The Federal Bridge Certification Authority

Overview of Operations

Judith Spencer
Chair, Federal PKI Steering Committee
www.cio.gov/fpkisc

T he Problem

- There is no single Public Key Infrastructure
- U.S. does not license or accredit PKIs
- Discrete Trust Domains abound
- Different systems incorporate differing
  - Technical Solutions
  - Policy Decisions
- The Federal Government needs a mechanism for reliance on external Trust Domains.
- Interoperability is the CHALLENGE
  - Technical Interoperability
  - Policy Interoperability

Federal Public Key Infrastructure Steering Committee

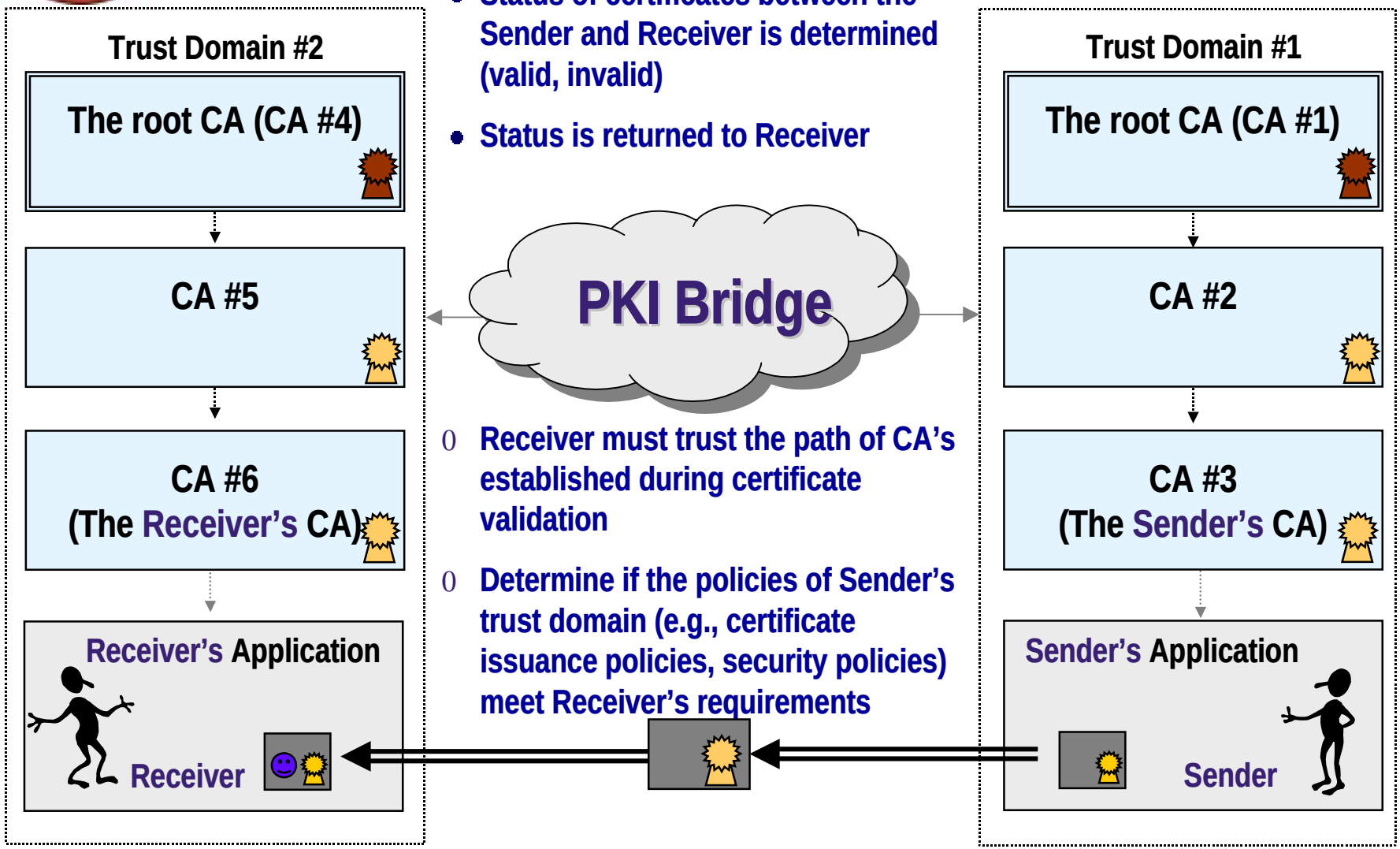
Bridging Trust Domains

- What is required technically to trust a certificate from one trust domain to another?
  - Cross-certificate is one valid representation of explicit trust between PKI domains
  - Must validate the certificate within sender's PKI domain
  - Might need to validate another certificate within your own PKI domain (i.e., your trust anchor)
  - Must be able to create a path between the two domains
- Components for interoperating with a bridge
  - Client application (for signing)
  - Relying party application (for validation)
  - Validation middleware
  - Certificate authority repositories (for certificate status)

