GSA

Federal CIO Council

Federal Public Key Infrastructure

Steering Committee

Federal Approach to Electronic Credentials

Information Assurance in an E-World

Judith Spencer
Chair of the Federal PKI Steering Committee
judith.spencer@gsa.gov
http://www.cio.gov/fpkisc

Privacy Act of 1974

- 4 Basic Objectives
  - To restrict disclosures of personally identifiable records
  - To grant individuals more rights to access records agencies maintain on them
  - To grant individuals the right to seek amendments to agency records maintained on themselves
  - To establish a code of "fair information practices" which requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records

Identity Credentials

- Driver's License
- Employee Identification Card
- Passport
- Birth Certificate
- Physical Presence
- Signature

Legislative Mandate

- Government Paperwork Elimination Act, October 1998
  - Commitment to on-line government
  - Public electronic access by October 2003
- Electronic Signatures in Global and National Commerce Act, June 2000
  - *“A signature may not be denied legal effect simply because it is electronic”*

E-Transaction Landscape

Internal Effectiveness and Efficiency

Government to Business

Government to Government

Government to Citizen

E-Gov Initiatives

Government to Citizen

• USA Service	GSA
• EZ Tax Filing	Treas
• Online Access (Loans)	DoEd
• Recreation One-Stop	DOI
• Eligibility Assist Online	Labor

Government to Government

• e-Vital (business case)	SSA
• e-Grants	HHS
• Disaster Assistance and Crisis Response	FEMA
• Geo-spatial Information One-Stop	DOI
• Wireless Networks	DOJ
• Enterprise Legal Case Management	DOJ

Government to Business

• Federal Asset Sales	GSA
• Online Rulemaking	DOT
• Simplified and Unified Tax and Wage Reporting	Treas
• Consolidated Health Informatics	HHS
• Business Compliance One-Stop	SBA
• Int'l Trade Process Streamlining	DOC

Internal Effectiveness and Efficiency

• E-Training	OPM
• Recruitment One-stop	OPM
• Enterprise HR Integration including e-Travel	OPM
• Integrated Acquisition	GSA
• E-Records Management	NARA

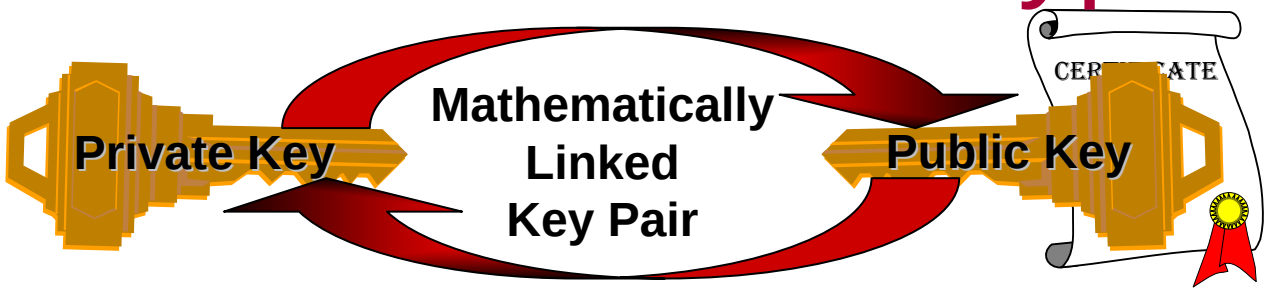
A Few Facts

- Internet is perceived as inherently anonymous
- In order to protect privacy, government must know with whom it is dealing
- Knowledge must be within reasonable risk limits
- Electronic credentials provide the means to link identity in the electronic medium

What is Security on the Internet?

- User Authentication
  - Knowing who your correspondent is
- Transaction Integrity
  - Ensuring the message sent is the message received
- Non-Repudiation
  - Correspondent cannot deny conducting transaction
- Confidentiality
  - Only authorized persons can read the message

Asymmetric Key Encryption



- Protected by Owner
- Used as Identity Credential
- Used to Sign Messages
- Used to Decrypt
- Distributed Openly
- Used to Authenticate Identity
- Used to Verify Signatures
- Used to Encrypt

