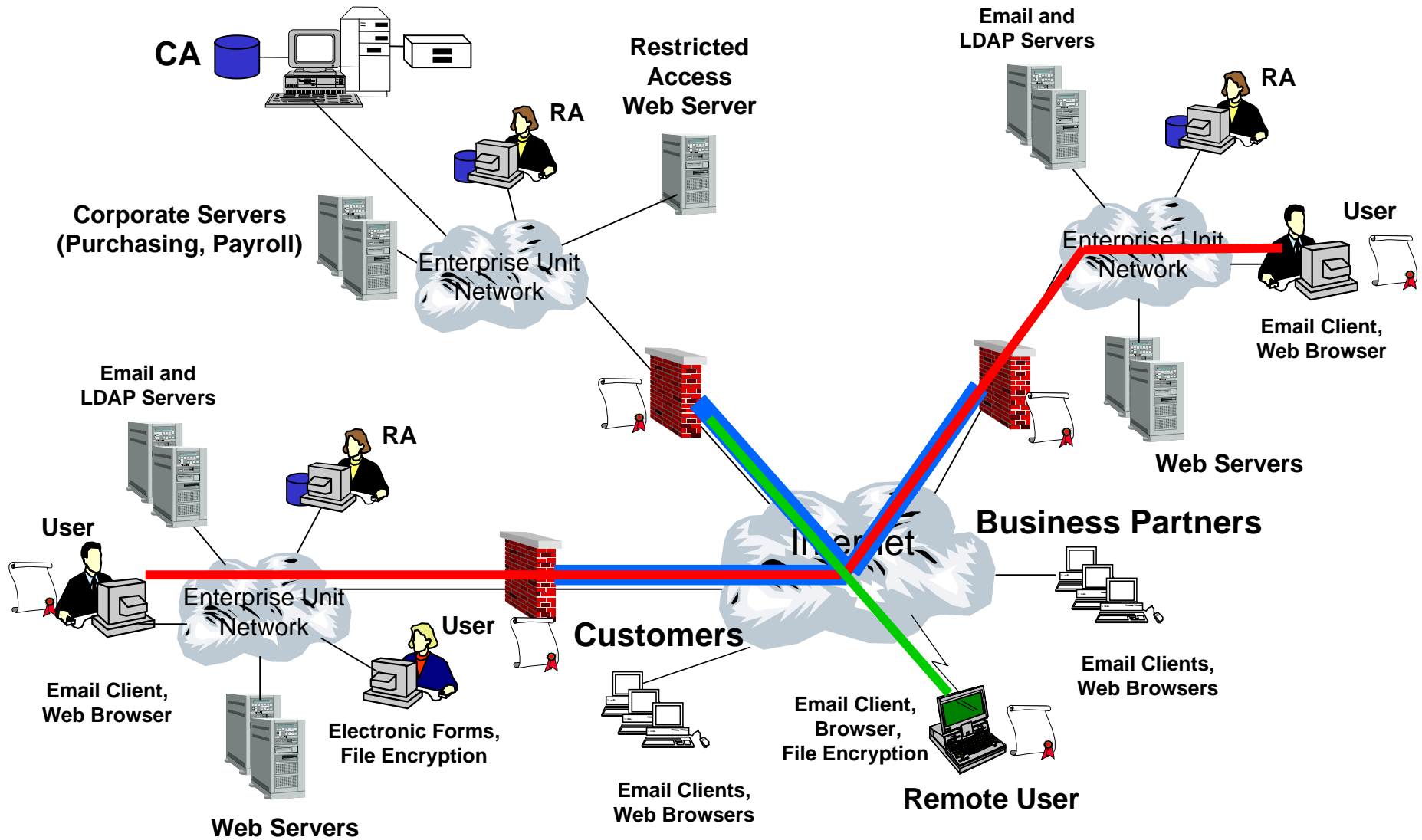
Secure Mail



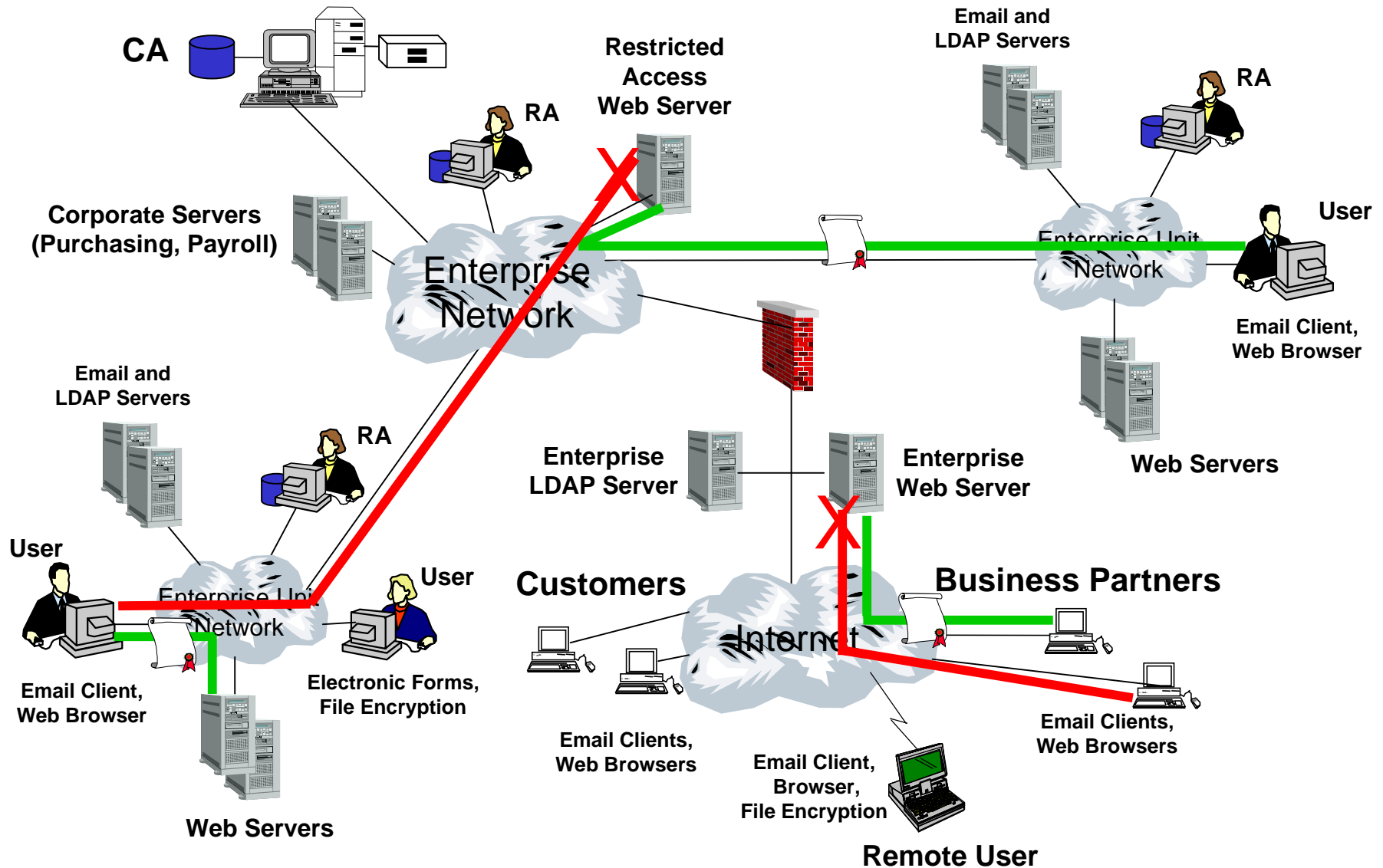
Electronic Form Signing



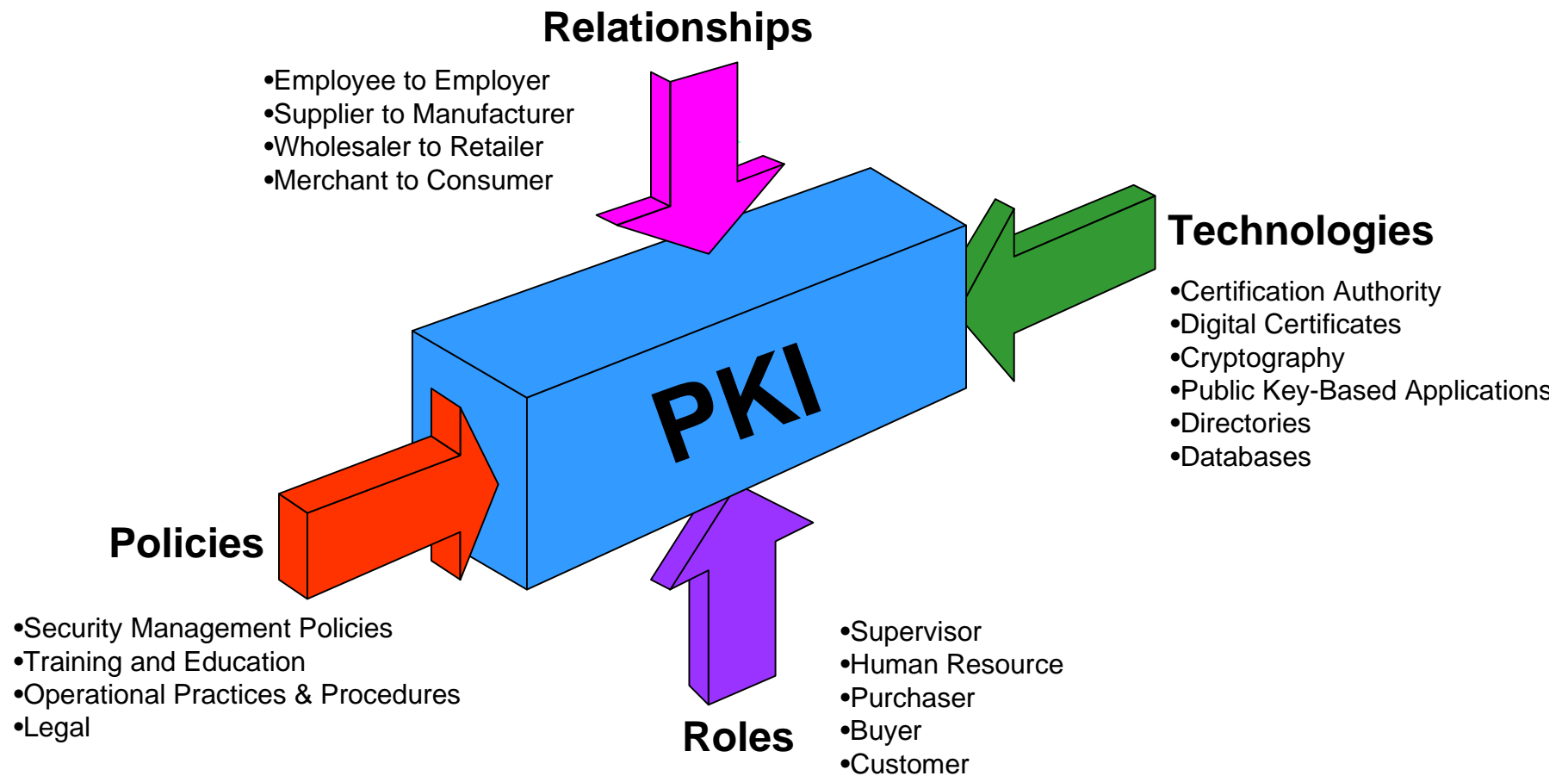
Virtual Private Networks



Secure Web Access



A Complete PKI



**A complete PKI is much more than technology
It is a careful blending of business processes, technology,
policies and procedures**

Contact Information



Judith A. Furlong

judith.furlong@cybertrust.gte.com

Phone: 781-455-4968

Fax: 781-455-3506

www.cybertrust.com