Federal Public Key Infrastructure Steering Committee

Overview

- Status of certificates between the Sender and Receiver is determined (valid, invalid)
- Status is returned to Receiver



- Receiver must trust the path of CA's established during certificate validation
- Determine if the policies of Sender's trust domain (e.g., certificate issuance policies, security policies) meet Receiver's requirements

Cross-Certification

- Definition of a cross-certificate *

```
CertificatePair : : = SEQUENCE {
    issuedToThisCA      [0] Certificate OPTIONAL,
    issuedByThisCA      [1] Certificate OPTIONAL
    -- at least one of the pair shall be present
```

- Cross-certificates can define explicit trust levels of assurance equivalency through policy mappings

```
Object identifier       '2.16.840.1.101.3.2.1.3.1'
Object identifier       '2.16.840.1.101.3.2.1.3.4'
```

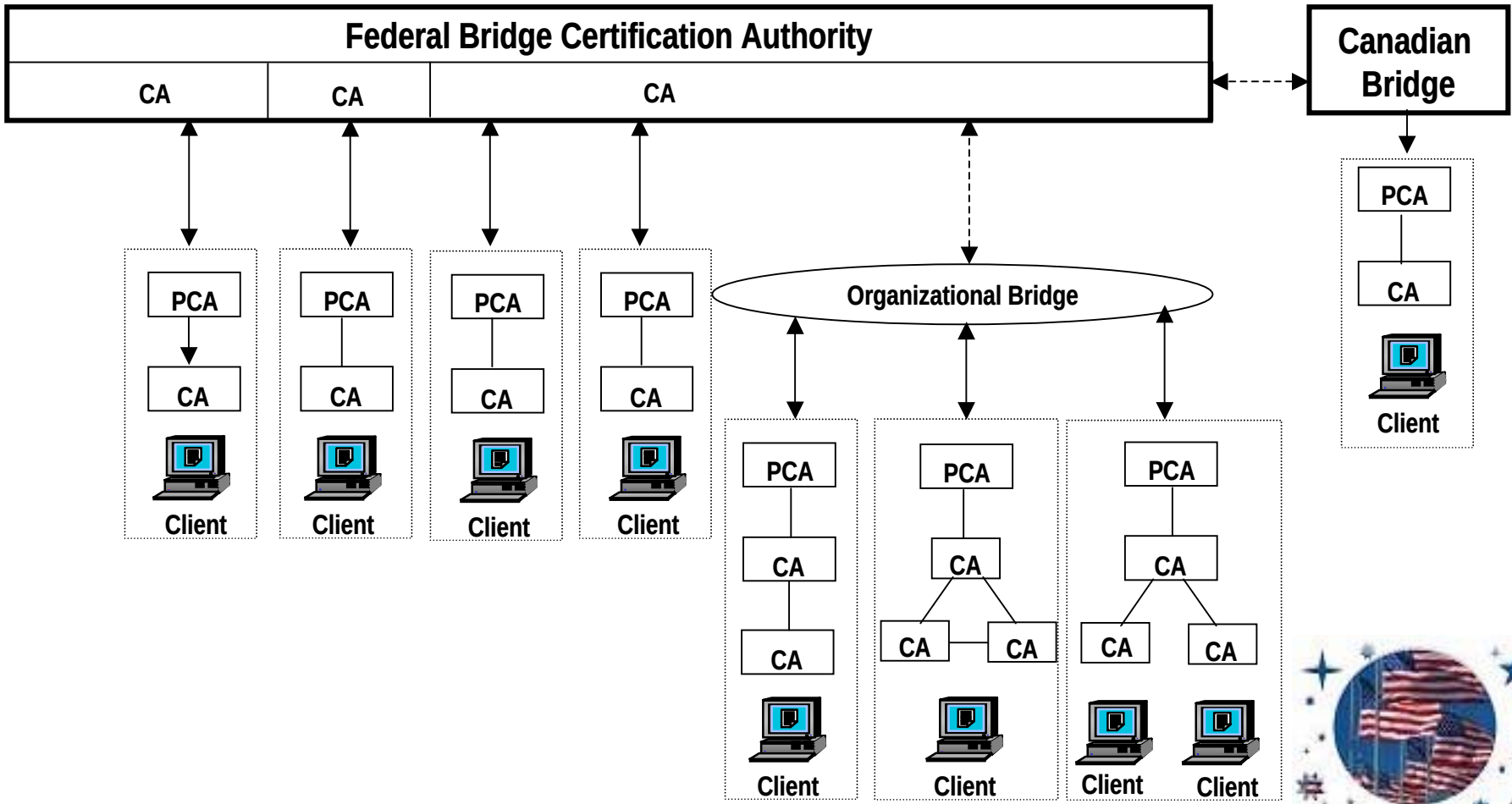
- Cross-certificates can manage transitive trust via name constraints extension

```
permittedSubtrees 'dc=gov, dc=gsa…'
excludedSubtrees  'dc=cuba, …'
```

