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
# President’s 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

## Lead
- GSA
- Treasury
- DOI
- Labor

## Government to Business
1. Federal Asset Sales
2. Online Rulemaking Management
3. Simplified and Unified Tax and Wage Reporting
4. **Consolidated Health Informatics**
5. Business Gateway
6. Int’l Trade Process Streamlining

## Lead
- GSA
- EPA
- Treasury
- HHS
- SBA
- DOC

## Cross-cutting Infrastructure: E-Authentication

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

### Lead
- SSA
- HHS
- FEMA
- DOI

### 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

### Lead
- OPM
- OPM
- OPM
- OPM
- GSA
- OPM
- GSA
- 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

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

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 -

- Increased $ Cost
- Increased Need for Identity Assurance

- PIN/User ID
- Knowledge-Based
  - Strong Password
- Multi-Factor Token
- PKI/ Digital Signature
- Access to Protected Website
- Applying for a Loan Online
- Obtaining Govt. Benefits
- Employee Screening for a High Risk Job
A VERY Simplified View of the Federal EAI Architecture

Levels 1 & 2 CSPs

EAI SAML Trust List

Levels 3 & 4 CSPs

CAF

Banks
Financial Inst.
Universities
Agency Apps
Commercial CSPs

FBCA X-Certification

FBCA PKI Trust List

Levels 1 & 2 Online Apps & Services

PIN, Passwords
User ID

SAML Assertions

SDT

Levels 3 & 4 Online Apps & Services

(HSPD-12)

Digital Certificates

One-Time Passwords
Multi-Factor Authentication

Digital Certificates

Federal Agency PKIs
Other Gov PKIs
Commercial PKIs
PKI Bridges
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

Agency Applications/Identity Credential Issuers

- Business & Operating Rules
- Operational Infrastructure

Policy

Technical Standards

Federation Roll-out FY 2006 and beyond

Completed FY 2005

Completed FY 2004
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*

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
Step #1: User goes to Portal to select the AA and CS

Step #2: The user is redirected to the selected CS with an AA identifier. The portal also cookies the user with their selected CS.

Step #3: The CS authenticates the user and hands them off to the selected AA with their identity information. The CS also cookies the user as Authenticated.

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.

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

- EAP
  - Common Governance
  - Common Trust Framework & Rules
  - Common Architecture & Interoperable Products

Federation 1
- IDP
- SP/RP

Federation 2
- IDP
- SP/RP

EAP Vision:

Multiple, Interoperable Federations

- EAP
  - Common Governance
  - Common Trust Framework & Rules
  - Common Architecture & Interoperable Products

Federation 1
- IDP
- SP/RP

Federation 2
- IDP
- SP/RP
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://csrd.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