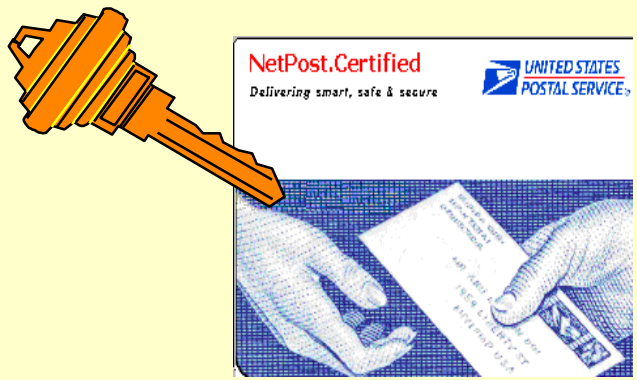
Cryptographic Module Validation Program (CMVP) 2002 Conference



Kim Mitchel

Deputy Associate Commissioner

Office of Telecommunications and Systems Operations

March 27, 2002

"As new discoveries are made, new truths discovered, and manners and opinions change, institutions must advance also to keep pace with the times."

Thomas Jefferson

UBIQUITOUS

OUR VISION

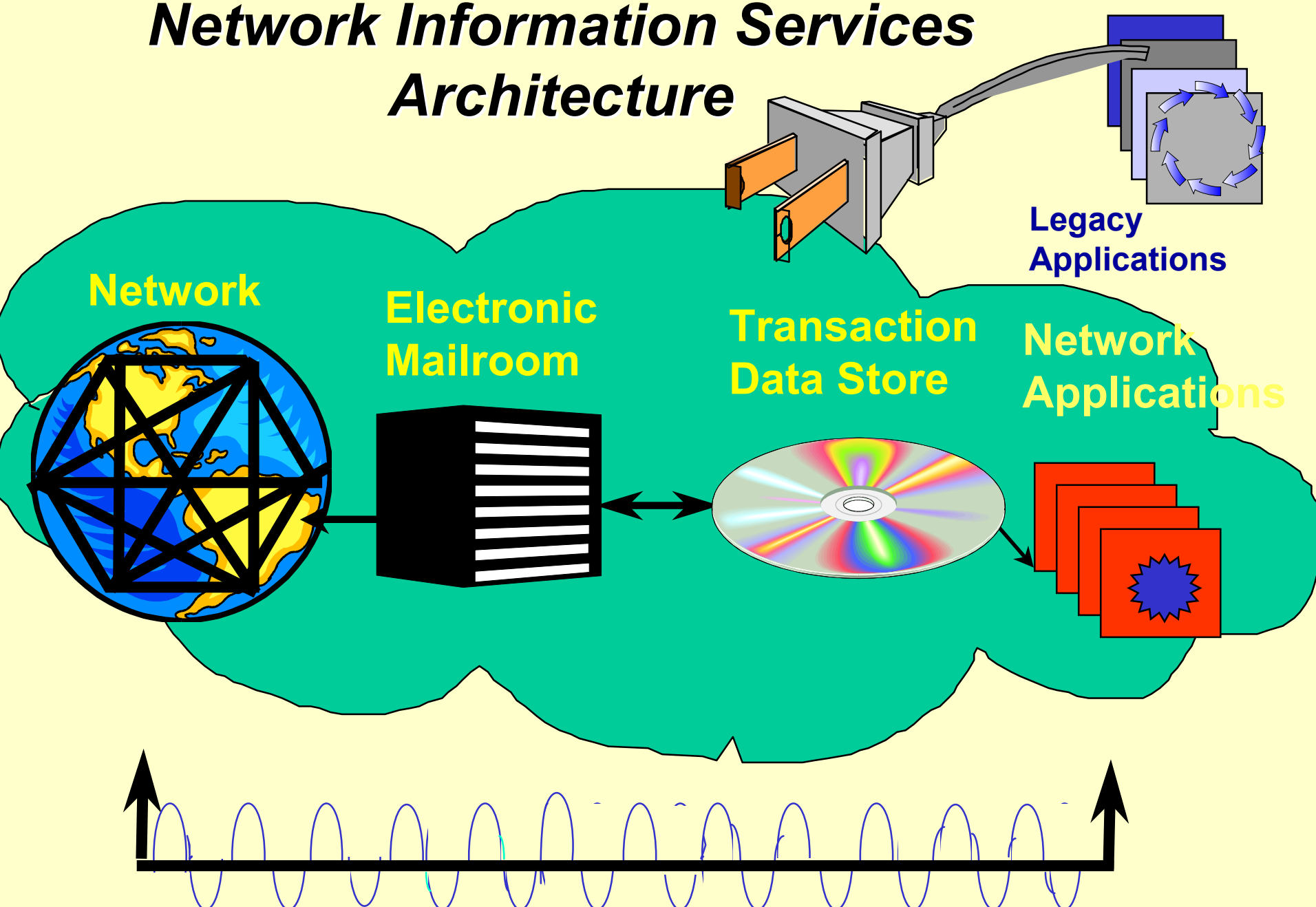
Global Communications

….Where All Information Barriers
Have Been Eliminated

Equalitarian

When implemented costs are low enough for anyone to use it…….

Network Information Services Architecture



Challenges E-GOV Applications Face

- **Authentication of Users**
- **Non-repudiation for transactions**
- **Confidentiality (privacy)**
- **Liability**
- **Scalability/extensibility**
- **Timestamp**

The further backward you look, the further forward you can see.

Sir Winston Churchill

Back to the Future

1936

USPS issues 26 million SSNs

UNITED STATES POSTAL SERVICE

USPS NetPost.Certified (NPC) Program

200?