*** X.509 4th Edition, Draft v7, Section 11.2.3**

Federal Public Key Infrastructure Steering Committee

Cross-Certification: An Example



Federal Public Key Infrastructure Steering Committee

Directory Interoperability

- Directory interoperability is required to complete certificate path validation
- Directories differ in structure and protocols supported
  - X.500 directory systems and
  - Other various product databases
- Support for one or several protocols is required
  - Directory Access Protocol (DAP)
  - Lightweight Directory Access Protocol (LDAP)
  - Directory Service Protocol (DSP)
  - On-line Certificate Status Protocol (OCSP)
  - Simple Certificate Validation Protocol (SCVP)
- Challenge is to traverse heterogeneous directory systems and protocols to complete validation

Validation Models

- Client-based validation (desktop application)
  - Determination of trusted domains managed locally at the desktop
  - “Discovers” certificate validation path across bridges and domains
  - Retrieves status information for certificates in validation path
  - Processes information and determines status
- Server-based validation
  - Determination of trusted domains managed at the server and/or desktop
  - “Thin” client forwards request for validation to a local server or enterprise validation application
  - Path discovery, status retrieval, and processing of performed by the server
  - Status returned to the desktop
- Service-based validation

Validation Methods and Protocols

- Validation can be completed through a combination of models
- All validation models need to support multiple protocols
- Method and protocol for validation of a certificate is determined by information contained within the certificate
  - Each certificate (CA, cross-certificate, and end-entity certificate) contains information within the AIA, CDP, and/or other extensions defining protocol and location of CRL or status for that certificate
- Full path discovery and validation could involve several different directory systems and access protocols

Federal Public Key Infrastructure Steering Committee

Two Phase Approach to Interoperability

Policy:

- **Mapping**
- **Annual Audits**
- **Organizational Membership**

Technical:

- **Testing Interoperability in the Lab**
- **Cross-Certification**
- **Directory Interoperability**

