



BALTIMORE™
www.baltimore.com

Public Key Infrastructure (PKI) and Its Application in the New Economy

Rick LaRowe

Director of Engineering, Needham Center

October 23, 2000

Outline



BALTIMORE™
www.baltimore.com

- Core Security Services
- Public Key Cryptography
- Introduction to PKI
- Applications



BALTIMORE[™]
www.baltimore.com

Some Security Issues....



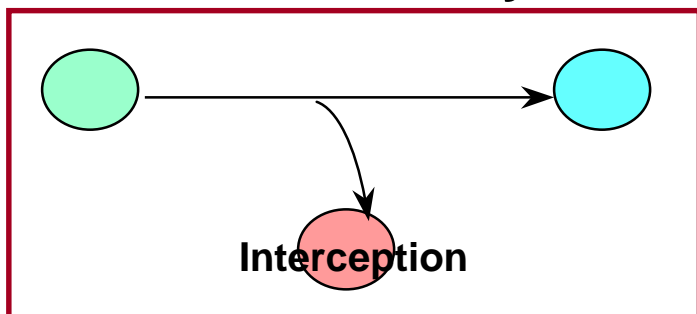
“On The Internet, Nobody Knows You’re A Dog”

Drawing by P. Steiner; © 1993 The New Yorker magazine, Inc.



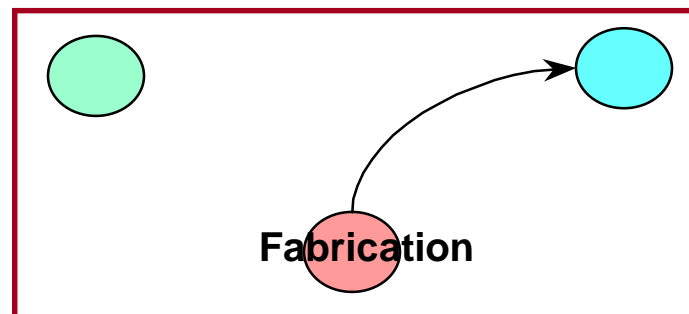
Core Security Services

Confidentiality



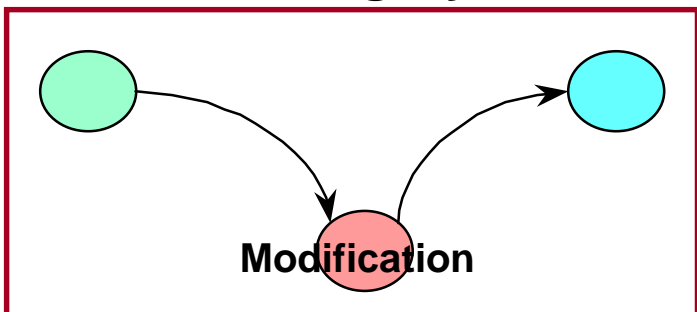
Is my communication private?

Authentication



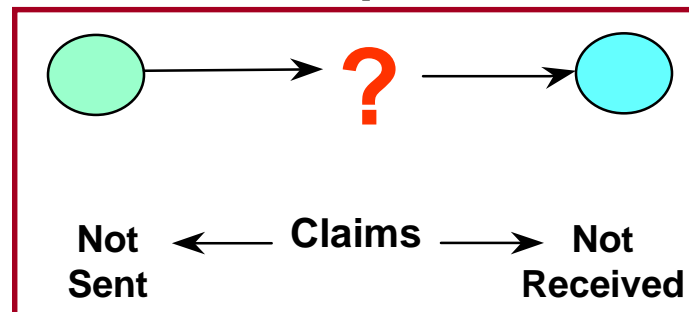
Who am I dealing with?

Integrity



Has my communication been altered?

Non-repudiation



Who sent/received it and when?

Confidentiality Provided by Encryption



BALTIMORETM
www.baltimore.com



Conventional (Symmetric)

One Key

**Used for both
Encryption and Decryption**

Must be protected, kept private

Secure distribution a challenge



Public Key (Asymmetric)

Two Keys

Mathematically related

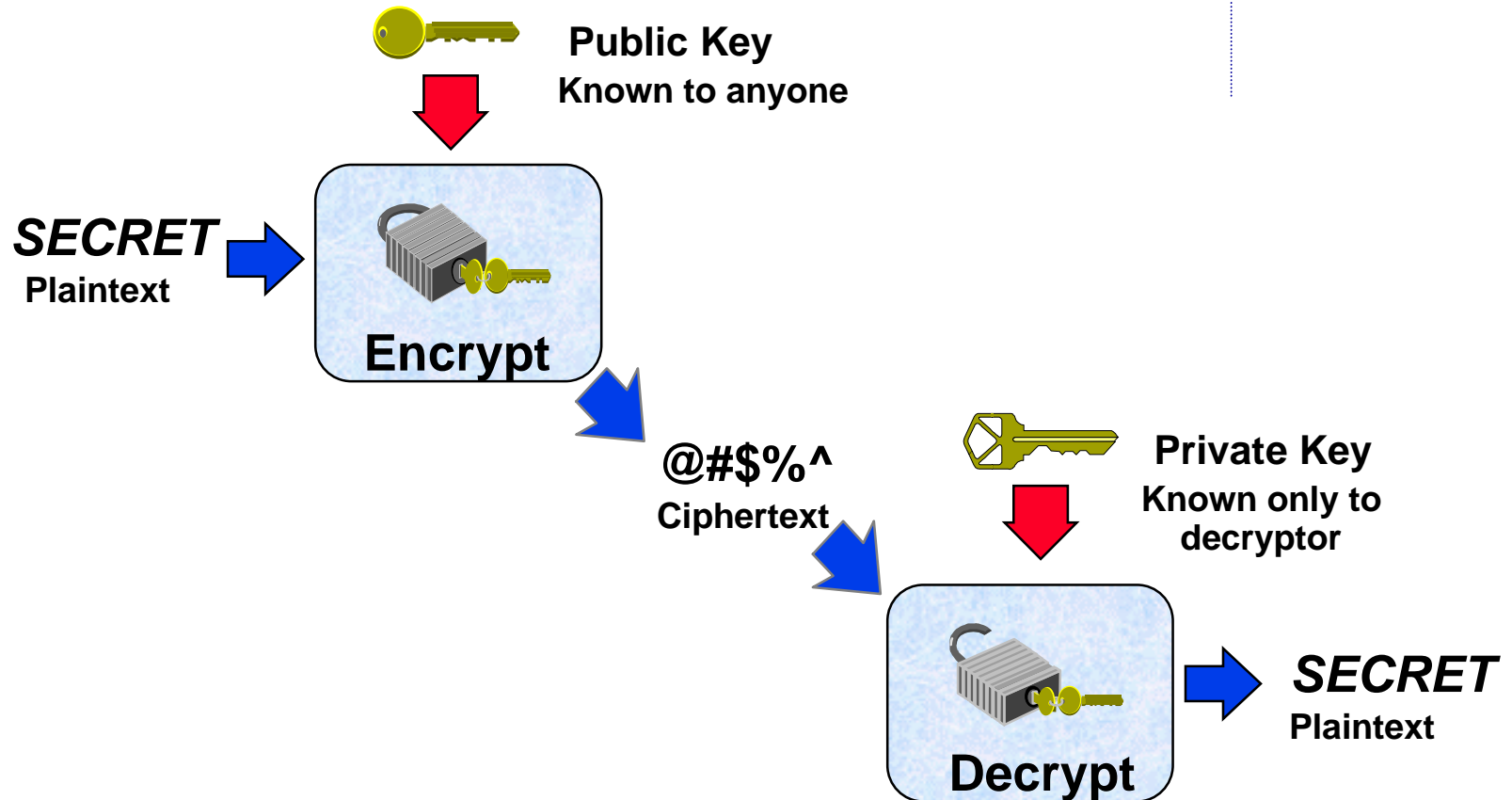
**One key used for encryption,
may be made public**

