E-Authentication Initiative: Identity Federation for the Federal Government

David Temoshok
Director, Identity Policy and Management
GSA Office of Governmentwide Policy

Liberty Alliance e-Health SIG Workshop
April 26, 2006

Prioritize E-Government

- **President's Management Agenda**:
  1. Strategic Management of Human Capital
  2. Competitive Sourcing
  3. Improved Financial performance
  4. **Expanded Electronic Government**
  5. Budget and Performance Integration
- **E-Government Act of 2002**
- **OMB Office of E-Government and Technology**

Authentication
SECURE GOVERNMENT ACCESS | ONLINE

President's E-Gov Agenda

Government to Citizen	Lead
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	Lead
1. Federal Asset Sales	GSA
2. Online Rulemaking Management	EPA
3. Simplified and Unified Tax and Wage Reporting	Treasury
4. Consolidated Health Informatics	HHS
5. Business Gateway	SBA
6. Int'l Trade Process Streamlining	DOC

Cross-cutting Infrastructure: E-Authentication GSA

Government to Govt.	Lead
1. e-Vital (business case)	SSA
2. Grants.gov	HHS
3. Disaster Assistance and Crisis Response	FEMA
4. Geospatial Information One Stop	DOI
5. Wireless Networks	FEMA

Internal Effectiveness and Efficiency	Lead
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

E-Authentication Key Policy Considerations

- **For Government-wide deployment**:
  - No National ID
  - No National unique identifier
  - No central registry of personal information, attributes, or authorization privileges
  - Different authentication assurance levels are needed for different types of transactions
  - Authentication **–** not authorization
- **For E-Authentication technical approach**:
  - No single proprietary solution
  - Deploy multiple COTS products **–** user's choice
  - Products must interoperate together
  - Controls must protect privacy of personal information

Four Identity Assurance Levels

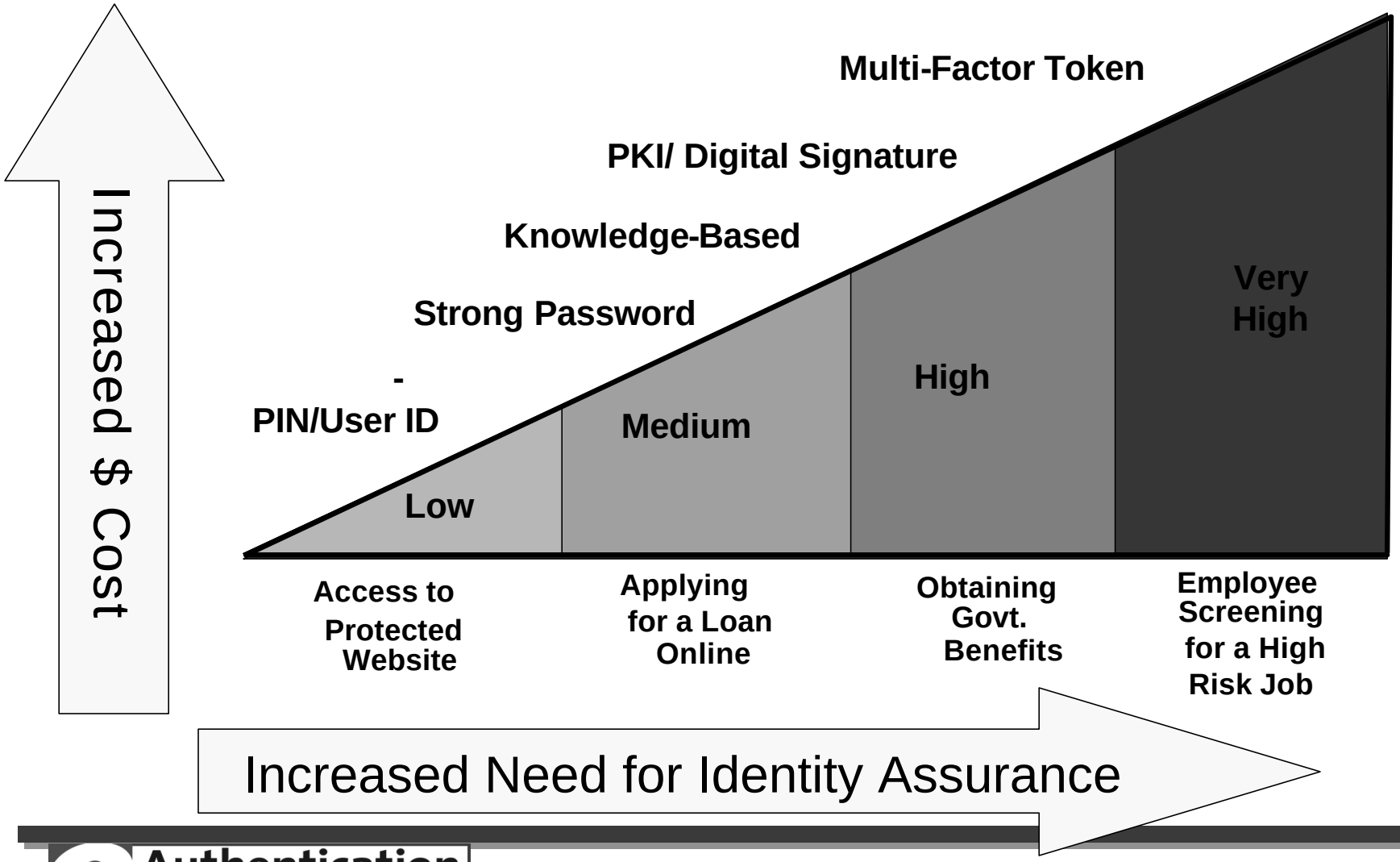
OMB E-Authentication Guidance establishes four assurance levels for consistent application of E-Authentication across gov't

