

Federal Identity Credentialing



PMC E-Gov Agenda

Government to Citizen

1. USA Service
2. EZ Tax Filing
3. Online Access for Loans
4. Recreation One Stop
5. Eligibility Assistance Online

Government to Business

1. Federal Asset Sales
2. Online Rulemaking
3. Management
4. Integrated and Unified
5. Wage Reporting
6. Health
7. (business case)
8. Stop
9. ing

Managing Partner

GSA
EPA

Treasury

HHS

SBA
DOC

Cross-cutting Infrastructure:

OMB

Government to Govt.

1. e-Vital (business case)
2. e-Grants
3. Disaster Assistance and Crisis Response
4. Geospatial Information One Stop
5. Wireless Networks

Managing Partner

SSA
HHS
FEMA

DOI

FEMA

Internal Effectiveness and Efficiency

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

Managing Partner

OPM

OPM

OPM

GSA

OPM

OPM

GSA

NARA



Vision

A common, ubiquitous, interoperable, Federal identity credential that facilitates trusted physical and logical access to buildings and services across the Federal sector while preserving the unique requirements of individual Federal organizations.

FICC addresses the needs of U.S. Federal Entities providing employee identity credentials



Value

- Improved reliability of physical credentials for asserting identity and authorizing access.
 - Ability to positively connect physical credential to the individual presenting it - biometric validation
 - Ability to verify the credential's validity - real time validation request to issuing organization.
 - Ability to automate visit requests, authorize/deny access
- Improved reliability and reliance on logical credentials
 - Logical access to networks
 - Reduced password/pin insecurity
 - Cross organizational access/authorization/identity validation
 - E-mail
 - Electronic Signature capability



FICC Goals

- Simplify and Unify Identity Authentication for Federal Employees
- Create requirements for Physical Credentials, electronic credentials, and issuance
- Develop the Federal Identity Credentialing Component of the Federal Enterprise Architecture



3 Major Subcomponents

- Smart Card Interoperability
 - Federal Smart Card Policy
 - Government Smart Card Interoperability Specification v. 2.1
 - Minimum requirements for topology, data sets, implementation
 - Aggregated Buy
- PKI Interoperability
 - Common Federal PKI Policy
 - Federal Bridge Certification Authority
 - Shared Services Migration
- Identity Assurance Interoperability
 - Guidance on minimum standards for identity assurance in credential issuance



Participants

- Smart Card Managers
- PKI Managers
- Human Resource Managers
- Physical Security Managers
- NIST
- OMB



The Committee

Department of Veterans Affairs

Office of Personnel Management

Department of Homeland Security

Department of Labor

Nuclear Regulatory Commission

General Services Administration

Department of Energy

Department of Commerce

Department of Justice

Department of State

Department of Education

Environmental Protection Agency

Department of Defense

Department of the Interior

US Agency for International Development

Department of Transportation

National Archives and Records Administration

Department of Housing and Urban Development

National Aeronautic and Space Administration

Social Security Administration

Small Business Administration

Department of Health and Human Services

National Science Foundation

US Department of Agriculture

Department of the Treasury

Office of Management and Budget



FJCC Working Groups

- Federal Smart Card Managers Group DOI/BLM
- Federal PKI Policy Authority Treasury
- PKI Certificate Policy Working Group NIST
- Identity Assurance Working Group TBD
- Smart Card Policy Working Group GSA
- Smart Card Data Modeling Working Group DOT
- Smart Card Topology Working Group GSA
- Shared Service Providers Working Group VA



The E-Authentication Connection

- FICC meets the needs of the 4th Sector: Internal Effectiveness and Efficiency.
- It Provides Federal Employees the means to perform their official and personal business using their Federally-issued logical identity credential.
- The FICC Common PKI Certificate Policy meets Assurance Level 3 of the *E-Authentication Guidance for Federal Agencies*
- E-Authentication Architecture includes interface with Common Policy Server and Federal Bridge Certification Authority (FBCA)



Parting Thoughts

This approach will end the proliferation of stove-pipes, drive standards adoption, and simplify interoperability across the Federal Enterprise.

The resulting infrastructure will enable the implementation of diverse capabilities that take advantage of standardized identity credentials and enhance security across and between Federal entities.