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

Public Key Cryptography: Encryption



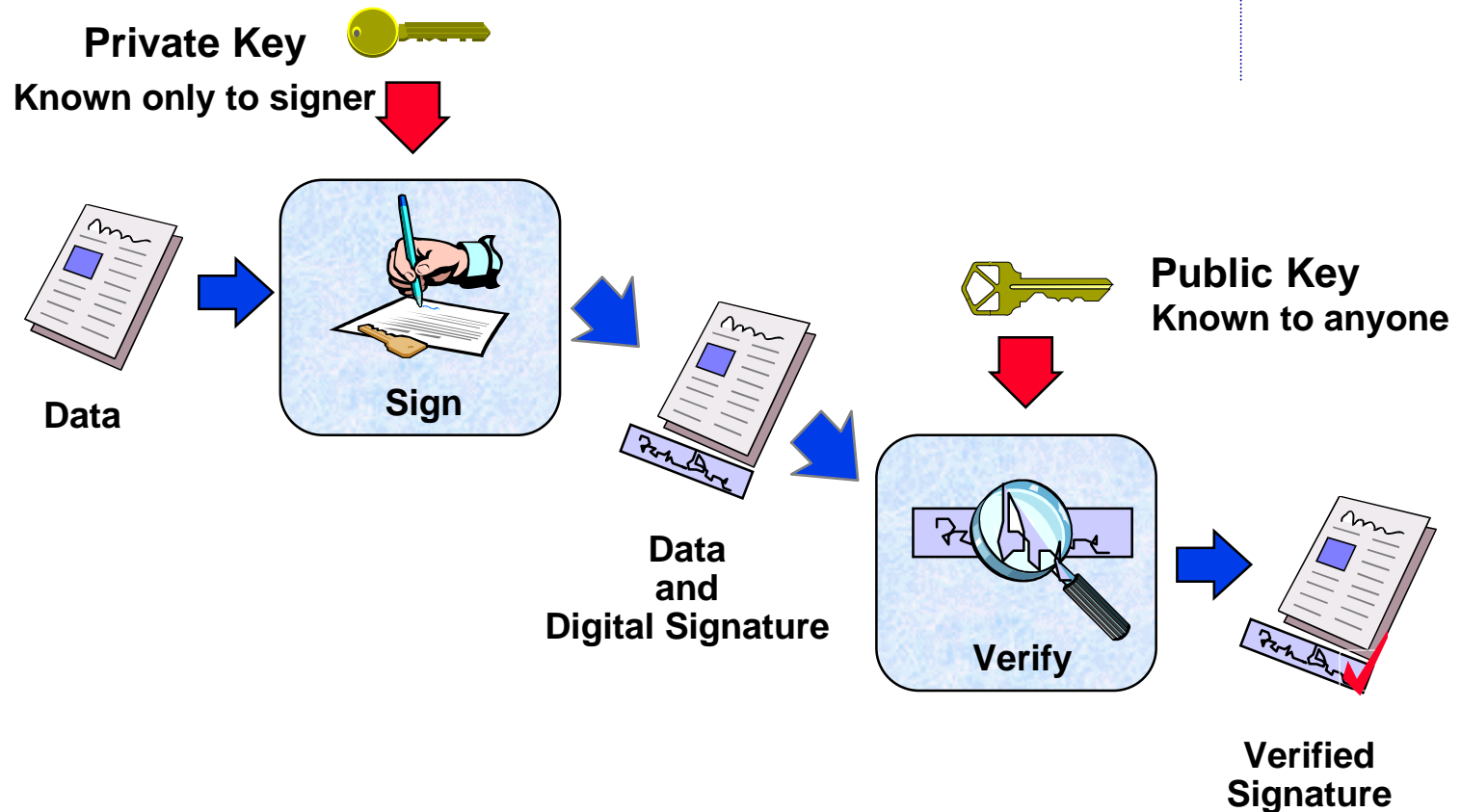
BALTIMORETM
www.baltimore.com



Integrity Provided by Digital Signature



BALTIMORE™
www.baltimore.com



Authentication Provided by Digital Certificates



BALTIMORETM
www.baltimore.com

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

Physical World Analogies

ATM Card -	A Certificate to conduct electronic banking
Driver's license -	A Certificate to operate a vehicle
Passport -	A Certificate to identify you to foreign governments