USPS issues millions of PKI Smartcards for E-Gov

The NetPost Solution

Major Components / Current Status

NetPost.Certified Compares to Mail System

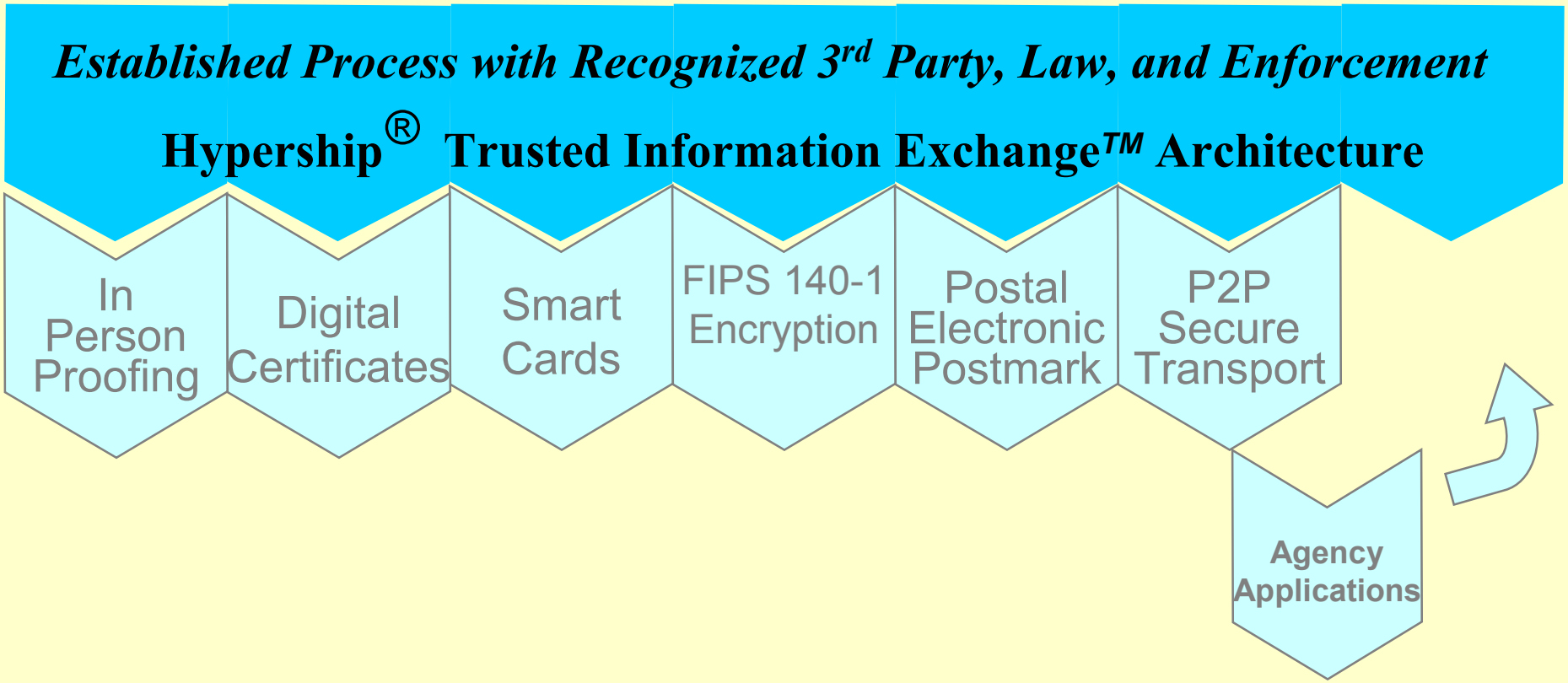
Business Application Independent