Level 1	Level 2	Level 3	Level 4
Little or no confidence in asserted identity (e.g. self identified user/password)	Some confidence in asserted identity (e.g. PIN/Password)	High confidence in asserted identity (e.g. digital cert)	Very high confidence in the asserted identity (e.g. Smart Card)

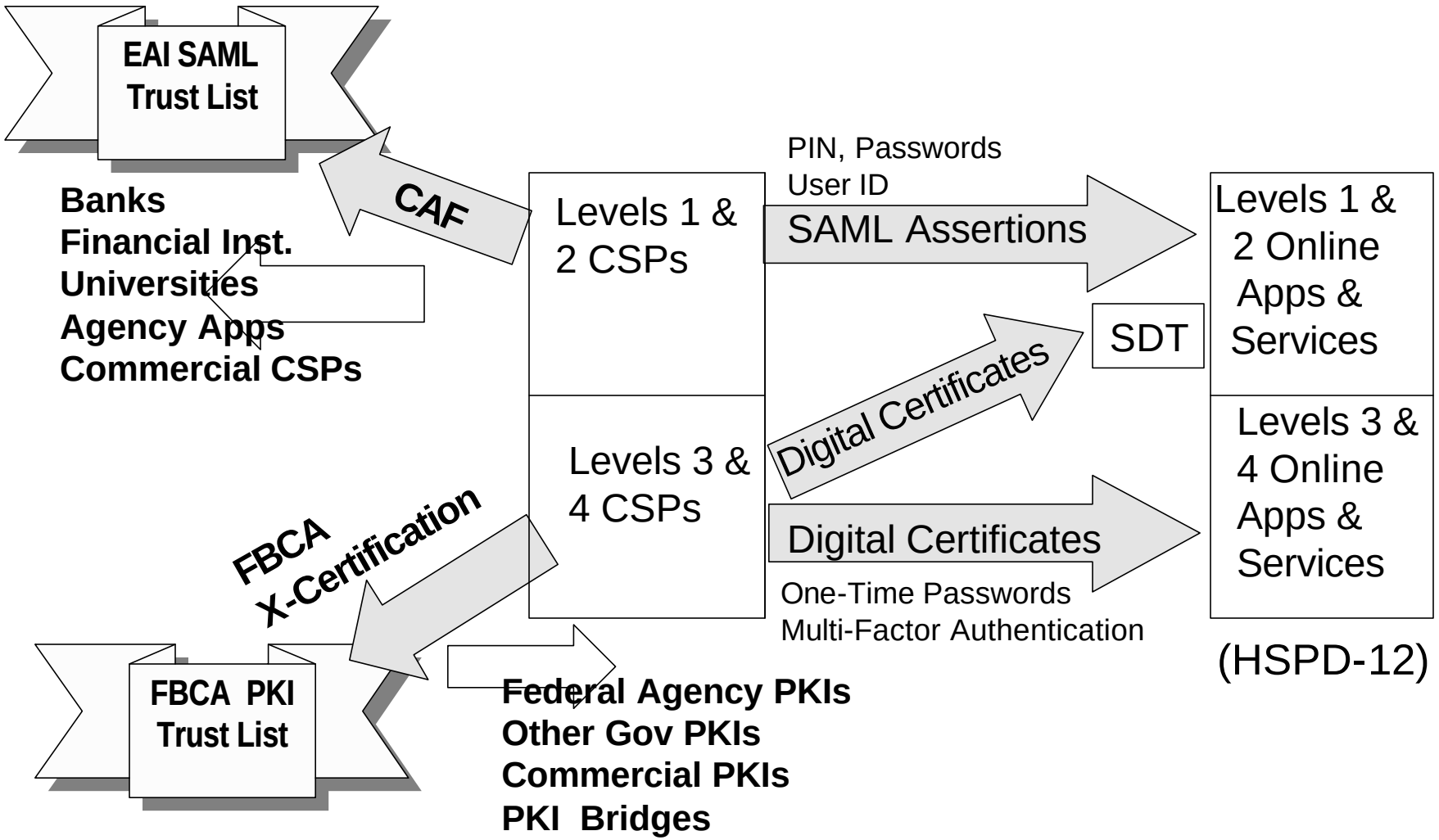
E-RA tool assists agencies in defining authentication requirements & mapping them to the appropriate assurance level

NIST SP800-63 Electronic Authentication technical guidance matches technology to each assurance level