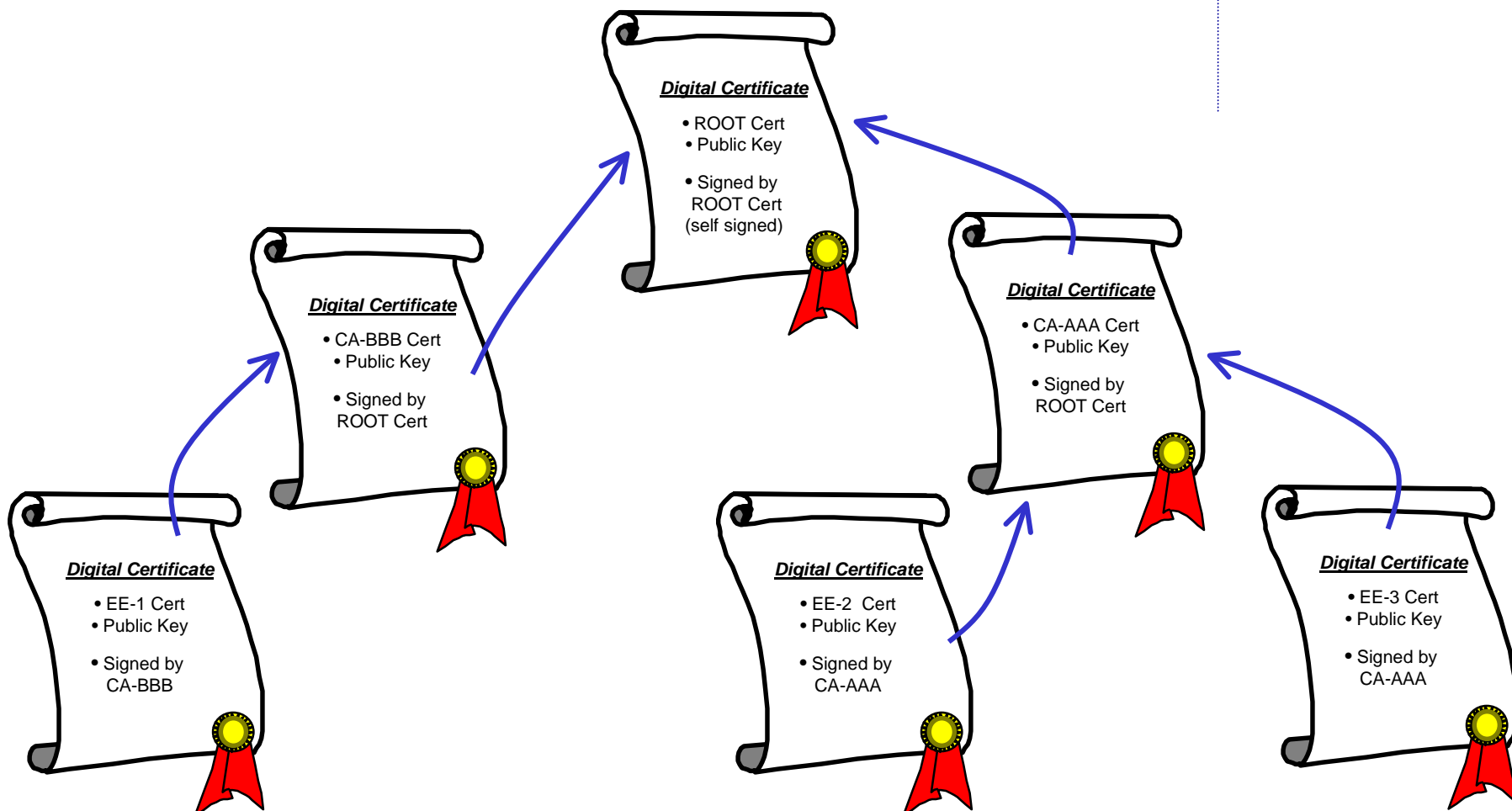
How do you securely generate and distribute certificates?

Certification Authority and Trust

- A CA/RA verifies and vouches for the identity information in a Certificate by signing that certificate with its private key
- Trust hierarchies:
 - End Entity certificates are signed by CA certificates
 - CA certificates are either self-signed (a ROOT) or signed by another CA certificate
 - Trust chains to the root : the self-signed certificate.
- Cross-certification:
 - CA certificates that establish trust relationships without explicit chaining to a common root



A simple Trust Hierarchy





BALTIMORE™

www.baltimore.com

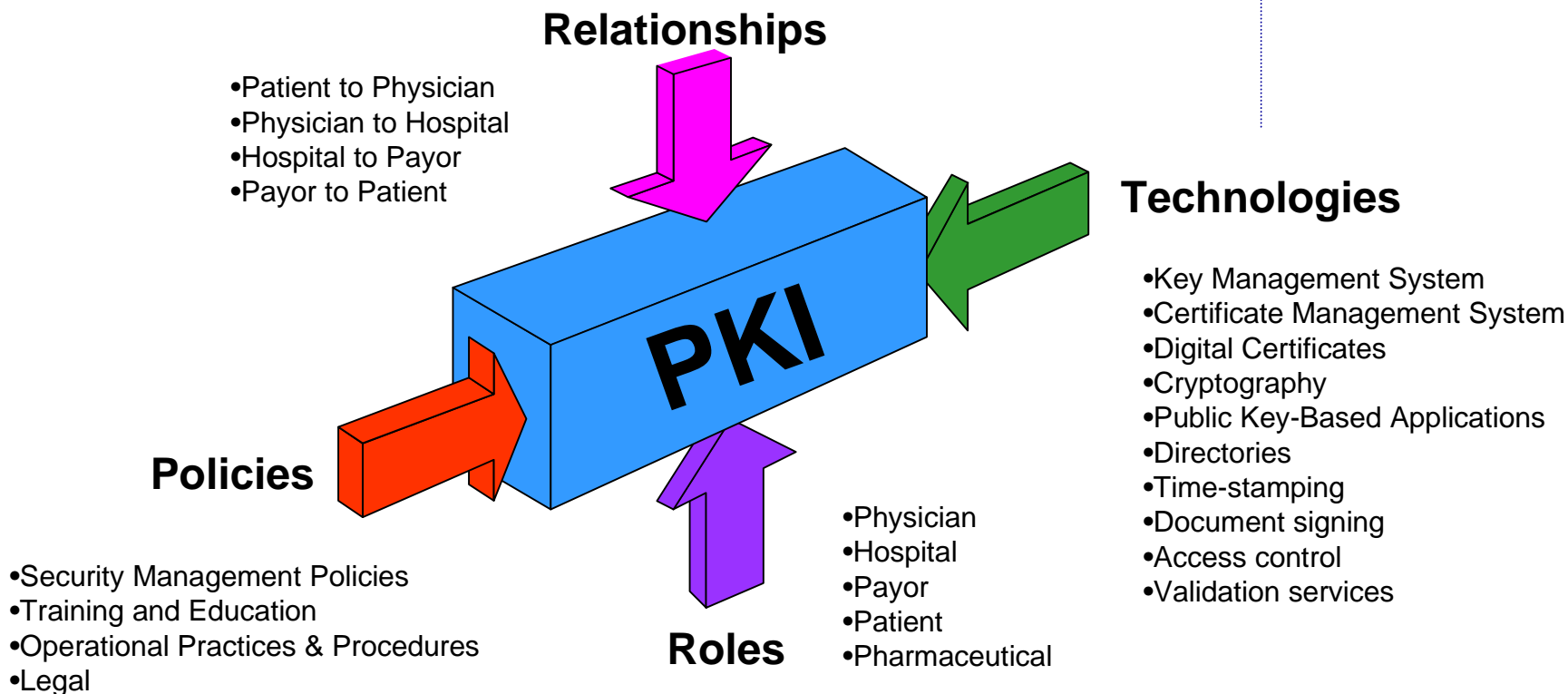
What is a PKI?