File Type Independent

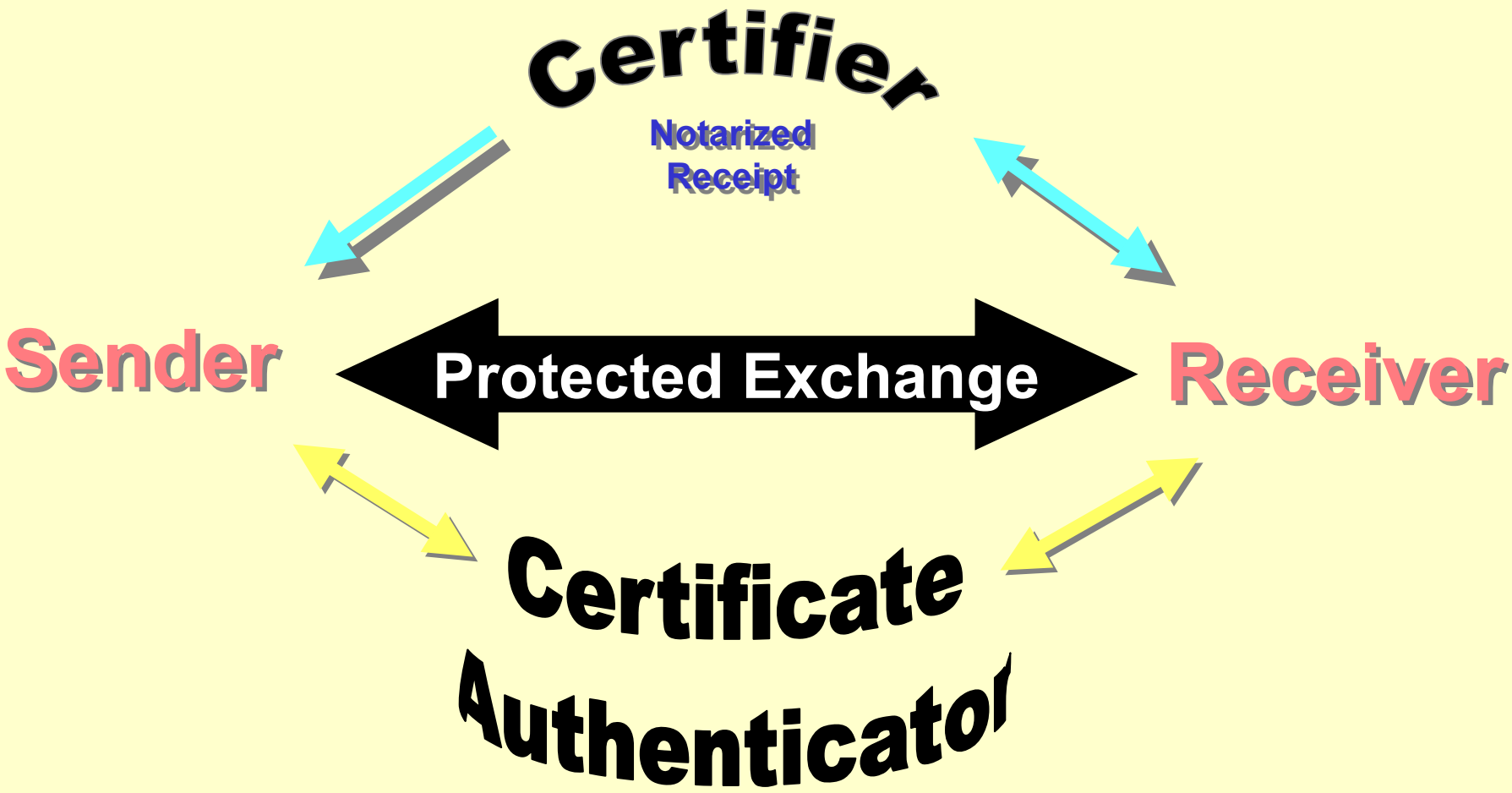
File Size Independent

Transport Independent

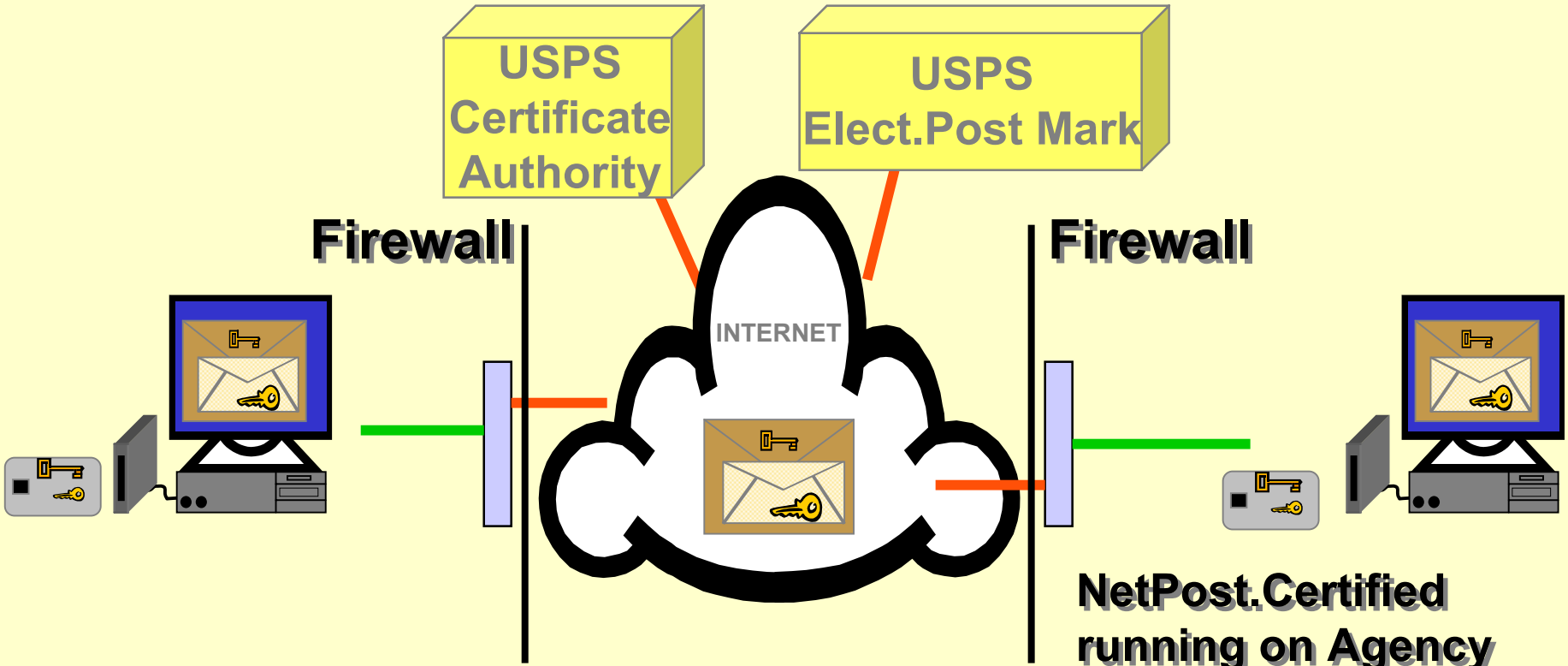
USPS NetPost.Certified



Peer-to-Peer
Trusted Information Exchange



How NetPost.Certified Works



NetPost.Certified ™ Provides

- In-Person Authentication of Sender
- Data Integrity
- Confidentiality
- Secure Transport
- Postal Date/Time Stamp
- Legal Status Protection