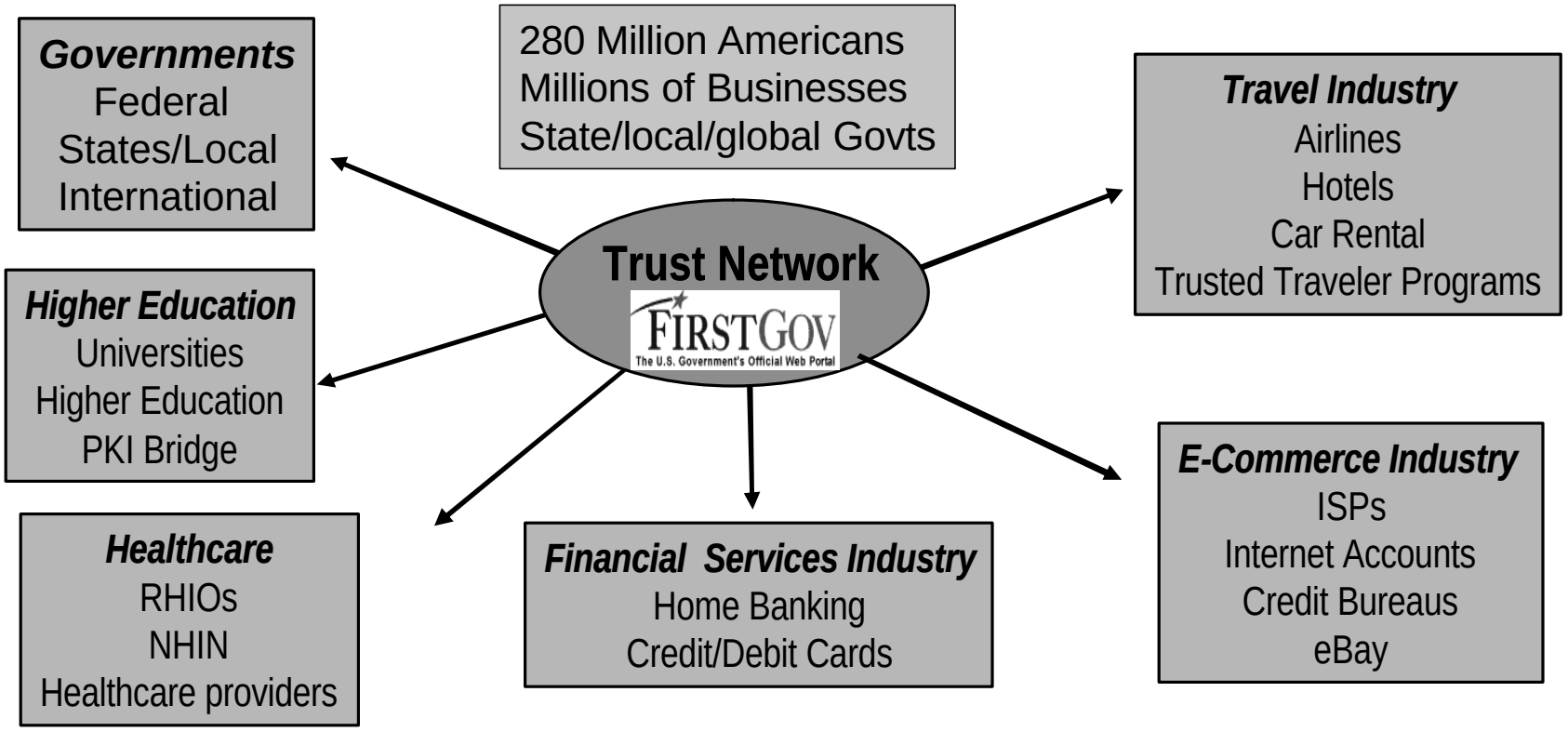
Four Authentication Assurance Levels to meet multiple risk levels -