- A PKI (Public Key Infrastructure) 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



BALTIMORETM
www.baltimore.com

A Complete PKI



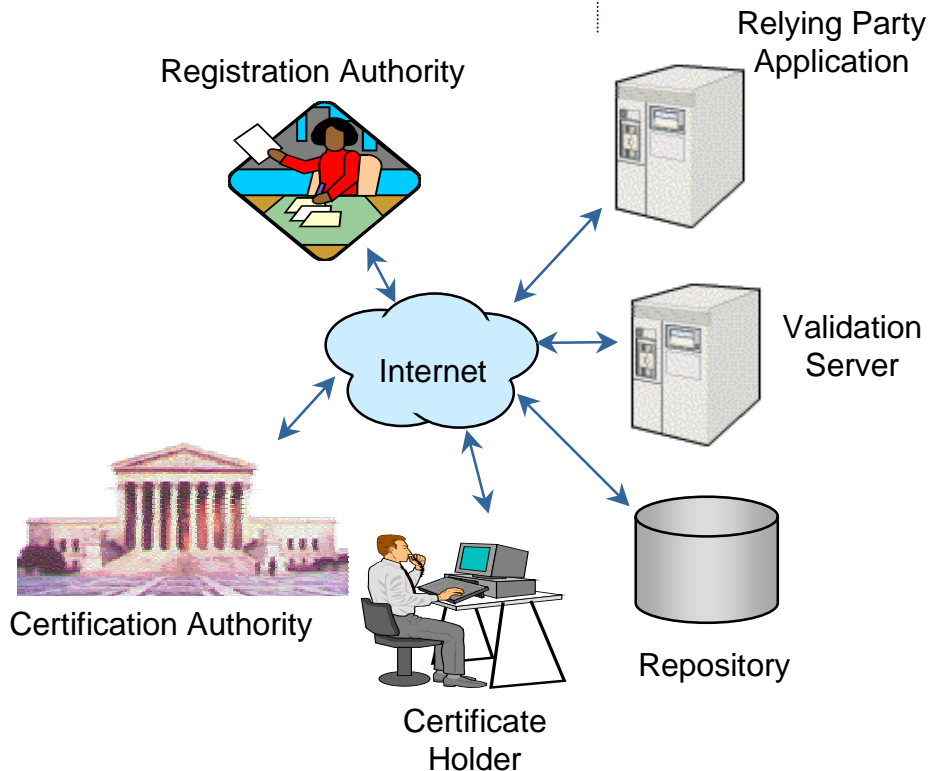
A complete PKI is much more than technology

It is a careful blending of business processes, technology, policies and procedures



Components of a PKI

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





BALTIMORE™

www.baltimore.com

PKI in the New Economy

- The basics - SSL, S/MIME, and IPSEC
- The Wireless revolution
- Access control
 - Extranets (employees, partners, customers)
- Secure payments
 - SET, Identrus, home banking, international payments
- Secure electronic document signing
 - Legally binding contracts
- Secure content delivery
 - Download software, e-books, e-music, e-video, e-tickets

Web Server Authentication (SSL - Secure Sockets Layer)



BALTIMORE™
www.baltimore.com

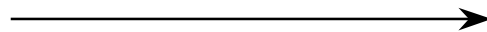
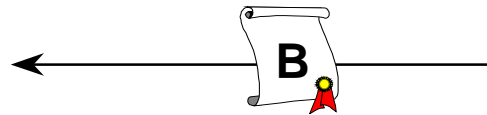


Browser (A)

Secure Web Server (B)



- A Connects to B
- A verifies signature on B's certificate
- A generates Secret Session Key
- A uses B's public key to encrypt Secret Session Key



- B sends copy of its certificate to A

- B uses its private key to decrypt Secret Session Key

A and B use SSL Session Key to encrypt all data exchanged

Mutual Web Authentication (Client-Auth SSL)