Federal PKI Policy Authority

FBCA Operational Authority

Federal Public Key Infrastructure Steering Committee

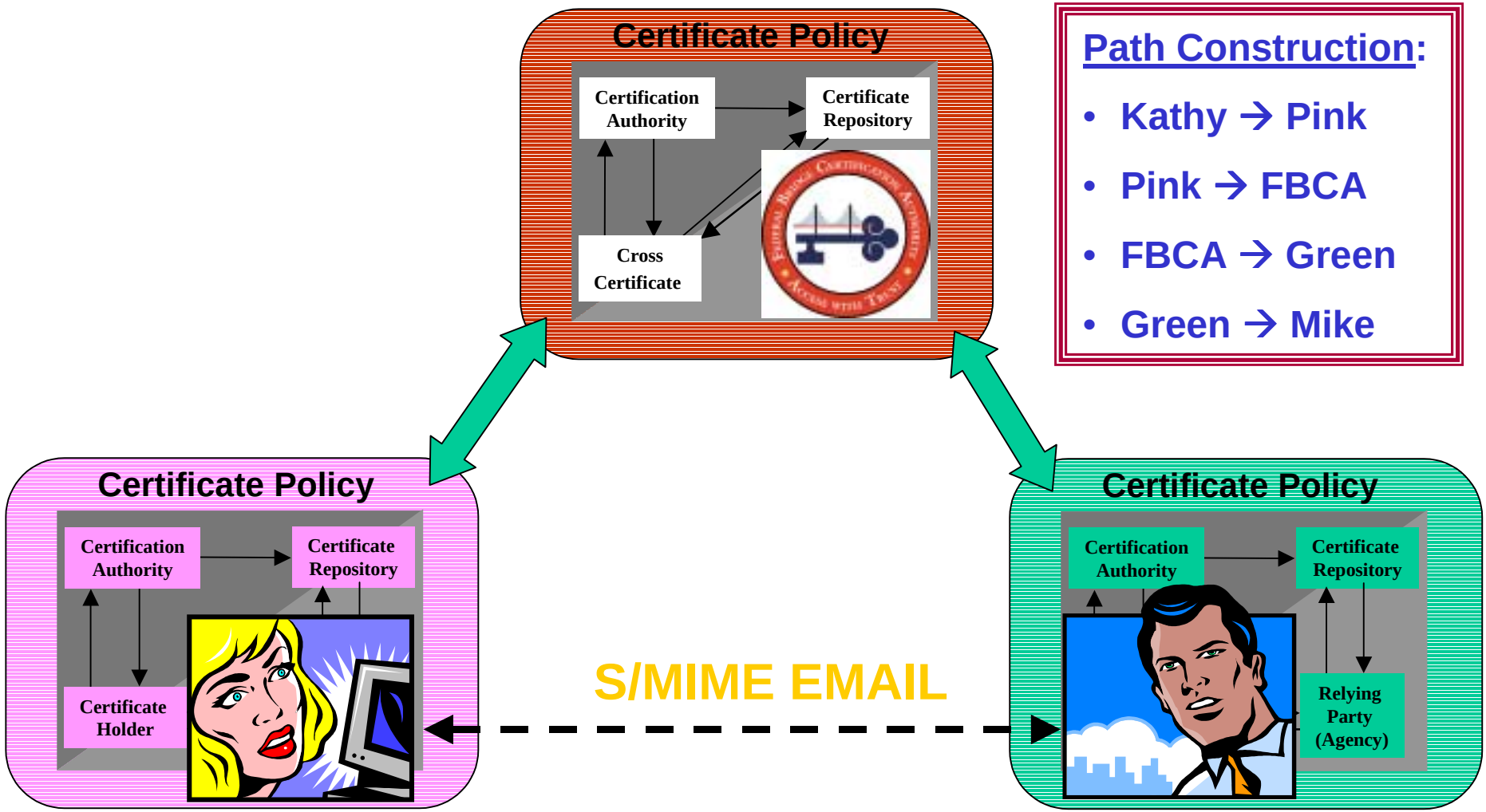
Cross-Certified Organizations

September 18, 2002

- National Aeronautics and Space Administration
- USDA/National Finance Center
- US Department of Treasury
- Department of Defense

Federal Public Key Infrastructure Steering Committee

Federal Bridge Certification Authority



Path Construction:

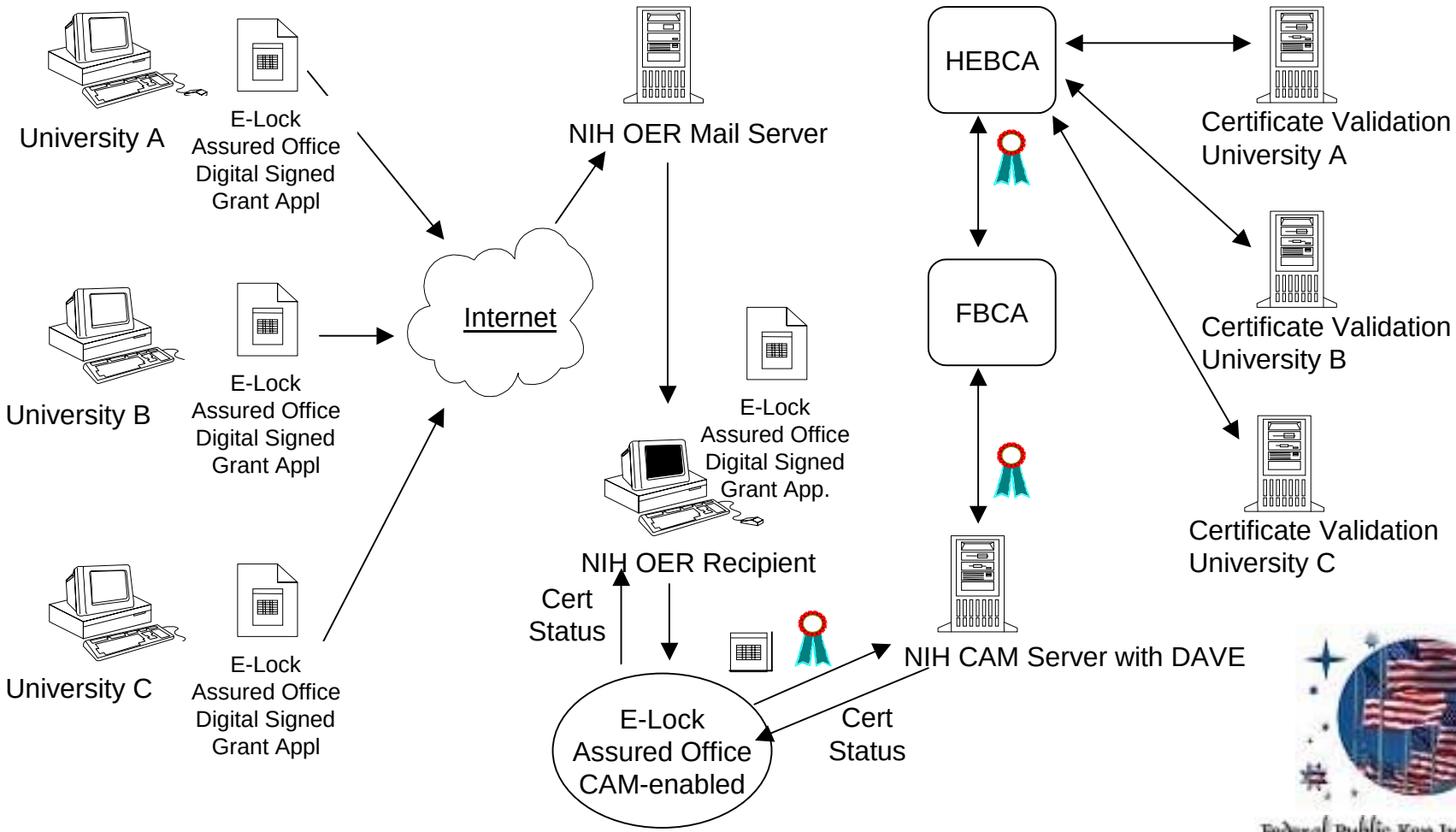
- Kathy → Pink
- Pink → FBCA
- FBCA → Green
- Green → Mike

Organizations in the Queue

- Department of State
- Department of Labor
- State of Illinois
- Government of Canada
- Higher Education
- Access Certificates for Electronic Services
- Aerospace Industry

Federal Public Key Infrastructure Steering Committee

Bridge-to-Bridge



Federal Public Key Infrastructure Steering Committee

Outreach to the Public

- DEA – Physicians and Drug Distributors for movement of controlled substances
- US Patent and Trademark Office – Patent Attorneys
- Federal Emergency Management Agency – Emergency Response Personnel
- Environmental Protection Agency – Environmental Hazard Reporting
- Veteran's Affairs – Veteran's Benefits and Health Programs
- Department of Labor – Students, Labor Union Management
- National Institutes of Health – Colleges and Universities

Federal Public Key Infrastructure Steering Committee

E-Authentication

An E-Gov Initiative

The New E-Gov Initiatives

Vision:

An order of magnitude improvement in the federal government's value to the citizen.

Definition:

The use of digital technologies to transform government operations in order to improve effectiveness, efficiency, and service delivery.

Principles:

Market-based, Results-oriented, Citizen-centered

Simplify and Unify

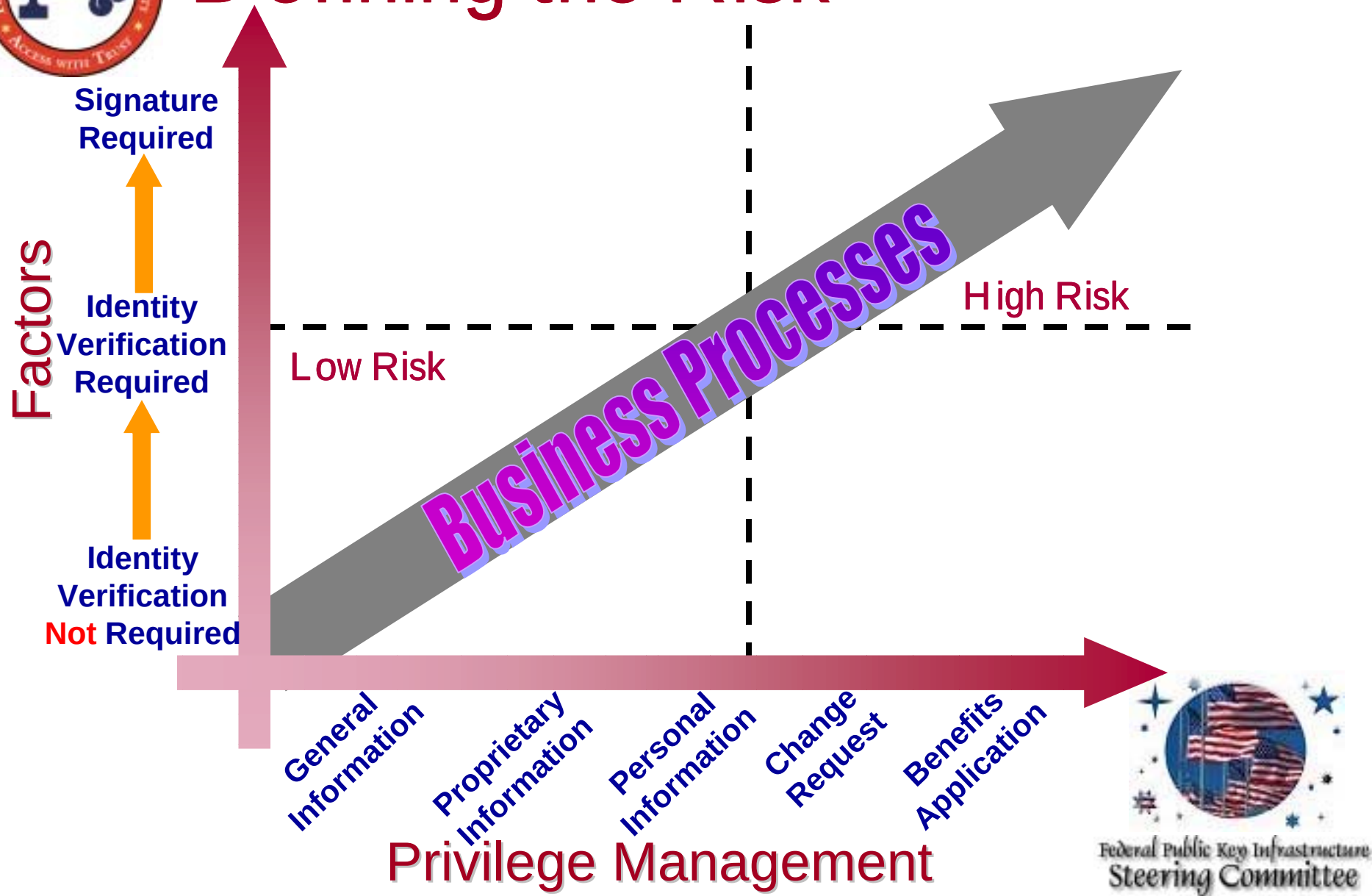
E-Authentication

Three Focus Areas:

- Agency Application Risk Analysis (OCTAVE)
  - Modified for E-Authentication Needs (ERA)
  - Focused on Identity Assurance at the Transaction Level
- Authentication Guidance
  - Privacy Policy
  - OMB Guidance on relating Risk to Levels of Assurance
  - NIST Guidance on Technical Criteria for Electronic Credential Providers
- Authentication Gateway