Identity Credentials

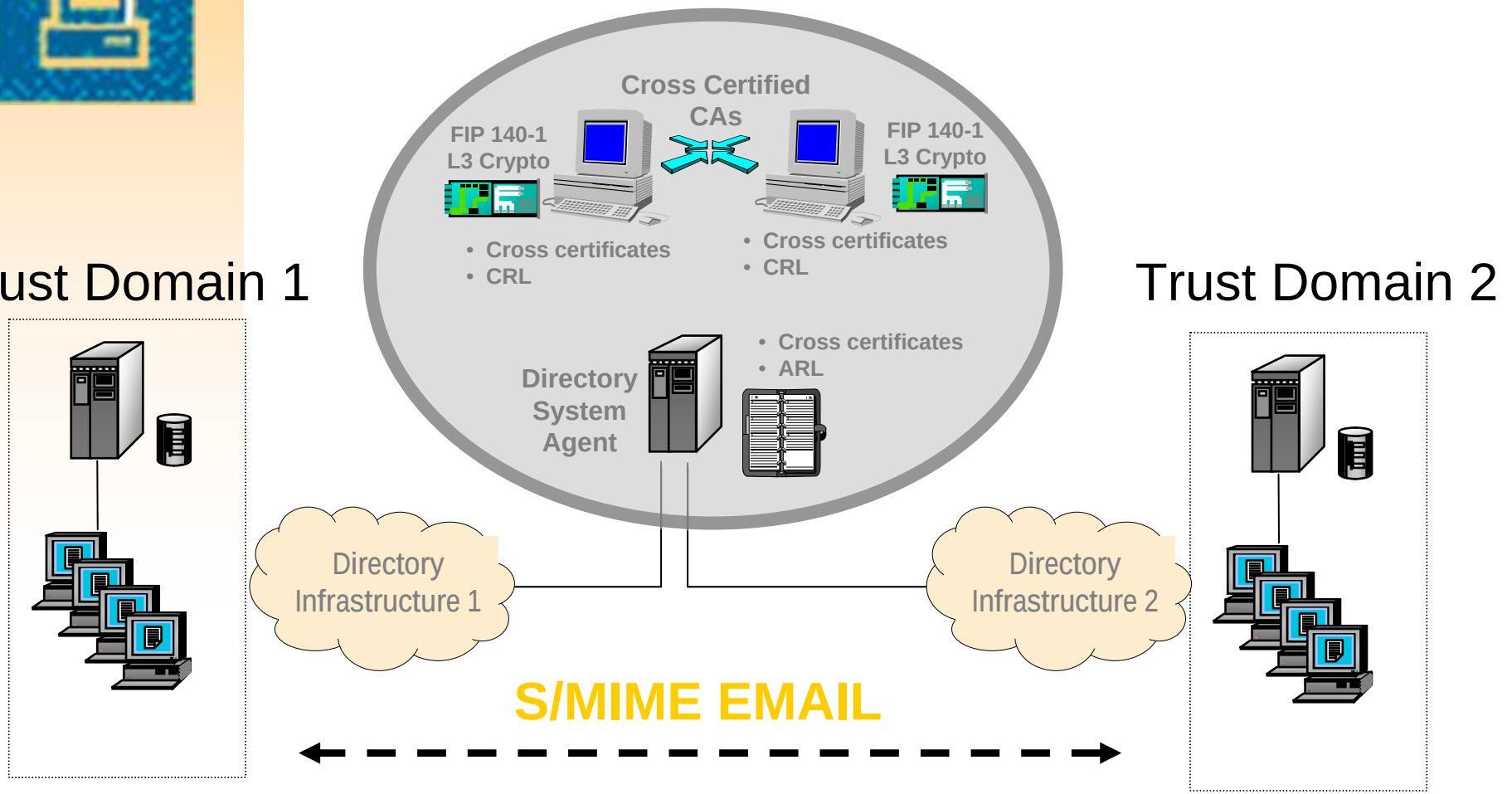
- Driver's License
- Employee Identification Card
- Passport
- Birth Certificate
- Physical Presence
- Signature
- Electronic Credentials (PKI Certificates)

The Way Forward

Simplify and Unify

- Promote Quicksilver e-Authentication Initiative
- Assist other initiatives in defining their identity authentication needs
- Develop applications for cross-governmental use
- Coordinate consolidated buy of authentication products and services
- Promote interoperability with other entities through FBCA