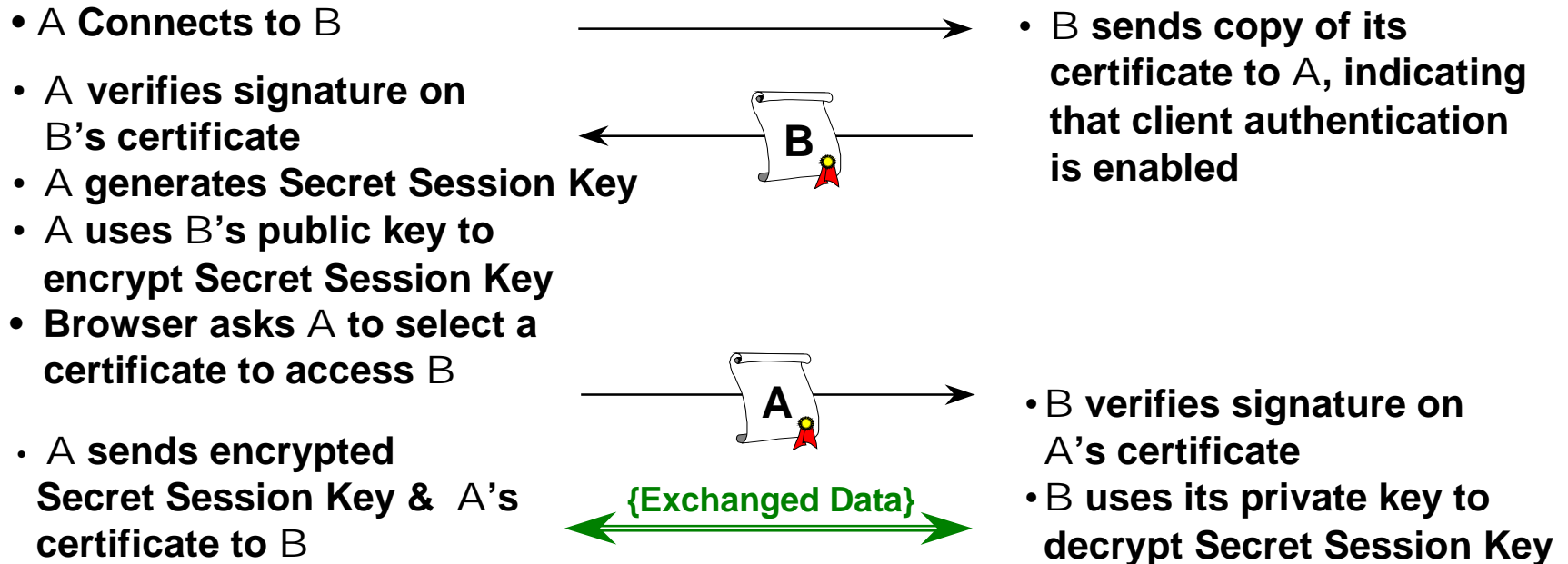


BALTIMORE™
www.baltimore.com



Browser (A)

Secure Web Server (B)

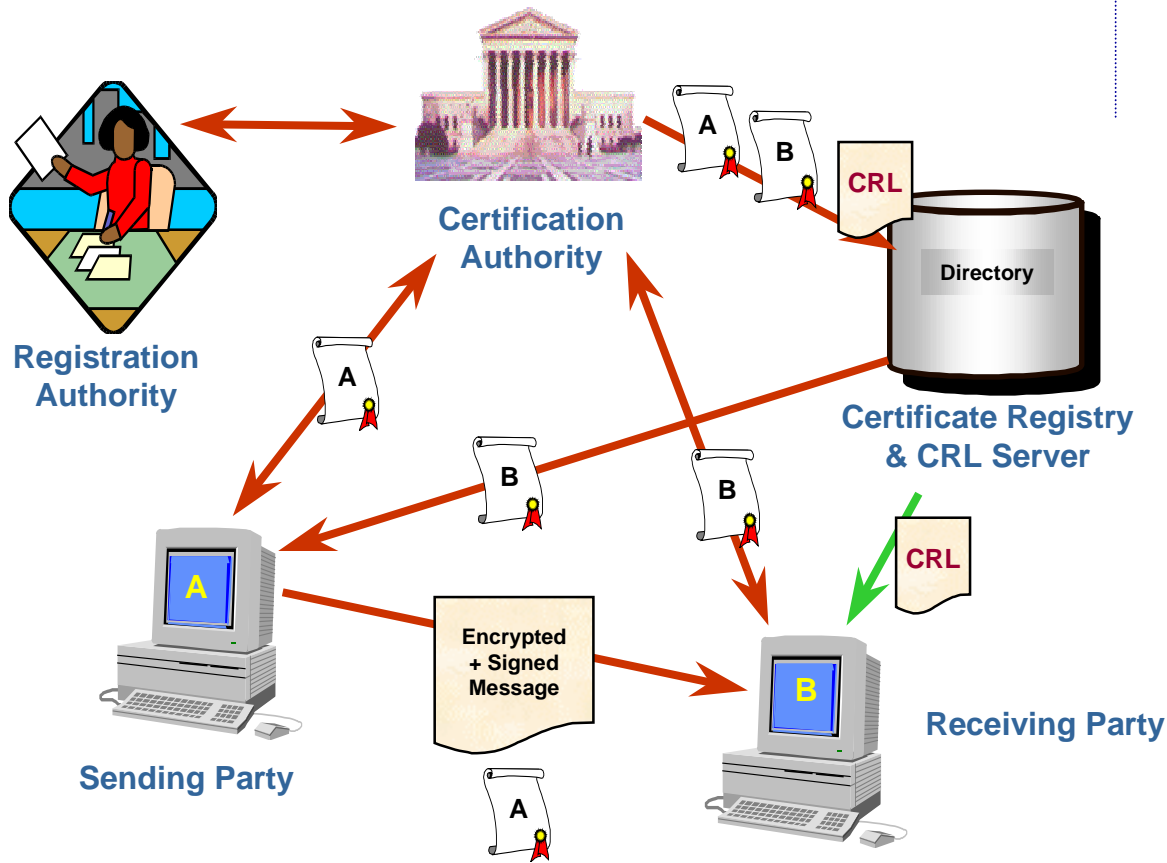


A and B use SSL Session Key to encrypt all data exchanged

Secure E-mail (S/MIME)