A VERY Simplified View of the Federal EAI Architecture

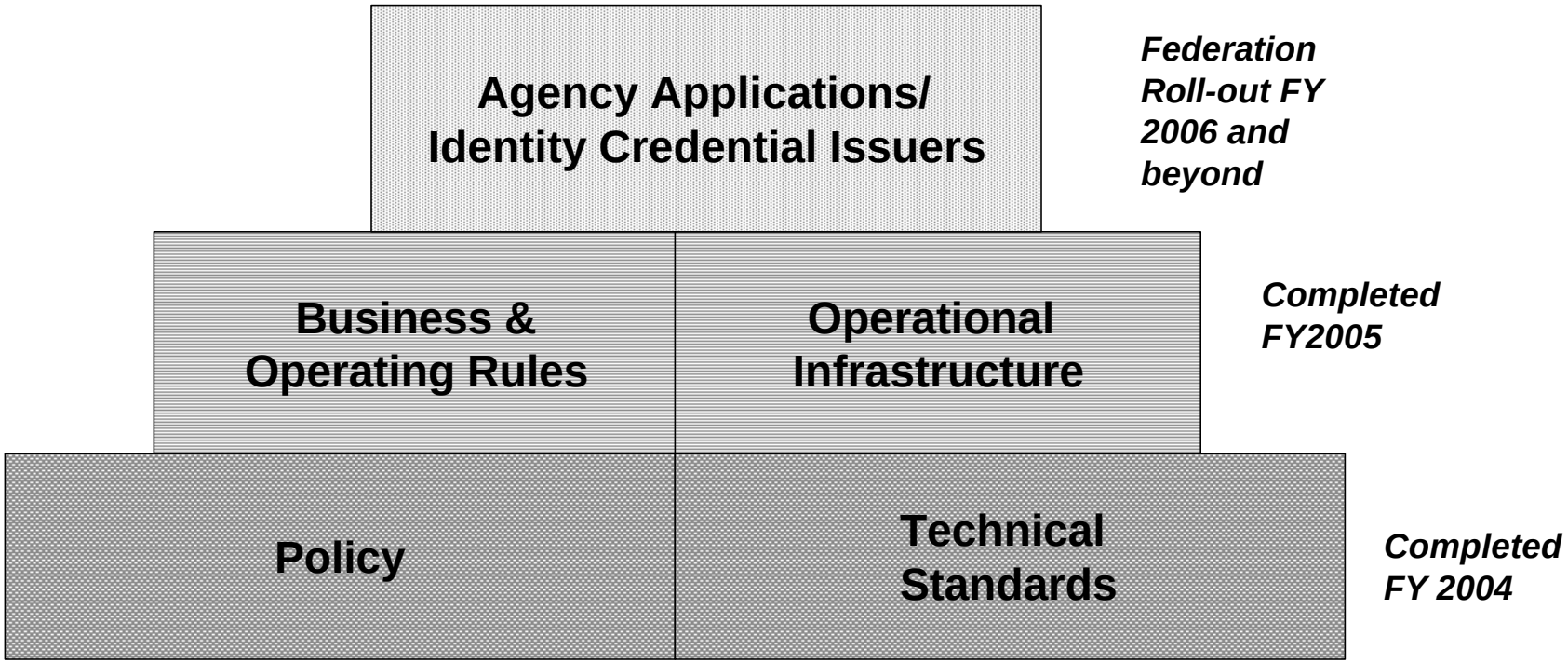


Central Issue with Federated Identity – Who do you Trust?



Absent a National ID and unique National Identifier, the e-Authentication initiative will establish trusted credentials/providers at determined assurance levels.

Building the E-Authentication Federation



Federation Infrastructure

- Interoperable Technology (Communications)
  - ✓ Determine intra-Federation communication architecture
  - ✓ Administer common interface specifications, use cases, profiles
  - ✓ Conduct interoperability testing (as needed) according to the specifications
  - ✓ Provide a common portal service (I.e., discovery and interaction services)
- Trust
  - ✓ Establish common trust model
  - ✓ Administer common identity management/authentication policies for Federation members
- Business Relationships
  - ✓ Establish and administer common business rules
  - ✓ Manage relations among relying parties and CSPs
  - ✓ Manage compliance/dispute resolution

Government Adoption of Federated IDM

- Necessary in order to meet President's E-Gov mandates
  - GSA is directed to provide common authentication infrastructure for all Federal E-Gov business applications and E-access control.
- In 2004 GSA established the EAI Federation
  - EAI Federation allows identity federation between multiple industry and government entities and the Federal Government
  - Technical architecture supports multiple authentication technologies, protocols, and IDM software products and components
- In 2004 GSA partnered with industry to establish the Electronic Authentication Partnership
  - Incorporated non-profit public/private sector forum to advance and accelerate IDM federation
  - Focuses on interoperability and trust
  - EAP Trust Framework issued 12/04

Federal Trust Model for Federated Identity

1. Establish & define authentication risk and assurance levels

- **OMB M-04-04 -** ***Established and defined 4 authentication assurance levels as Governmentwide policy***
- **FBCA Certificate Policy -** ***Established 4 authentication assurance levels for Federal PKI domains***

2. Establish technical standards & requirements for e-Authentication systems at each assurance level

- **NIST Special Pub 800-63 Recommendation for E-Authentication –** ***Established authentication process & technical standards at 4 established assurance levels***
- **FBCA Common, Commerce Certificate Policies –** ***Established PKI-specific standards and requirements.***

3. Establish methodology for evaluating authentication systems at each assurance level

- **Credential Assessment Framework –** ***Standard methodology for assessing authentication systems of credential service providers.***
- **FBCA Cross-Certification Requirements –** ***Standard methodology for policy mapping, audit, and testing interoperability for cross-certification with the FBCA.***

5. Perform assessments and maintain trust list of trusted CSPs

- **E-Authentication Trusted CSP List –** ***CAF, boarding & Interoperability testing***
- **FBCA Trust List --***tests for policy mapping,, audit compliance, cross-certification & directory interoperability*

