The Federal PKI - Looking Forward

A Perspective on the Federal Government Secure Infrastructure

Judith Spencer

Chair, Federal PKI Steering Committee

www.cio.gov/fpkisc

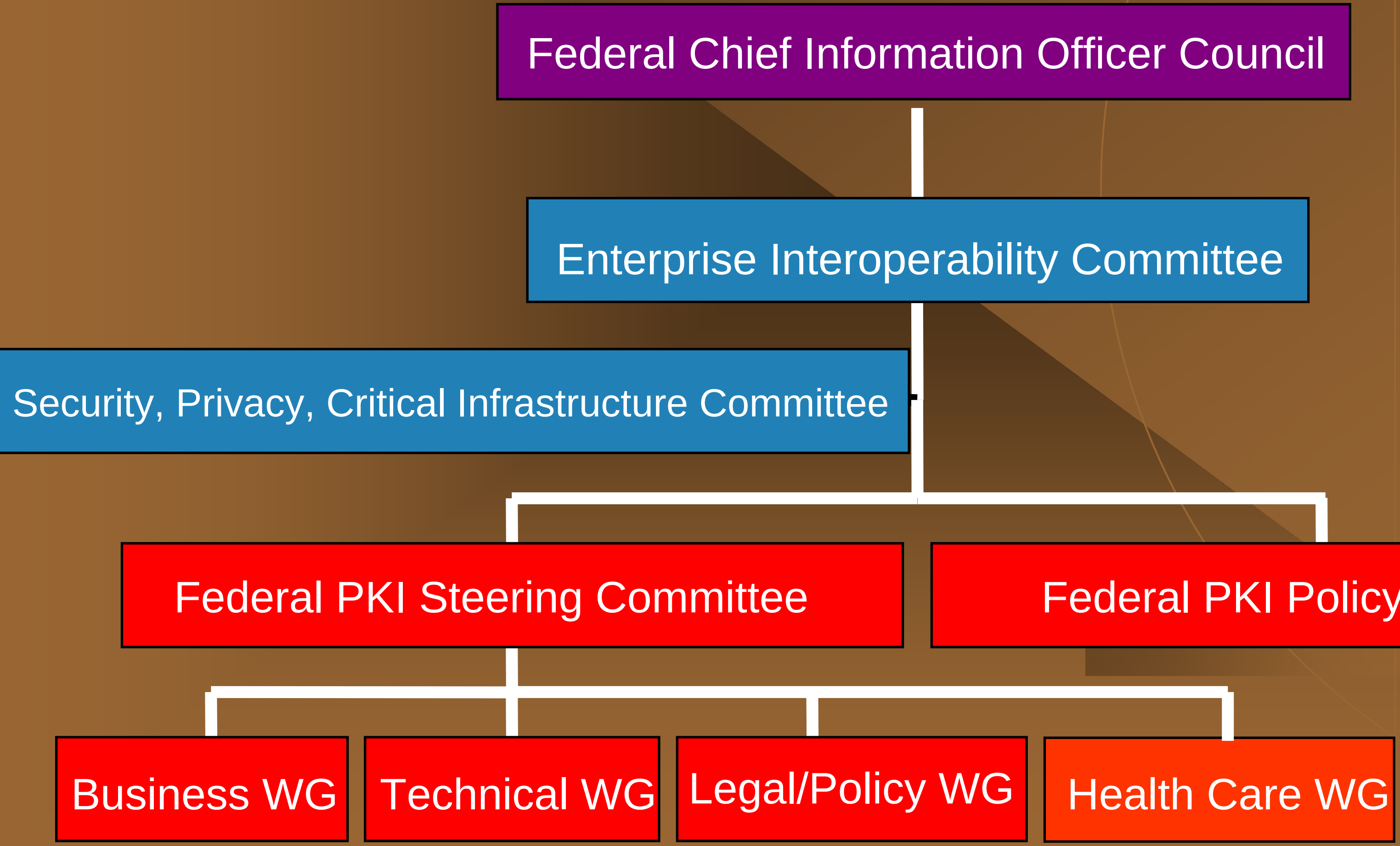
Goals

- A cross-governmental, ubiquitous, interoperable Public Key Infrastructure.
- The development and use of applications which employ that PKI in support of Agency business processes.