Federal Bridge Certification Authority



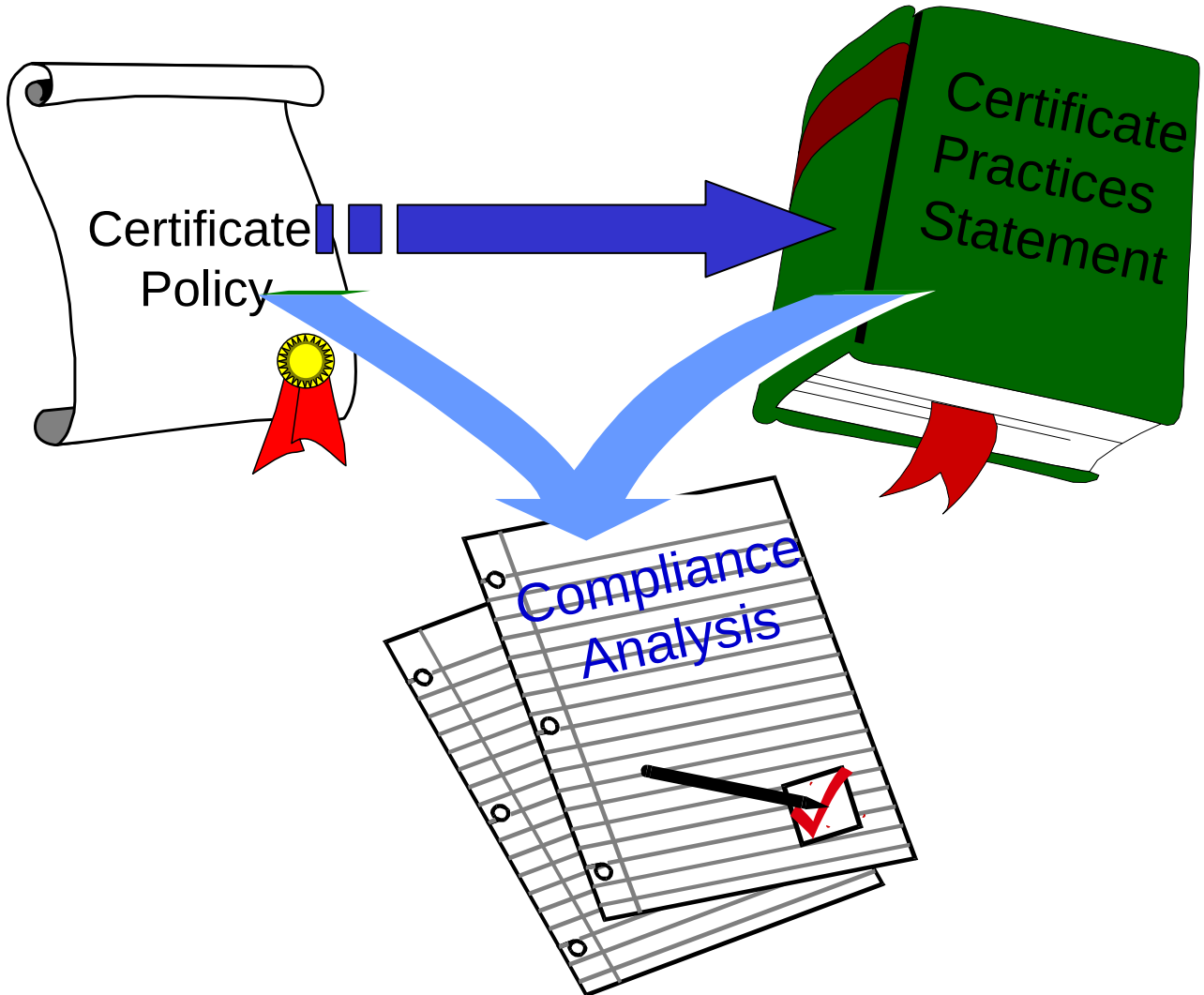
Federal PKI Policy Authority

- Voluntary interagency group - NOT "agency"
- Governing body for FBCA interoperability
- Oversees operation of FBCA, authorizes issuance of FBCA certificates
- Answers to Federal CIO Council
- Six Charter Members:
  - GSA, Justice, DoC, NSA, OMB, Treasury