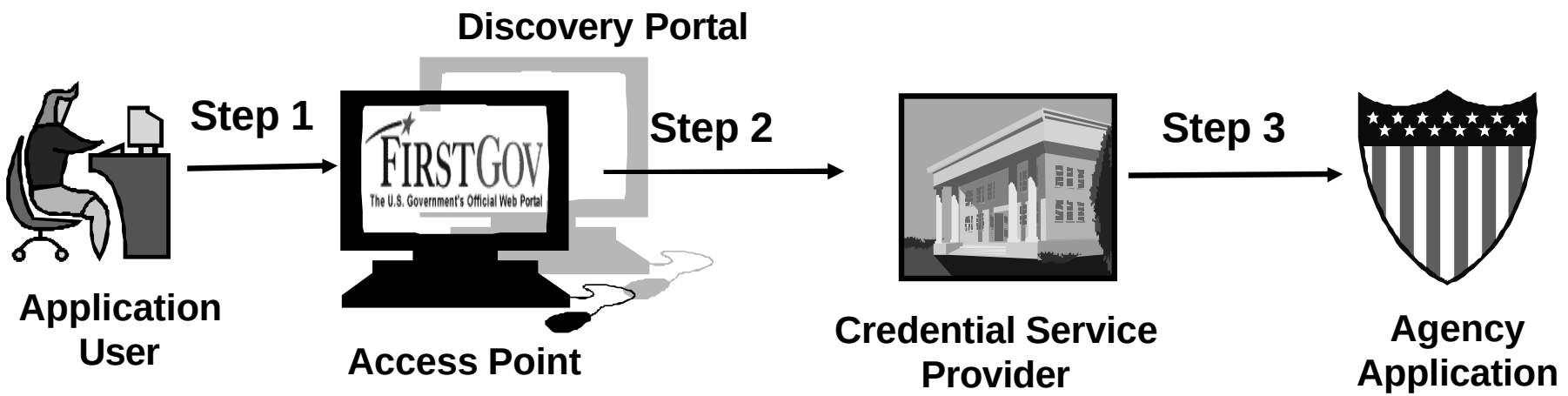
6. Establish common business and operating rules for participants

- **EAI Federation Business and Operating Rules and Participant Agreements**
- **MOA with Federal PKI Policy Authority**

Key Architecture Design Considerations

- No central registry of personal information, attributes, or authorization privileges – decentralized approach means federation.
- Different authentication assurance levels are needed for different types of transactions.
- Architecture must support multiple authentication technologies.
- Architecture must support multiple protocols.
- Federal Government will not mandate a single proprietary solution, therefore, Architecture must support multiple COTS products.
- Federal Government will adopt prevailing industry standards that best meet the Government's needs.
- All architecture components must interoperate with ALL other components.
- Controls must protect privacy of personal information.

The Federal E-Authentication Service



Step 1:

At access point (portal, agency Web site or credential service provider) user selects agency application and credential provider (Discovery Portal)

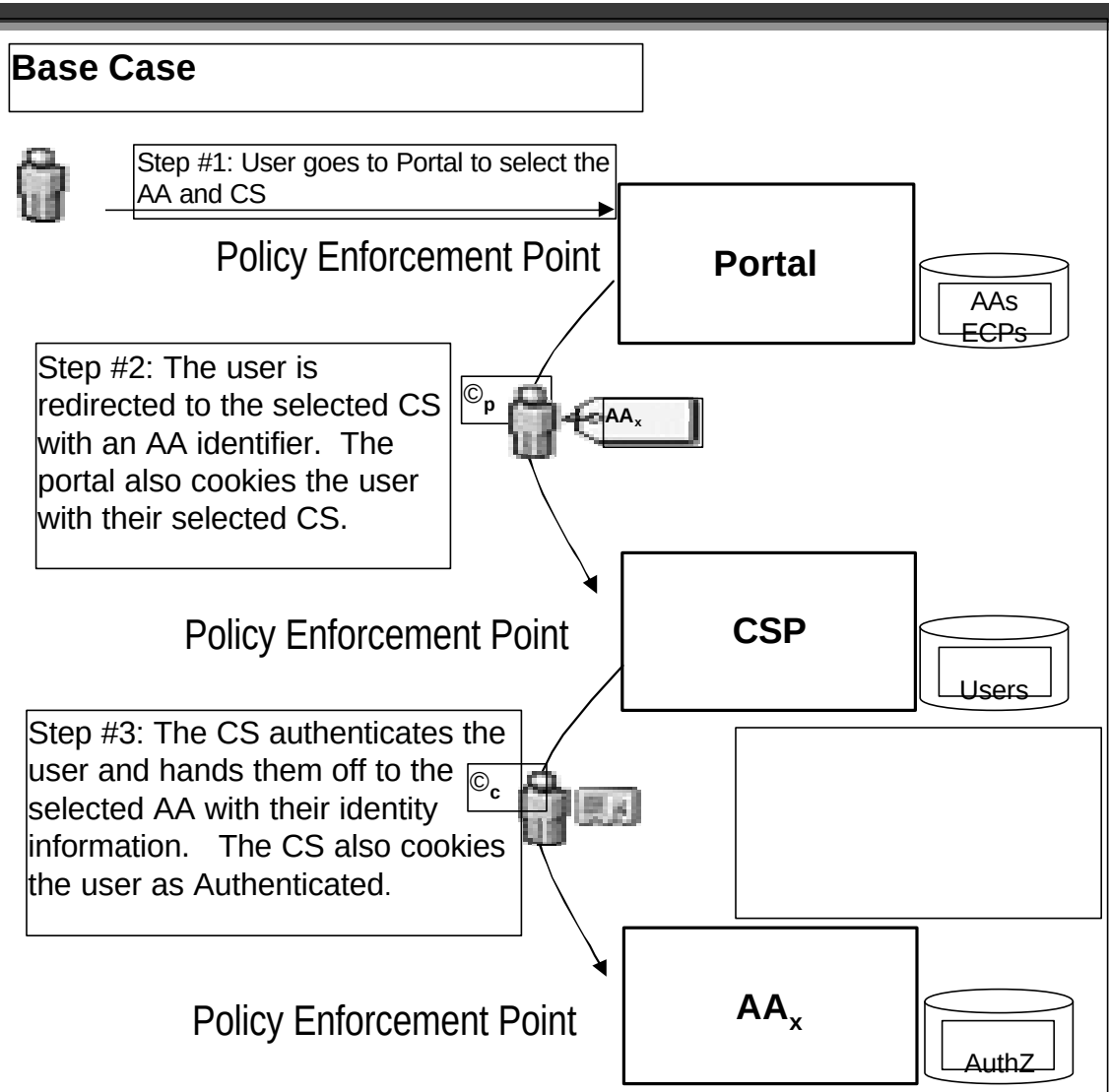
Step 2:

- **User is redirected to selected credential service provider**
- **If user already possesses credential, user authenticates**
- **If not, user acquires credential and then authenticates**

Step 3:

Credential service hands off authenticated user to the agency application user selected at the access point

e-Authentication Technical Interfaces – Base Case



Data/Information Flows

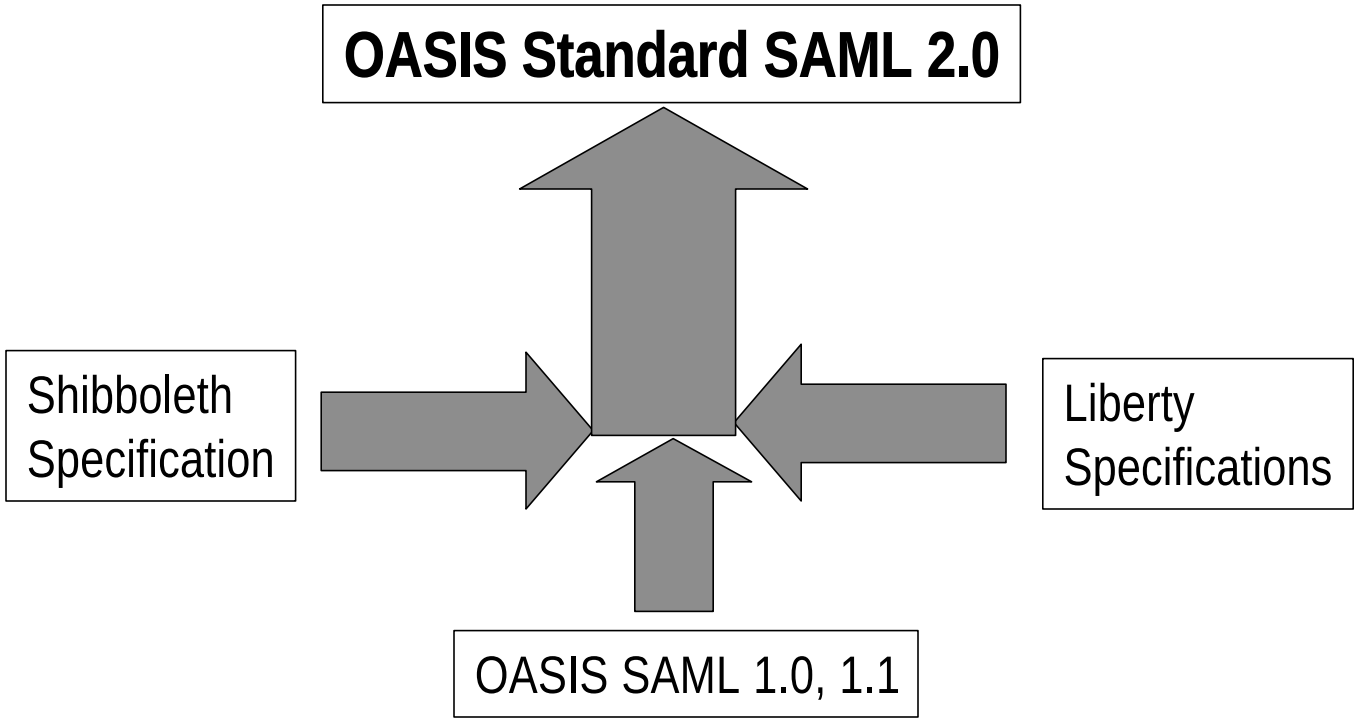
Step #1: No PII is presented to the portal, no transaction data is recorded, no system of records is maintained.

