Identity, Credential, and Access Management

FICAM Ecosystem

June 9, 2011

Chris Louden
Identity, Credential, and Access Management

Agenda
- Standard Disclaimer
- Background / Scope
  - Goals / Drivers
  - Policy Foundation
- Trust Frameworks
- Structure
Goals / Drivers

- Principle focus on Government to Citizen
- Support E-Government traction
  - Electronic methods are cheaper, easier
  - Authentication often necessary
- Avoid credentialing of citizens
  - Costly, cumbersome to manage
  - “One more password” for citizens
- Accept identity asserted from trusted commercial providers

Government instance of NSTIC Vision…
<table>
<thead>
<tr>
<th>Potential Impact Categories for Authentication Errors</th>
<th>Assurance Level Impact Profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inconvenience, distress or damage to standing or reputation</td>
<td>1: Low</td>
</tr>
<tr>
<td>Financial loss or agency liability</td>
<td>1: Low</td>
</tr>
<tr>
<td>Harm to agency programs or public interests</td>
<td>N/A</td>
</tr>
<tr>
<td>Unauthorized release of sensitive information</td>
<td>N/A</td>
</tr>
<tr>
<td>Personal Safety</td>
<td>N/A</td>
</tr>
<tr>
<td>Civil or criminal violations</td>
<td>N/A</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>
Non-PKI 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. OAuth2 in Progress

- Federal ICAM Identity Scheme Adoption Process and scheme profiles posted on http://www.IDmanagement.gov
Non-PKI 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

*Federal ICAM Trust Framework Provider Adoption Process posted on http://www.IDmanagement.gov*
Non-PKI Approach: Trust Framework Adoption

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

- TFP’s are key
  - Public / Private partnership
  - Scalability

*Provisional until finalization of the Privacy Guidance for Trust Framework Assessors and Auditors
### Non-PKI 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>

- Higher assurance levels?
Structure

- Identity Credentialing and Access Sub Committee (ICAMSC)
  - Federal CIO Council
  - Information Security and Identity Management Committee (ISIMC)

- Trust Framework Evaluation Team (TFET)
  - Assesses Trust Framework Providers
  - Stakeholder Representation
    - DHS, FTC, GSA, IRS, NASA, NIH, NSS

- Architecture Working Group (AWG)
  - Scheme profiles

- Infrastructure
  - E-Governance Trust Services (EGTS)
    - Metadata, IDP Certificates