Mandates

- Long-term Cost Savings
- Trading Partner Practices
- Public Expectations
- International Competition
- Government Paperwork Elimination Act

Organization



Federal Chief Information Officer Council

Enterprise Interoperability Committee

Security, Privacy, Critical Infrastructure Committee

Federal PKI Steering Committee

Federal PKI Policy Authority

Business WG

Technical WG

Legal/Policy WG

Health Care WG

FPKISC Overview

- Sponsored by CIO Council, Enterprise Interoperability and Emerging Information Technologies Committee
- Provides guidance regarding all aspects of the Federal PKI
- Identifies and resolves Federal PKI technical and business issues
- Recommends solutions to policy and interoperability issues.
- Establishes and maintains liaison with other organizations interested in PKI activities.

Federal Approach

- Develop agency PKIs from the bottom up
- Establish the Federal PKI Policy Authority
- Implement the Federal Bridge CA using COTS products
- Ensure directory compatibility
- Use ACES for transactions with the public

Federal PKI Policy Authority

- Voluntary interagency group - NOT “agency”
- Governing body for FBCA interoperability
- Oversees operation of FBCA, authorizes issuance of FBCA certificates
- Under Federal CIO Council
- Six Charter Members:
  - GSA, Justice, NIST, NSA, OMB, Treasury

FBCA Overview

- Designed for the purpose of creating trust paths between disparate PKI domains
- Employs a distributed NOT a hierarchical model
- Commercial products participate within the membrane of the Bridge
- Develops cross certificates within the membrane to bridge the gap between dissimilar products

FBCA Operation

- FPKISC oversees FBCA development and operations
  - Bridge Documentation
  - Enhancements
- FPKI Policy Authority determines participants and levels of cross- certification
  - Administers Certificate Policy
  - Enforces compliance by member organizations
- GSA named Operational Authority
  - Operates in accordance with Policy Authority and FPKISC direction