Electronic Postmark

Notary - **USPS Certified Electronic Post Mark**

A NetPost.Certified powered network enables an automated, third party notary that notarizes the delivery of every package.

Pilot Capabilities- Operational

- Encryption/Decryption
- Digital Signatures
- Secure Transport
- Automatic File Transfer and Routing (via Data Linked Directories)
- GUI to Select File and Recipient
- Electronic PostMark Receipts

NetPost.Certified Components

- USPS Electronic Post Mark (EPM)
- Patented (U.S. No. 6,219,669) Hypership ® TIE Architecture using Industry Standard TCP/IP
- Industry Leader RSA BSAFE ® -- Cert C and Cert J
- Industry Standard PKCS-11 Smart Card Interface
- Industry Standard Certificate Authority Interface
  - USPS RA & CA ⇔ in-person proofing
  - X.509 Certificates
  - Sign & encryption keys
  - LDAP Directory (CA & CRL)
  - Netscape, Microsoft
  - Cylink NetAuthority(used by USPS)

NetPost.Certified: FIPS 140-1

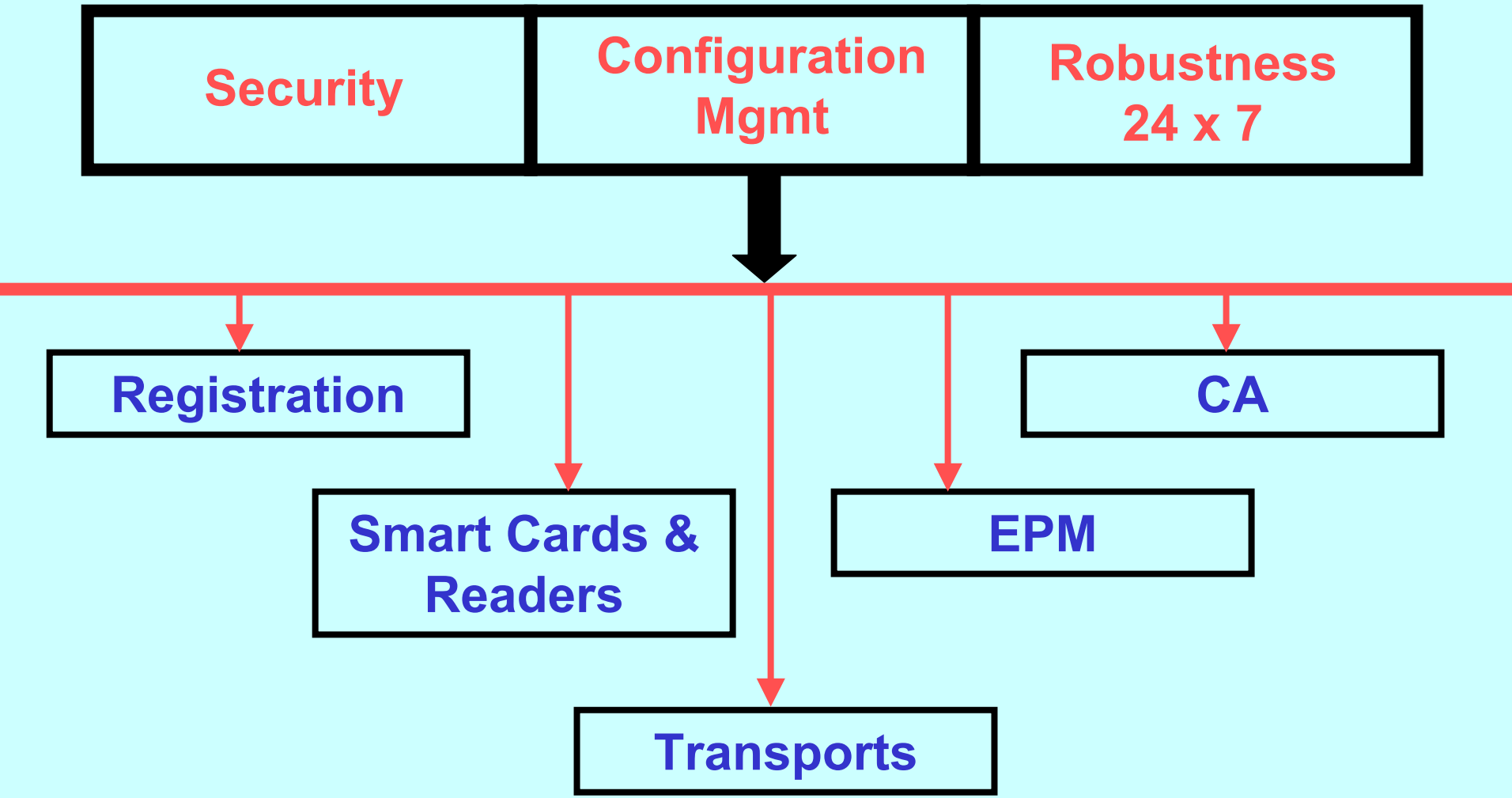
FIPS-approved algorithms: Triple-DES (Cert. #38); DSA/SHA-1 (Cert. #38)