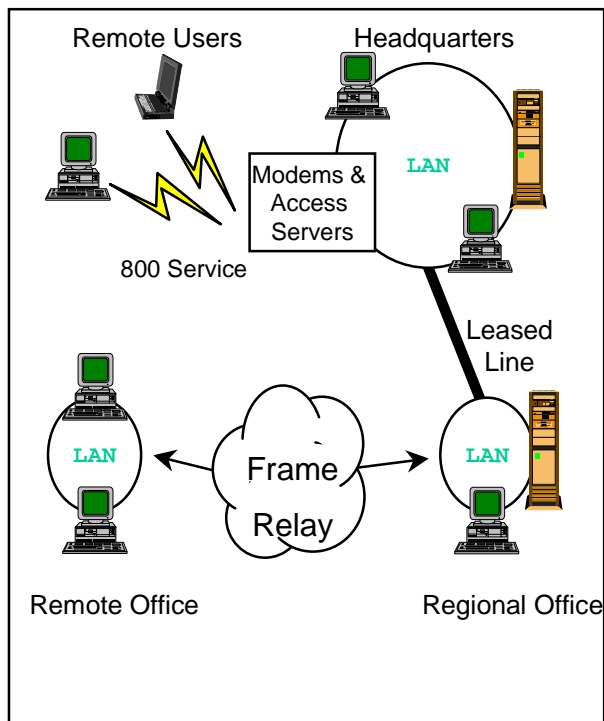
BALTIMORE™
www.baltimore.com





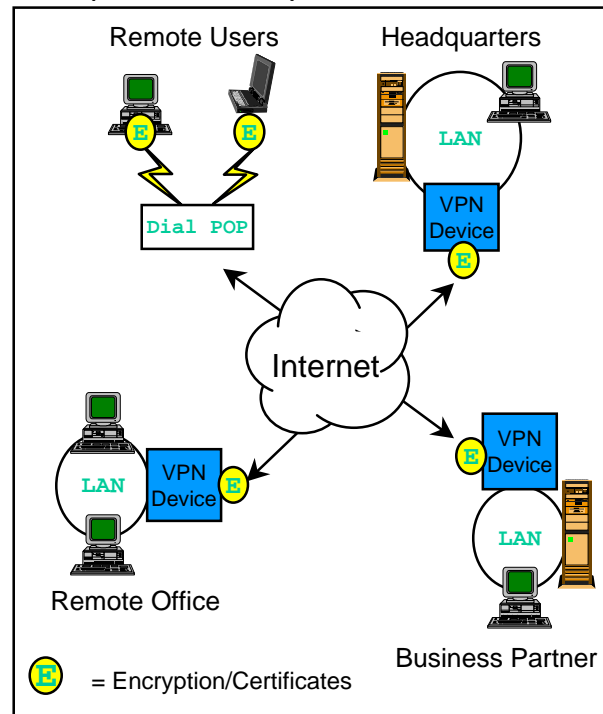
Virtual Private Network

Traditional Data Networks



- Costly,
- Inflexible,
- Limited locations
- Multiple infrastructures

VPN (IP-based) Data Networks

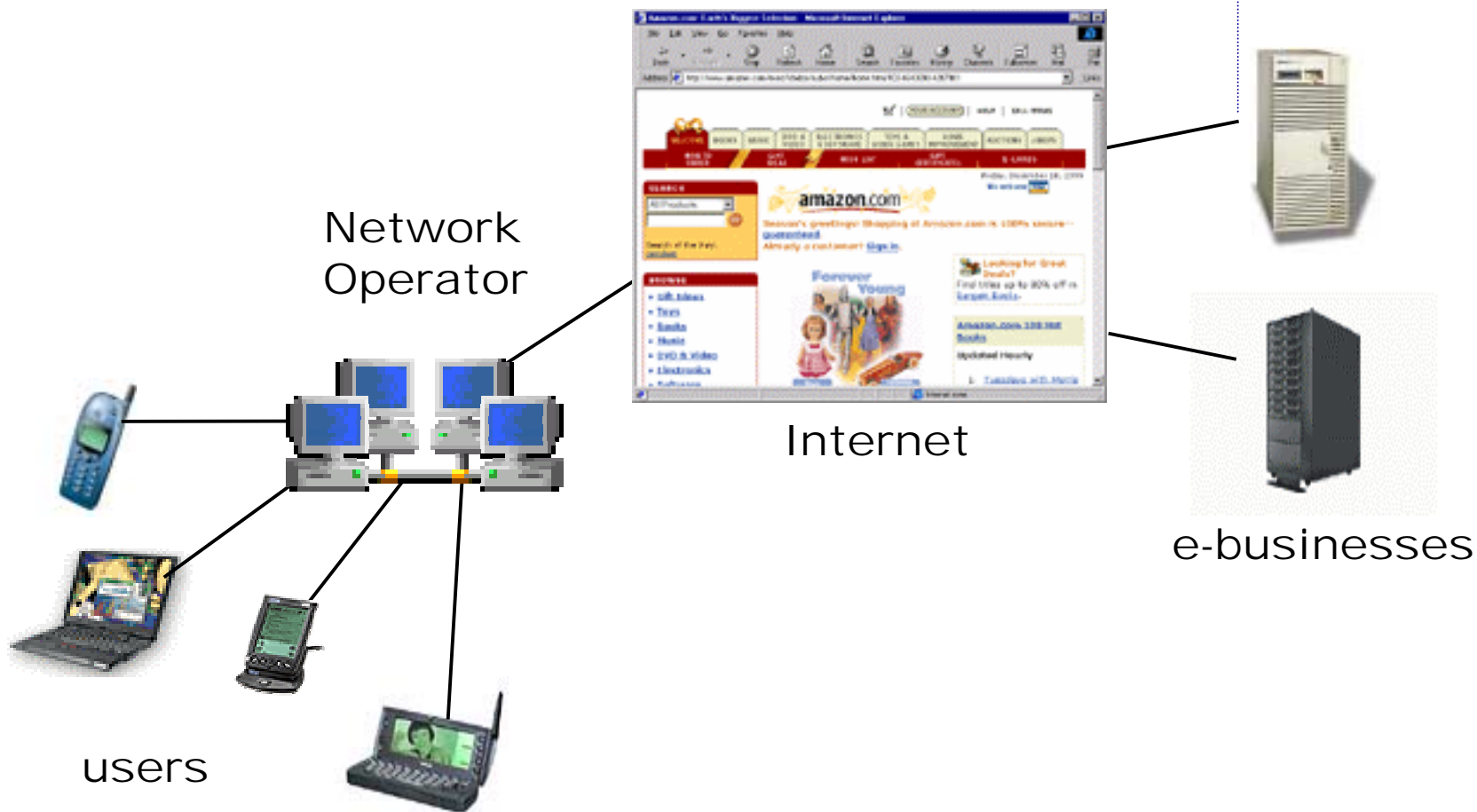


- Inexpensive,
- Dynamically configurable,
- Ubiquitous
- Single infrastructure



BALTIMORE™
www.baltimore.com

Wireless World - How Will it Work?





