Agenda

➢ Policy Foundation
  ▪ Portable Identity Approach
    ▪ Technology
    ▪ Trust
  ▪ Implementation
Policy Foundation: OMB M04-04
E-Authentication Guidance for Federal Agencies

- Defines 4 Assurance Levels
- “Agencies should determine assurance levels using the following steps, (described in Section 2.3):
  1. Conduct a risk assessment of the e-government system.
  2. Map identified risks to the applicable assurance level.
  4. Validate that the implemented system has achieved the required assurance level.
  5. Periodically reassess the system to determine technology refresh requirements.”
## Policy Foundation: OMB M04-04

### FIPS 199 Risk/Impact Profiles

<table>
<thead>
<tr>
<th>Potential Impact Categories for Authentication Errors</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inconvenience, distress or damage to standing or reputation</td>
<td>Low</td>
<td>Mod</td>
<td>Mod</td>
<td>High</td>
</tr>
<tr>
<td>Financial loss or agency liability</td>
<td>Low</td>
<td>Mod</td>
<td>Mod</td>
<td>High</td>
</tr>
<tr>
<td>Harm to agency programs or public interests</td>
<td>N/A</td>
<td>Low</td>
<td>Mod</td>
<td>High</td>
</tr>
<tr>
<td>Unauthorized release of sensitive information</td>
<td>N/A</td>
<td>Low</td>
<td>Mod</td>
<td>High</td>
</tr>
<tr>
<td>Personal Safety</td>
<td>N/A</td>
<td>N/A</td>
<td>Low</td>
<td>Mod High</td>
</tr>
<tr>
<td>Civil or criminal violations</td>
<td>N/A</td>
<td>Low</td>
<td>Mod</td>
<td>High</td>
</tr>
</tbody>
</table>
**Policy Foundation: NIST Special Pub 800-63**

- **SP 800-63 Technical Guidance**

<table>
<thead>
<tr>
<th>Allowed Token Types</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hard crypto token</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>One-time Password Device</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Soft crypto token</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Password &amp; PINs</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Identity, Credential, and Access Management

Agenda

✓ Policy Foundation

➢ Portable Identity Approach
  ➢ Technology
    ▪ Trust
  ▪ Implementation
Identity, Credential, and Access Management

Approach

- Adopt technologies in use by industry
  - “Scheme Adoption”

- Adopt industry Trust Models
  - “Trust Framework Adoption”

- Approach documents posted on http://www.IDmanagement.gov
Identity, Credential, and Access Management

**Approach: Scheme Adoption**

![Diagram showing the adoption process of various identity management schemes]

- **Industry Standards**
  - PKIX
  - WS-Fed
  - OpenID
  - Other

- **Authoritative Government Bodies**
  - CIO Council
  - OMB
  - NIST

- **Government Policies, Standards, and Profiles**
  - SAML
  - X509 Cert Profile
  - OCSP
  - M0404
  - 800-63
  - FIPS 201
  - Other
Identity, Credential, and Access Management

**Approach: Scheme Adoption**

- **Scheme Adoption**
  - Scheme – specific type of authentication token and associated protocols (e.g. user ID & password; PKI; SAML assertion)
  - Scheme Adoption produces a *Federal Profile*
  - Profile defines MUSTs, SHOULDs, SHOULD NOTs, etc. for Identity Providers (IdPs) & Relying Parties (RPs)
  - *Goal is not to change the existing technical standard*
  - Profiles complete for OpenID, Information Card (IMI), and SAML.

- *Federal ICAM Identity Scheme Adoption Process* and scheme profiles posted on http://www.IDmanagement.gov
Identity, Credential, and Access Management

Agenda

✓ Policy Foundation

➢ Portable Identity Approach
  ✓ Technology
  ➢ Trust

▪ Implementation
Approach: Trust Framework Adoption

- Trust Framework Adoption
  - Adoption of Industry Trust Frameworks
  - Adopts at Assurance Levels
  - Considers requirements of NIST SP 800-63
  - Trust Framework Evaluation Team (TFET) reviews applications

- Privacy Principles included
  - Opt in
  - Minimalism
  - Activity Tracking
  - Adequate Notice
  - Non Compulsory
  - Termination