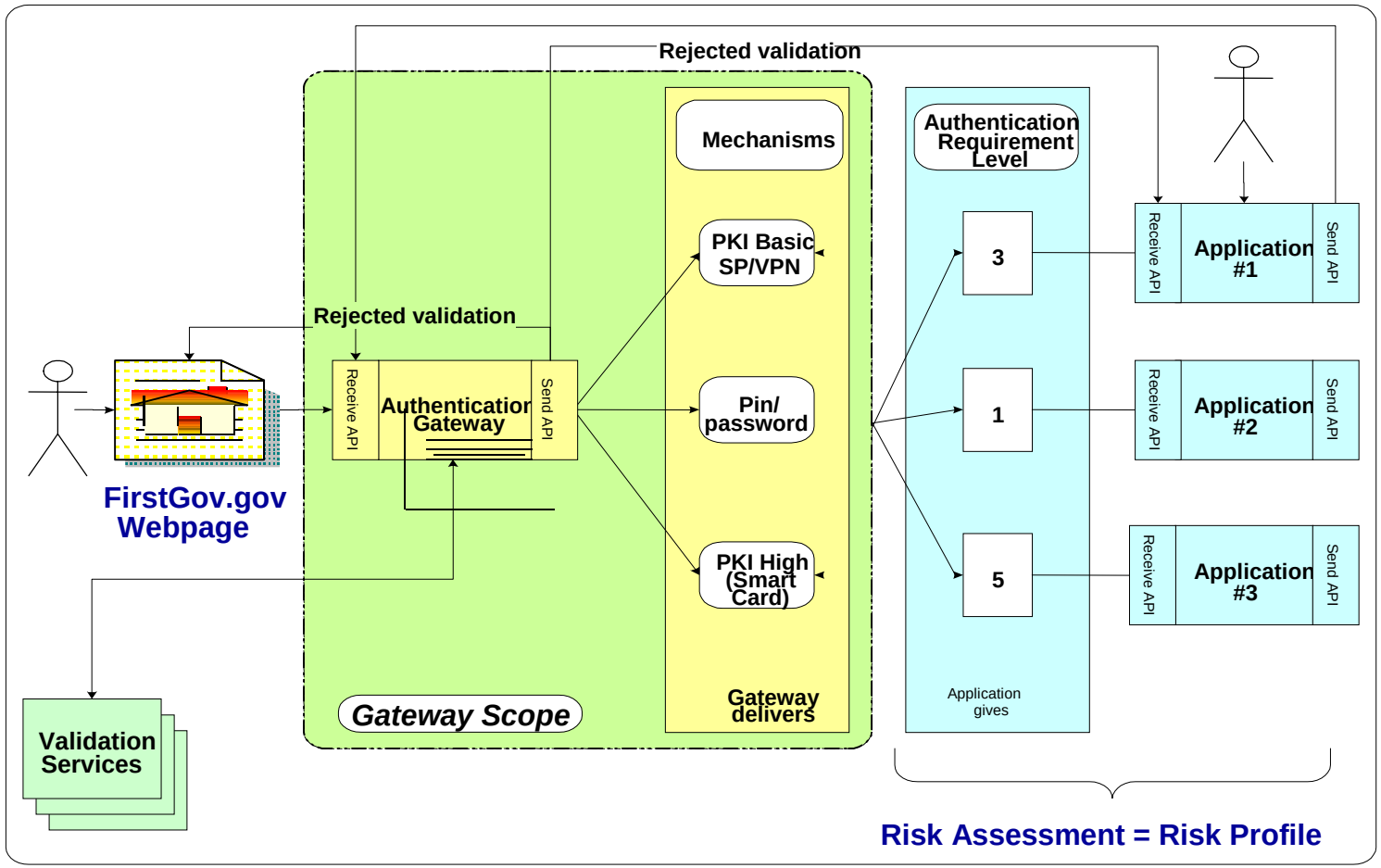
Federal Public Key Infrastructure Steering Committee

Defining the Risk



Federal Public Key Infrastructure Steering Committee

E-Authentication Gateway



Federal Public Key Infrastructure Steering Committee

E-Gov Initiatives

Government to Citizen

	Managing Partner
1. USA Service	GSA
2. EZ Tax Filing	Treasury
3. Online Access for Loans	DoEd
4. Recreation One Stop	DOI
5. Eligibility Assistance Online	Labor

Government to Business

	Managing Partner
1. Federal Asset Sales	GSA
2. Online Rulemaking Management	DOT
3. Simplified and Unified Tax and Wage Reporting	Treasury
4. Consolidated Health Informatics (business case)	HHS
5. Business Compliance 1 Stop	SBA
6. Int'l Trade Process Streamlining	DOC

Cross-cutting Barrier: e-Authentication GSA, Enterprise Architecture OMB

Government to Govt.