Key Management: RSA BSAFE Cert C / Crypto C

Certificate Authority: Cylink NetAuthority (X.509 Certs)

Cryptographic Standards: PKCS-7; PKCS-11; PKCS-12

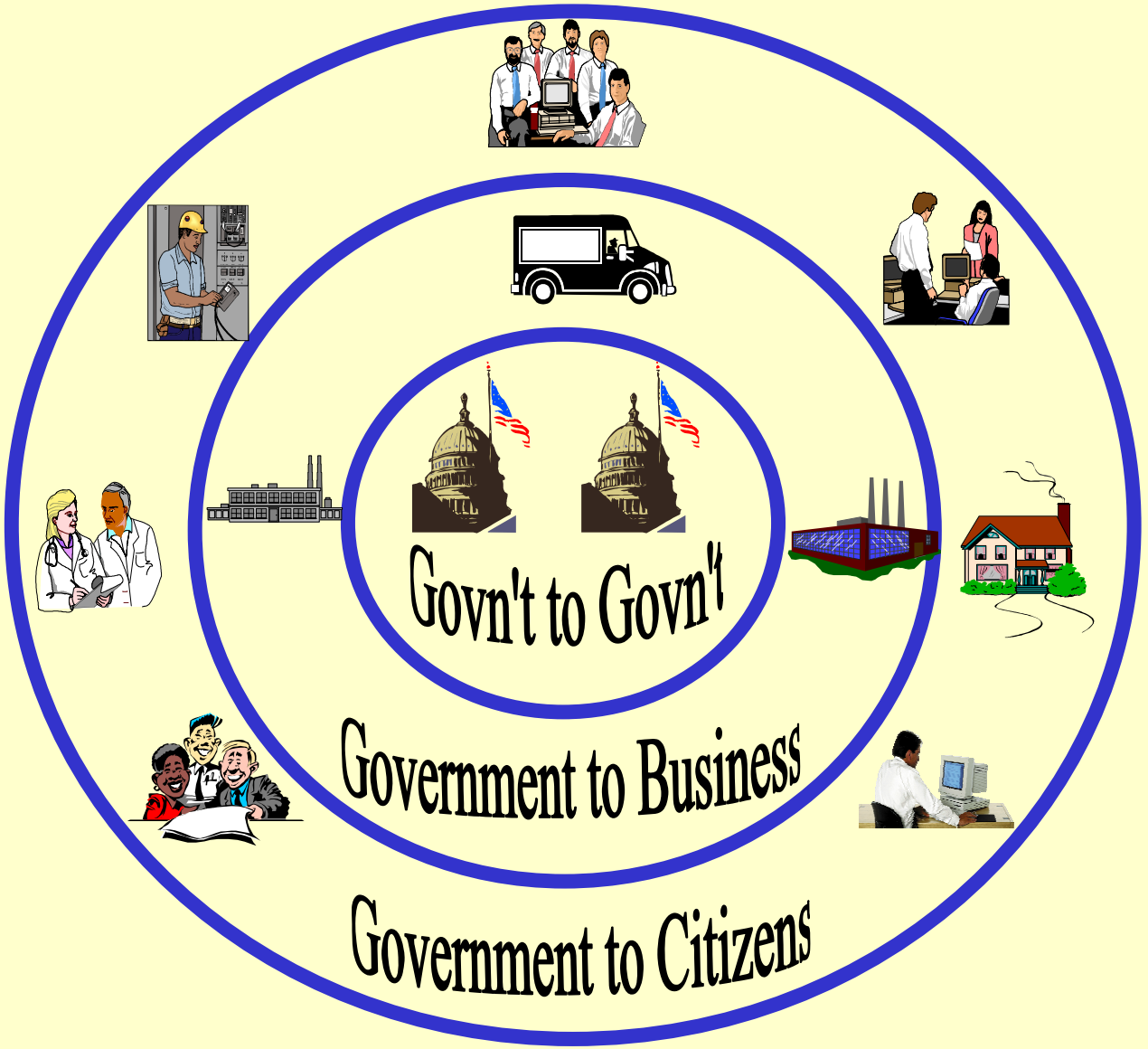
META TECHNICAL ARCHITECTURE



Why Partner with USPS?