Step #2: For Federal CSPs, no new PII is created. Users simply sign on using previously established processes with CSP (PIN, Password). PIN, Passwords are expressed only to CSP, not to e-Auth Portal or AA.

Step #3: For Assurance levels 1 and 2, CSP will need to provide users' common name + assurance level (at a minimum) to the AA. Interface Spec 1.1 allows attribute data to be exchanged. PII is protected in transmission through SOAP/SSL.

Standards Convergence

- SAML 1.X - Framework for exchanging security information about a principal: authentication, attributes, authorization information
- Liberty ID-FF 1.X – Extend SAML 1.0, 1.1 for federation, SSO, web services



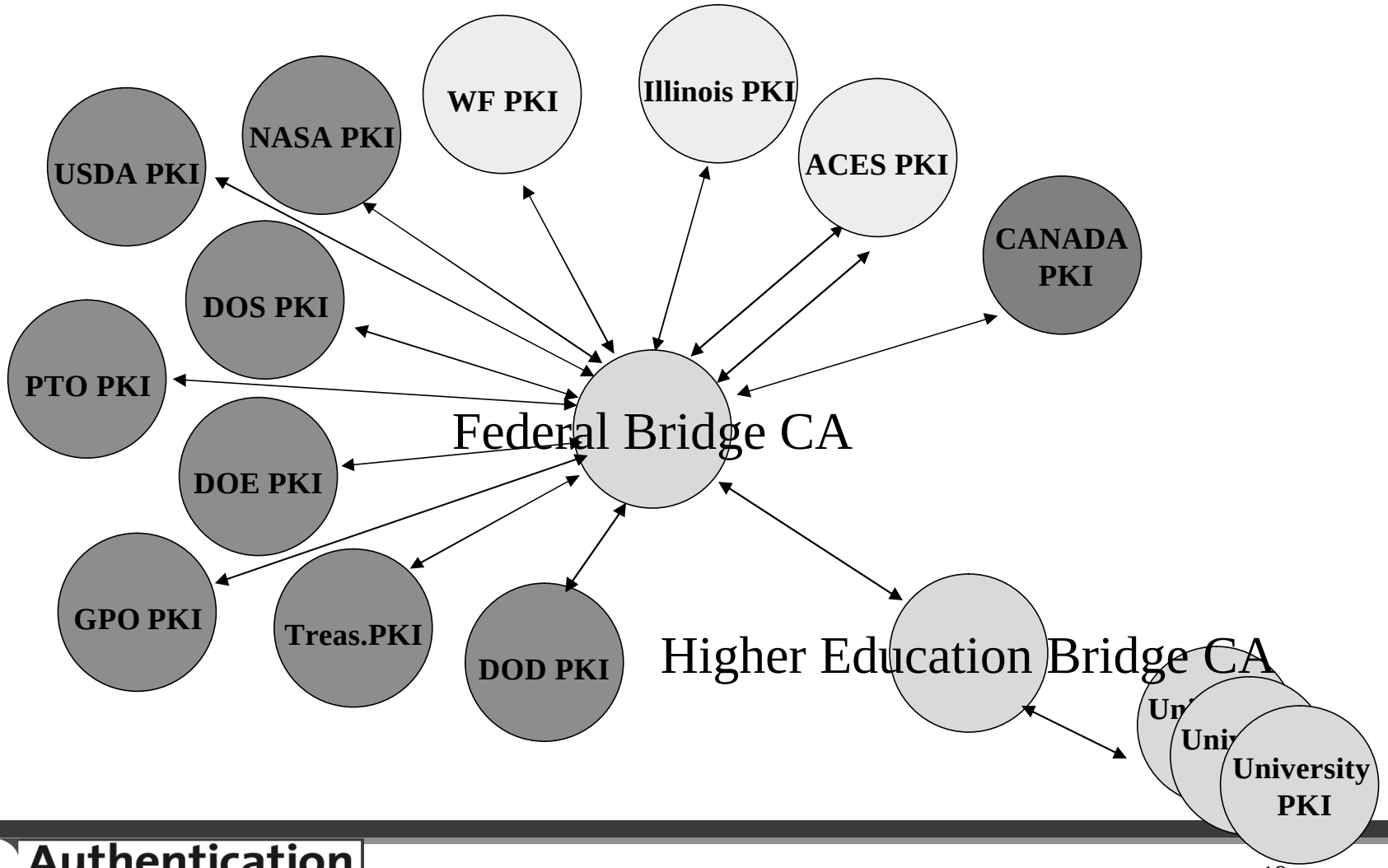
Federal Interoperability Lab

- **Tests interoperability of products for participation in e-Authentication architecture.**
  - ✓ Conformance testing to Fed e-Authentication Interface Specification
  - ✓ Interoperability testing among all approved products
- **Currently 11 SAML 1.0 products on Approved Product List.**
  - ✓ See URL: http://cio.gov/eauthentication
- **Multiple protocol interoperability testing will be very complex**
- **4 Products approved for PKI certificate path discovery & validation**
- **GSA intends to continue to test architecture components for interoperability and capability to meet governmentwide use requirements**