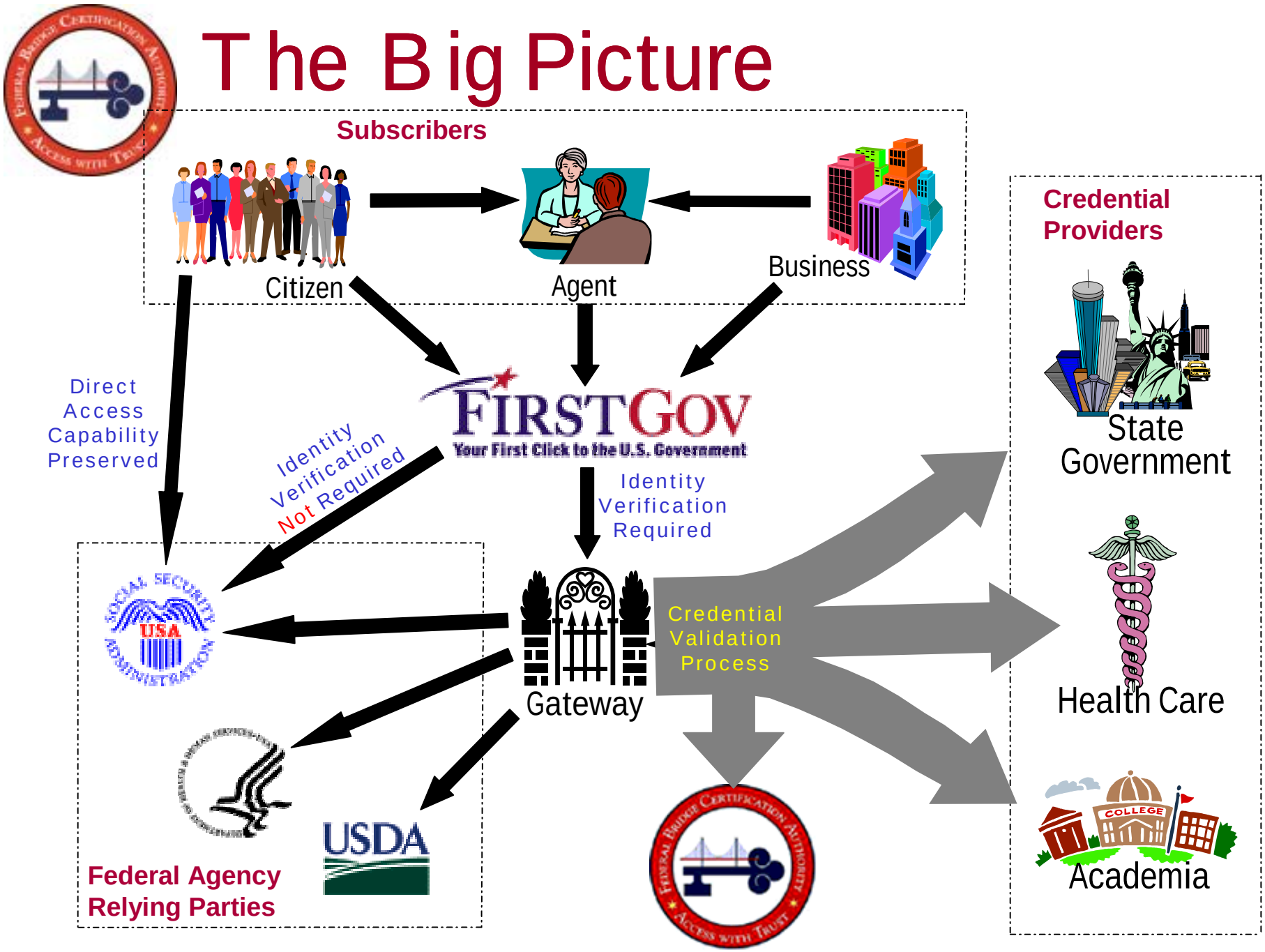
1. e-Vital (business case)	SSA
2. e-Grants	HHS
3. Disaster Assistance and Crisis Response	FEMA
4. Geo-spatial Information One Stop	DOI
5. Wireless Networks	Treasury

Internal Effectiveness and Efficiency

1. e-Training	OPM
2. Recruitment One Stop	OPM
3. Enterprise HR Integration	OPM
4. e-Travel	GSA
5. e-Clearance	OPM
6. e-Payroll	OPM
7. Integrated Acquisition	GSA
8. e-Records Management	NARA

Federal Public Key Infrastructure Steering Committee

The Big Picture



Learn more. . .

Visit our Websites

www.cio.gov/fpkisc

www.cio.gov/fpkipa

www.cio.gov/fbca

www.cio.gov/eauthentication

Federal Public Key Infrastructure Steering Committee