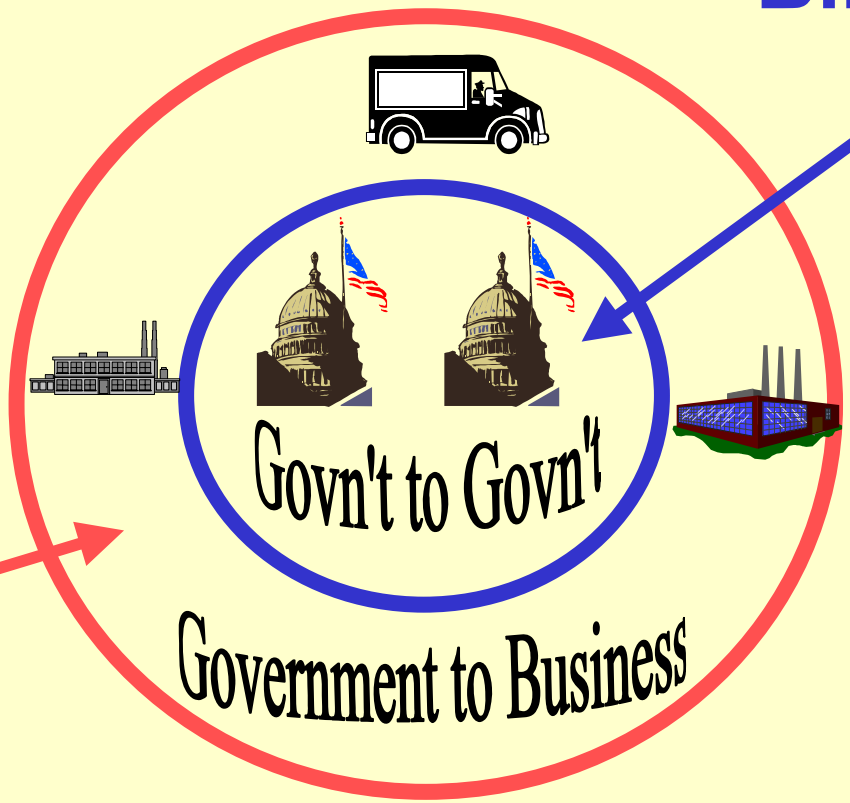
- Innovative Technology
- Integrated Solution
- Scalability
  - Logistics
  - Economics
- Legal Foundation
- Trusted Provider

The Strategic Implementation Plan



The Tactical Implementation Plan

Birth & Death



Prisons