BALTIMORE™

www.baltimore.com

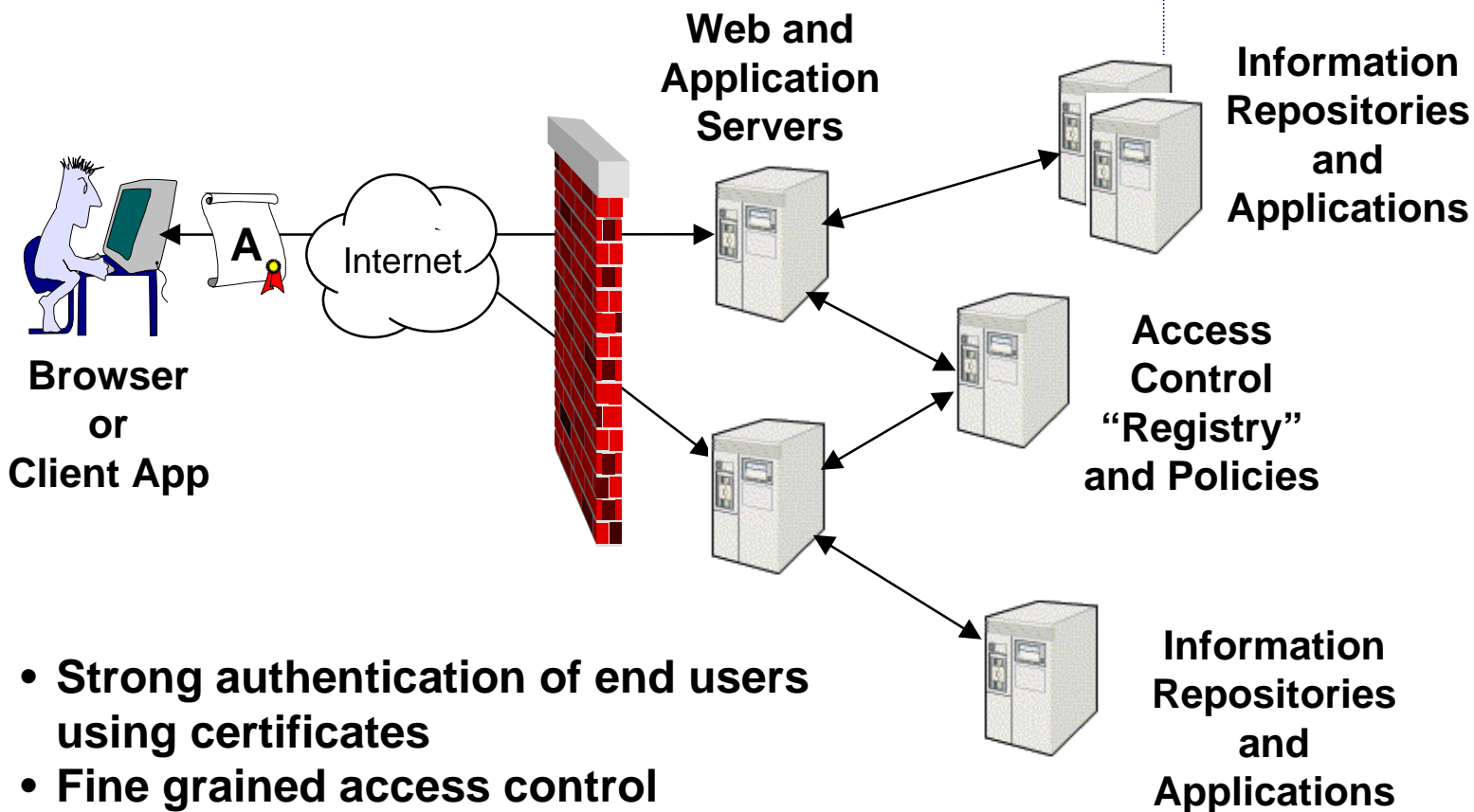
Wireless Session Security





BALTIMORE[™]
www.baltimore.com

Access Control

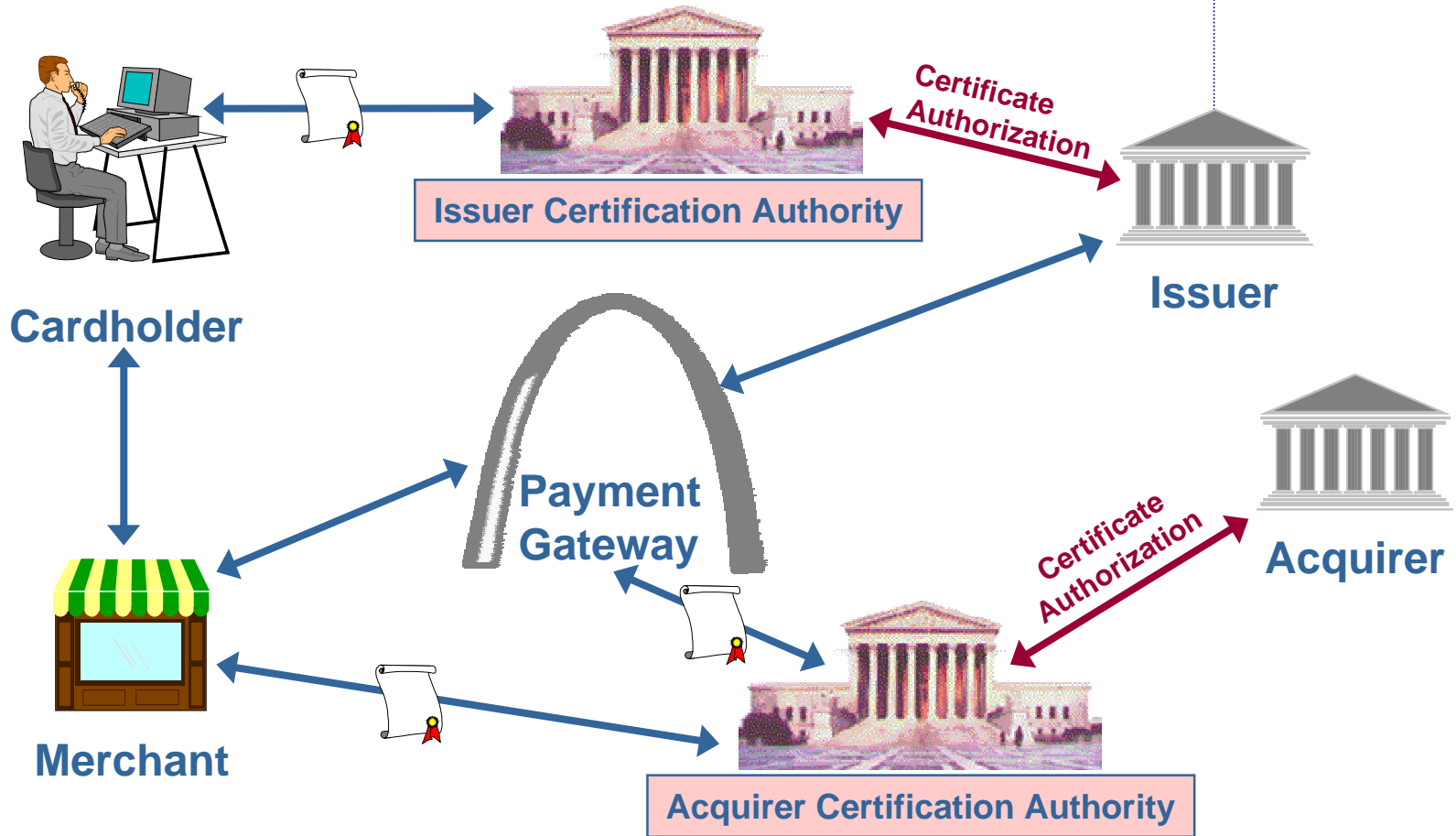


- Strong authentication of end users using certificates
- Fine grained access control
- "Single Sign On"

SET (Secure Electronic Transactions)

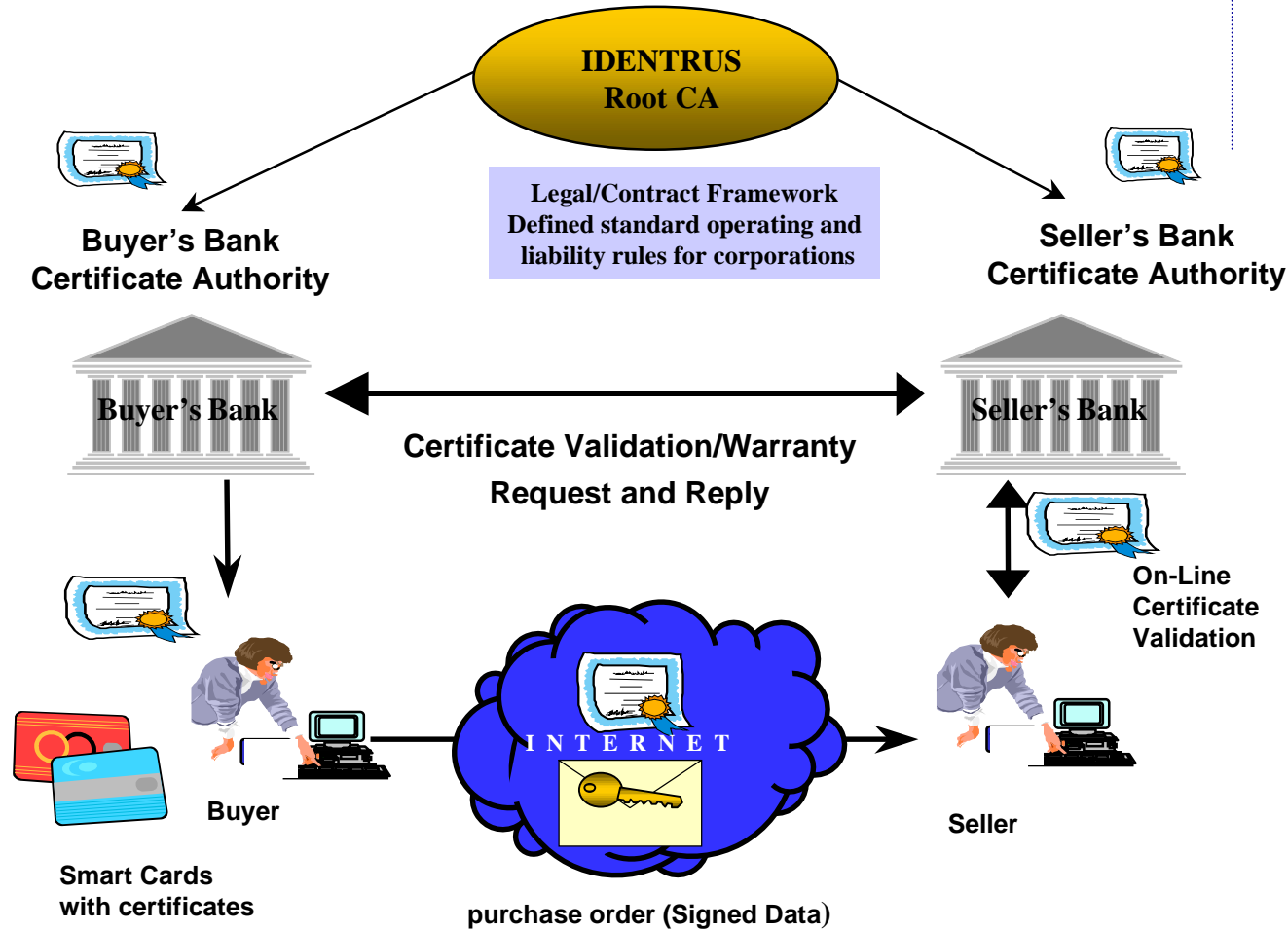


BALTIMORE™
www.baltimore.com





Identrus: B2B Commerce





BALTIMORE™
www.baltimore.com

Secure Electronic Document Signing

- Electronic Signatures in Global and National Commerce (E-Sign) Act
 - Signed into law October 2000
 - Ensures legal recognition of digital signatures
- <http://www.mbc.com/ecommerce.html>
- Germany, Italy, UK, EU and US Governments have enacted legislation
- Examples of applications:
 - Consumer form signing (FormSecure)
 - mortgage applications
 - brokerage accounts
 - insurance policies
 - B2B Contracts



BALTIMORE™

www.baltimore.com

Other applications

- E-tickets
 - encryptix --- signed Indicium, purchased over wireless web, etc.
 - stamps.com
- Lottery / gaming
- Content security (music, data, books, medical records, etc.)
- Secure desktops and enterprises (e.g., Windows 2000 EFS)
- Cable modems, set-top boxes, etc.
 - Device authentication, B2C e-commerce
- Interactive / Personalized TV
 - Content purchase (PPV), B2C e-commerce, home banking, etc.



BALTIMORE™
www.baltimore.com

Issues / Futures

- Standards and interoperability
- Policy management
- Applications integration
- Deployment
- Roaming solutions