Approach: Trust Framework Adoption

- Adopted Trust Framework Providers
  - Open Identity Exchange (OIX) (http://openidentityexchange.org/)
  - Kantarra Initiative (http://kantarainitiative.org/)
  - InCommon in progress (http://www.incommonfederation.org/)

- Approved Trust Framework Providers and Identity Providers posted on http://www.IDmanagement.gov
Open Identity Exchange

Executive Members

- AT&T
- Booz Allen Hamilton
- CA Technologies
- Equifax
- Google
- PayPal
- Symantec
- Verizon
- TNS Transaction Network Services
- LexisNexis
Identity, Credential, and Access Management

InCommon

- 202 Education Participants, 8 Govt/Non-Profit, 72 Sponsored Partners
- 5 million users

Current InCommon Participants

A community of more than 5 million end users.
(Source: Higher Education Students, Faculty, and Staff, Integrated Postsecondary Education Data System. Calculated October 2010)

<table>
<thead>
<tr>
<th>Higher Education Participants (202)</th>
<th>Government and Nonprofit Laboratories, Research Centers, and Agencies (8)</th>
<th>Sponsored Partners (72)</th>
</tr>
</thead>
<tbody>
<tr>
<td>American University</td>
<td>Argonne National Laboratory</td>
<td>Absolute Software, Inc.</td>
</tr>
<tr>
<td>Arizona State University</td>
<td>Energy Sciences Network (ESNet)</td>
<td>ALEKS Corporation</td>
</tr>
<tr>
<td>Augsburg College</td>
<td>Fermi National Accelerator Laboratory</td>
<td>Alexander Street Press</td>
</tr>
<tr>
<td>Baylor College of Medicine</td>
<td>Lawrence Berkeley National Laboratory</td>
<td>Apple - iTunes U</td>
</tr>
<tr>
<td>Baylor University</td>
<td>Moss Landing Marine Laboratories</td>
<td>Atlas Systems, Inc.</td>
</tr>
<tr>
<td>Boise State University</td>
<td>National Institutes of Health</td>
<td>BioOne, Inc.</td>
</tr>
<tr>
<td>Brown University</td>
<td>National Science Foundation</td>
<td>Blackboard, Inc.</td>
</tr>
<tr>
<td>California Institute of Technology</td>
<td>TeraGrid</td>
<td>Blanton Media Corporation</td>
</tr>
<tr>
<td>California Maritime Academy</td>
<td></td>
<td>Burton Group</td>
</tr>
<tr>
<td>California Polytechnic State University, San Luis Obispo</td>
<td></td>
<td>Cambridge University Press</td>
</tr>
<tr>
<td>California State Polytechnic University, Pomona</td>
<td></td>
<td>Cengage Learning, Inc.</td>
</tr>
<tr>
<td>California State University, Bakersfield</td>
<td></td>
<td>Colorado Alliance of Research Libraries</td>
</tr>
<tr>
<td>California State University, Channel Islands</td>
<td></td>
<td>CSO Research, Inc.</td>
</tr>
<tr>
<td>California State University, Chico</td>
<td></td>
<td>Davie County Schools</td>
</tr>
<tr>
<td>California State University, Dominguez Hills</td>
<td></td>
<td>Desire2Learn</td>
</tr>
<tr>
<td>California State University, East Bay</td>
<td></td>
<td>Digital Measures</td>
</tr>
<tr>
<td>California State University, Fresno</td>
<td></td>
<td>Docufide, Inc.</td>
</tr>
<tr>
<td>California State University, Fullerton</td>
<td></td>
<td>e-academy, Inc.</td>
</tr>
<tr>
<td>California State University, Long Beach</td>
<td></td>
<td>e2Campus by Omnilert, LLC</td>
</tr>
<tr>
<td>California State University, Los Angeles</td>
<td></td>
<td>Ebook Library - EBL</td>
</tr>
<tr>
<td>California State University, Monterey Bay</td>
<td></td>
<td>EBSCO Publishing</td>
</tr>
<tr>
<td>California State University, Northridge</td>
<td></td>
<td>EDUCAUSE</td>
</tr>
<tr>
<td>California State University, Office of the Chancellor</td>
<td></td>
<td>Elsevier</td>
</tr>
<tr>
<td>California State University, Sacramento</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Approach: Trust Framework Adoption