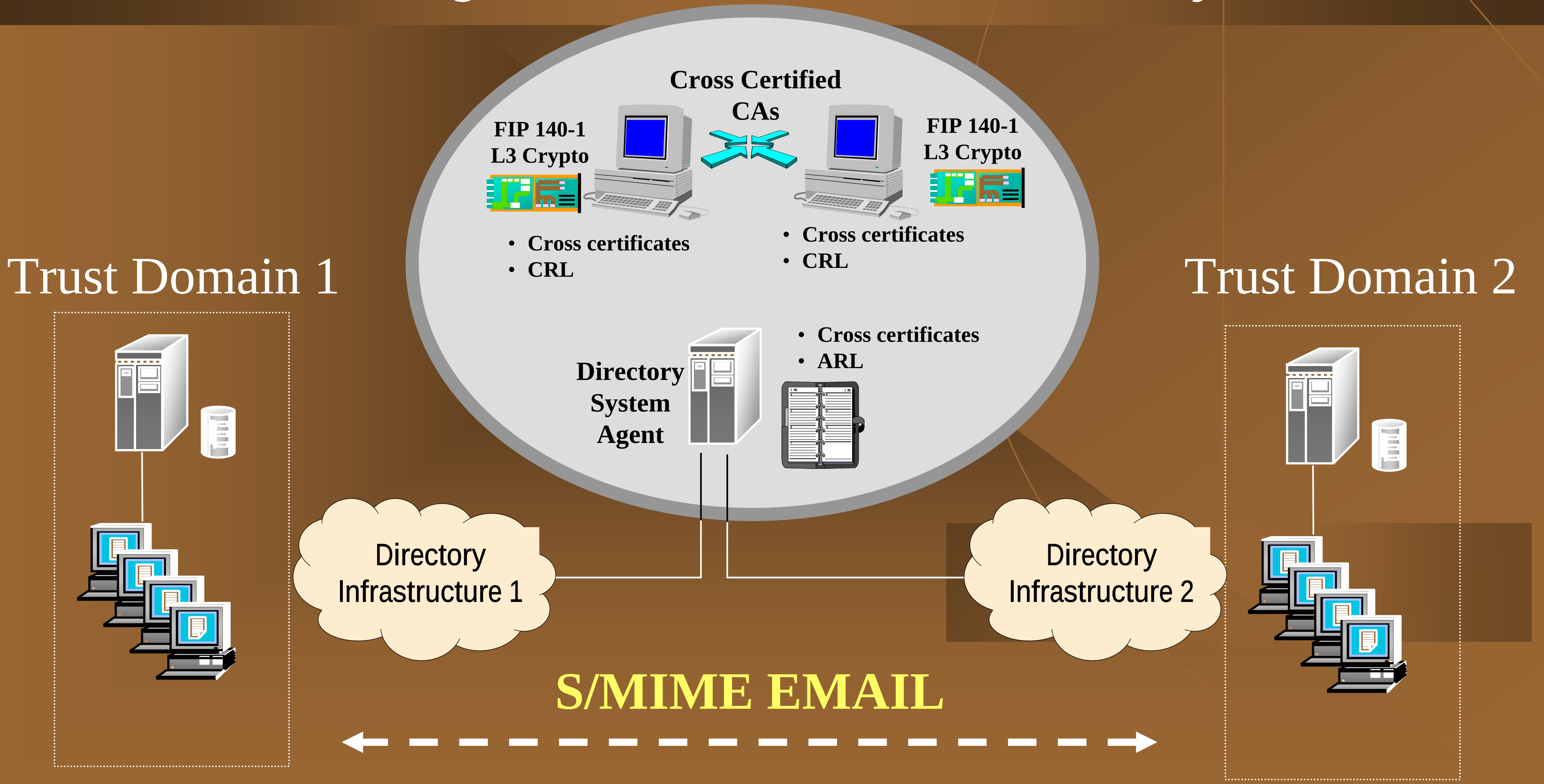
Current Bridge Status

- April 2000 - Successfully demonstrated Trust Path Creation during EMA Challenge, Boston, MA
- Two CA Products operational within the Membrane
  - Baltimore Technologies Unicert
  - Entrust/Authority
- Production bridge operational April 30, 2001

FBCA Organizational Lessons Learned

- Creation of Concept of Operations, Certificate Policy, Certificate Practices Statement is critical before deployment of PKI
- Documents are time-consuming to create, but not impossible
  - Who’s responsible for what?
- Policy Mapping for cross-certification can be technically challenging (an apparent oxymoron)
- Requires independent Audit – the bridge must be above suspicion
- The Policy Authority and the Steering Committee must be like Chang and Eng
- Never underestimate the significance of politics in Agencies and in the business sector

Federal Bridge Certification Authority



Technical Lessons Learned

- Bridge CAs can unite PKIs with
  - Different architectures
  - Different cryptographic algorithms
  - Different DITs
- Heterogeneous commercial products can be used inside the bridge
- Client software is the limiting factor
- X.500 chaining simplifies certificate retrieval
- Offline bridge architecture is secure but difficult to manage

Access Certificates for Electronic Services

- Provides the American Public secure electronic access to privacy related Federal Government information and services through the use of public key technology.
- Fosters cross-agency cooperation
- Uses the Certificate Arbitrator Module for processing PKI Certificates

Looking Forward

- Federal Bridge Certification Authority (FBCA)
- Policy Framework For Agency PKI Interoperability
- Key Industry Relationships And Technical Issues
- Federal And State Cooperation On PKI Initiatives
- International Liaison

And Then . . .

- A cross-governmental, interoperable, ubiquitous, Federal Public Key Infrastructure
- Federal Bridge interoperability with other Bridges
- International Cooperation and Interoperability