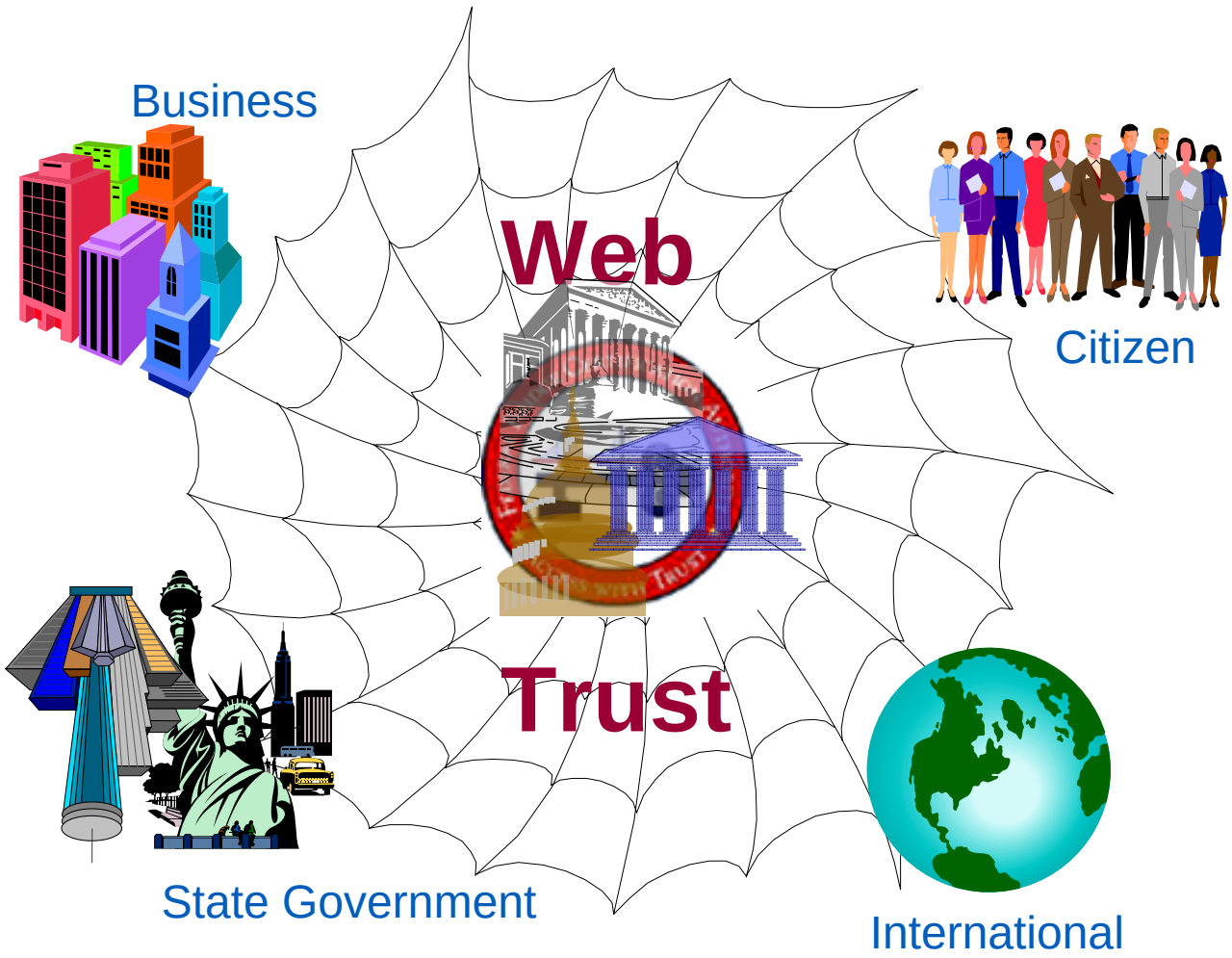
Policy Mapping

- Organization is mapped to one of 4 levels spelled out in Bridge Certificate Policy
  - Rudimentary
  - Basic
  - Medium
  - High
- Only applies to Organization relationship with Bridge for purposes of interoperability

Required Documentation



A Vision for the Future



Closing Words

- Our Vision - Enable e-government through:
  - A cross-governmental, ubiquitous, interoperable Public Key Infrastructure.
  - The development and use of applications which employ that PKI in support of Agency business processes.
- Government-wide initiatives include:
  - Federal PKI Steering Committee
  - Federal PKI Policy Authority
  - Federal Bridge Certification Authority
  - Access Certificates for Electronic Services