- Approved Identity Providers

<table>
<thead>
<tr>
<th>IDP</th>
<th>LOA</th>
<th>Scheme</th>
<th>TFP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google</td>
<td>1</td>
<td>OpenID</td>
<td>OIX</td>
</tr>
<tr>
<td>Equifax</td>
<td>1</td>
<td>IMI, OpenID</td>
<td>OIX</td>
</tr>
<tr>
<td>Paypal</td>
<td>1</td>
<td>IMI, OpenID</td>
<td>OIX</td>
</tr>
<tr>
<td>Verisign</td>
<td>1</td>
<td>OpenID</td>
<td>OIX</td>
</tr>
<tr>
<td>Wave</td>
<td>1</td>
<td>OpenID</td>
<td>OIX</td>
</tr>
</tbody>
</table>

- Approved Trust Framework Providers and Identity Providers posted on http://www.IDmanagement.gov
Identity, Credential, and Access Management

Agenda

✓ Policy Foundation
✓ Portable Identity Approach
  ✓ Technology
  ✓ Trust
➢ Implementation
Implementation

- Determine LOA for your application
  - M-04-04 levels of assurance
- Review Privacy Impact Assessment
  - use of third party credentials may effect PIA
Implementation

- Implement the appropriate scheme
  - e.g. “OpenID Enable” your site
  - OpenID, SAML, IMI Profiles on idmanagement.gov
  - Open Source, Free Libraries, Platform Modules, Commercial Products available
  - Schemes should be integrated into your existing application, probably by your existing web team
  - Details depend on how you built your website
  - Consider which IDPs support which schemes
  - Help available from the ICAM SC Lab
Implementation Considerations

- Configure metadata for approved IDPs
  - URLs, Configuration information for each IDP
  - Coordinate through ICAM SC Lab

- Consider User Interface (UI)
Implementation Considerations

UI
Implementation Considerations

- UI
Implementation Considerations

- Not rocket science
  - thousands of sites have implemented these technologies
  - does require attention from your web team
  - will impact release planning
  - does not require new commercial software, servers, bandwidth, capital expenditures, etc
  - impact similar to any new feature integrated into your site
Agenda

✓ Policy Foundation
✓ Portable Identity Approach
  ✓ Technology
  ✓ Trust
✓ Implementation
➢ Questions?
Backup Slides

- Scheme Details
Portable Identity Schemes: SAML

- **SAML**
  - OASIS SAML 2.0
  - Based on E-Gov Profile developed through Liberty
  - Broad COTS support
  - Has been used by government before

- **Federal Profile**
  - Requires E-Gov Profile
  - Requires encryption of PII
Portable Identity Schemes: SAML

1. User visits web site
2. Login page lists IdPs
3. User chooses an IdP
4. Browser redirected to IdP for login at LOA
5. IdP Challenges user to login to meet LOA
6. User logs in
7. IdP responds to RP with assertion
8. Validate Assertion
9. End user authenticated (access granted)
Portable Identity Schemes: OpenID

- OpenID
  - Open Source roots
  - OpenID Foundation serves as steward and provides necessary infrastructure
  - Used/supported by JanRain, SixApart, Google, Yahoo, Facebook, AOL, MySpace, Novell, Sun, etc.
  - 1 billion+ OpenID-enabled accounts
  - 40,000+ web sites support OpenID

- Federal Profile
  - Profile based on OpenID 2.0
  - Requires SSL/TLS on all endpoints
  - Requires Directed Identity Approach
  - Requires pair-wise unique pseudonymous identifiers
  - Requires short-lived association handles
Portable Identity Schemes: OpenID

1. End user visits web site
2. Login page lists IdPs
3. User chooses an IdP
4. IdP discovery
5. OpenID metadata information
6. Request association
7. Return association handle
8. Authentication Request
9. End user interaction (e.g., attribute exchange permission)
10. End user login
11. Assertion
12. Validate Assertion
13. End user authenticated (access granted)
Portable Identity Schemes: Information Card (IMI)