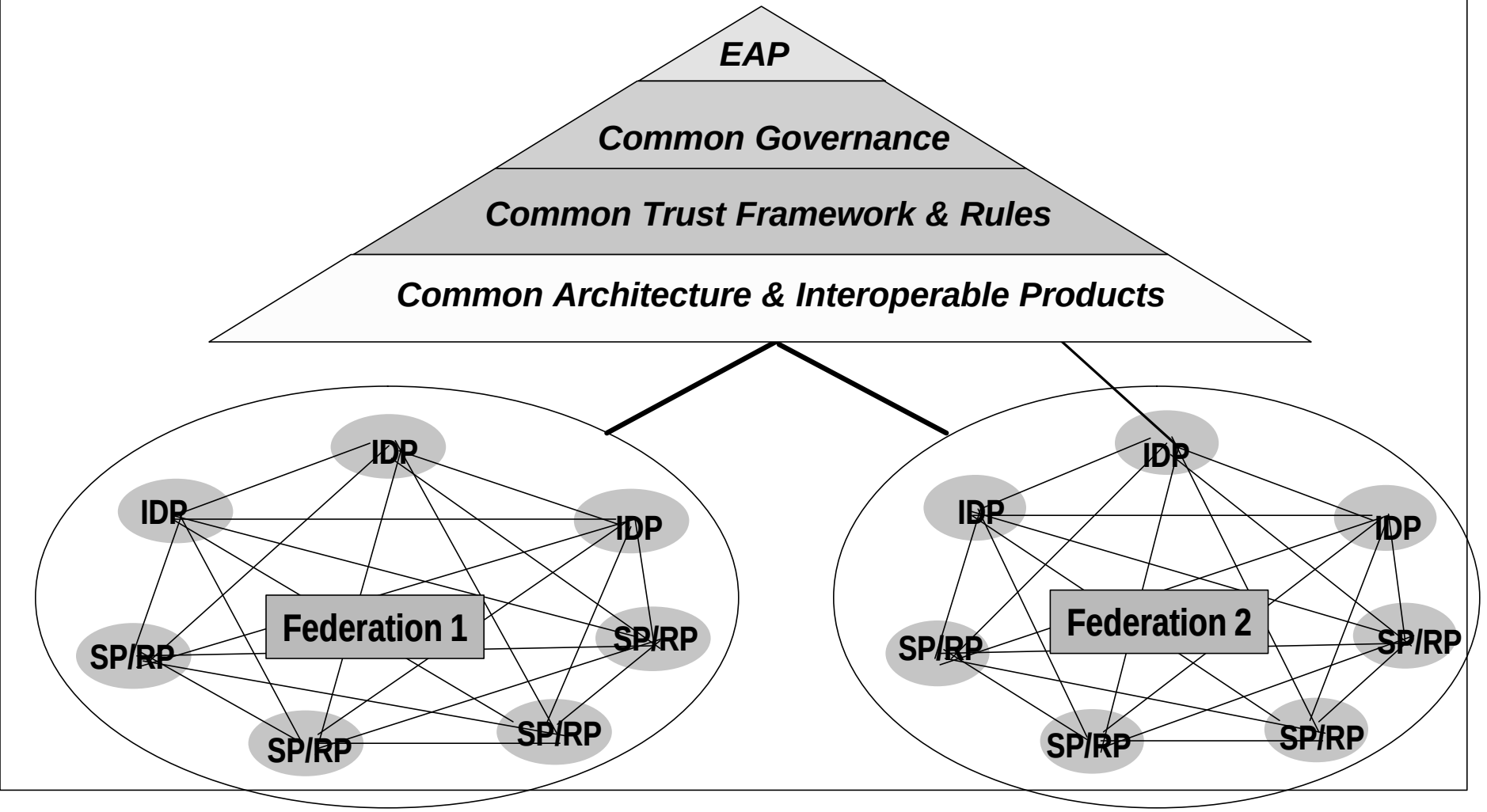
The Approach to a U.S. Federal PKI

- Allow Agencies to implement their own PKIs
- Create a Federal Bridge CA using COTS products to bind Agency PKIs together
- Establish a Federal PKI Policy Authority to oversee policy and operation of the Federal Bridge CA
- Ensure directory compatibility
- Use ACES for transactions with the public
- Use PKI Shared Service Providers for internal Federal Government provisioning
- Approve commercial products for certificate validation (local, hosted)

A Snapshot of the U.S. Federal PKI



EAP Vision:
Multiple, Interoperable Federations



For More Information

- Visit our Websites:
  - http://www.cio.gov/eauthentication
  - http://www.cio.gov/ficc
  - http://www.cio.gov/fbca
  - http://www.cio.gov/fpkipa
  - http://csrc.nist.gov/piv-project/
  - http://www.cio.gov/fpkisc
  - http://www.eapartnership.org
  - http://www.smart.gov/
- Or contact:

David Temoshok
Director, Identity Policy and Management
202-208-7655
david.temoshok@gsa.gov