- **Information Card**
  - Analogous to the cards you carry in wallet
  - Open Source & industry standards
  - Supported by Azigo, CA, Equifax, Google, Intel, Microsoft, Novell, Oracle, Paypal, etc.
  - Built into MS Vista; option for XP
  - Earlier stage of adoption than OpenID
  - ALs 1 thru 3; possibly AL 4

- **Federal Profile**
  - Profile of *Identity Metasystem Interoperability Document 1.0* (IMI)
  - Requires encryption of PII
  - Requires use of optional *Private Personal Identifier* (PPID)
  - Managed cards only
Portable Identity Schemes: Information Cards (IMI)

1. User navigates to RP
2. HTTP request for Login page
3. Login FORM with OBJECT tag
4. Card Selector evaluates policy within OBJECT tag and finds candidate cards
5. Displays cards and interact with end user
6. End user selects card
7. Request security policy
8. Return security policy
9. Provide required claims and request security token
10. Return security token
11. HTTP POST security token
12. Process security token
13. Establish session and display page
14. End user granted access
Backup Slides

- Full Privacy Principles
Trust Framework Privacy Principles

1. **Opt In** Identity Provider must obtain positive confirmation from the End User before any End User information is transmitted to any government applications. The End User must be able to see each attribute that is to be transmitted as part of the Opt In process. Identity Provider should allow End Users to opt out of individual attributes for each transaction.

2. **Minimalism** – Identity Provider must transmit only those attributes that were explicitly requested by the RP application or required by the Federal profile. RP Application attribute requests must be consistent with the data contemplated in their Privacy Impact Assessment (PIA) as required by the E-Government Act of 2002.
Trust Framework Privacy Principles

3. **Activity Tracking** – Commercial Identity Provider must not disclose information on End User activities with the government to any party, or use the information for any purpose other than federated authentication. RP Application use of PII must be consistent with RP PIA as required by the E-Government Act of 2002.

4. **Adequate Notice** – Identity Provider must provide End Users with adequate notice regarding federated authentication. Adequate Notice includes a general description of the authentication event, any transaction(s) with the RP, the purpose of the transaction(s), and a description of any disclosure or transmission of PII to any party. Adequate Notice should be incorporated into the Opt In process.
Trust Framework Privacy Principles

5. Non Compulsory – As an alternative to 3rd-party identity providers, agencies should provide alternative access such that the disclosure of End User PII to commercial partners must not be a condition of access to any Federal service.

6. Termination – In the event an Identity Provider ceases to provide this service, the Provider shall continue to protect any sensitive data including PII.
Identity, Credential, and Access Management

Backup Slides

- IDManagement.gov
Identity, Credential, and Access Management

Open ID Solutions for Open Govt
Open Identity Solutions for Open Government

The Open Identity initiative seeks to leverage existing industry credentials for Federal use. The initiative approves credentials for government use through our Trust Framework Providers who assess industry Identity Providers (IDPs).

The Trust Framework Provider Adoption Process outlines the process that the ICAM community uses to sanction organizations that assess commercial identity providers.

Trust Framework Providers:

- Open Identity Exchange - Level of Assurance 1 (Provisional Approval)
- Kamea Initiative - Level of Assurance 1, 2, and non-trusted (Provisional Approval)
- InCommon Federation - Draft submission under review

The Scheme Adoption Process outlines the process that the ICAM community uses to develop and/or approve specification profiles for achieving portable identity over the Internet.

Adopted Schemes:

- ICAM OpenID 2.0 Profile - Fully adopted
- ICAM IMI 1.0 Profile - Fully adopted
- ICAM SAML 2.0 Web Browser SSO Profile - Fully adopted

Certified Identity Providers:

- Google - ICAM OpenID 2.0 Profile, Level of Assurance 1 - http://google.com
- Equifax - ICAM IMI 1.0 Profile, Level of Assurance 1 - http://equifax.com
- PayPal - ICAM OpenID 2.0 Profile, Level of Assurance 1 - http://paypal.com
- ICAM SAML 2.0 Web Browser SSO Profile - Fully adopted
- VeriSign - ICAM OpenID 2.0 Profile, Level of Assurance 1 - http://www.verisignlabs.com
- Wave Systems - ICAM OpenID 2.0 Profile, Level of Assurance 1 - http://wave.com