Personal Identity Verification (PIV) Cards

as Federated Identities –

Challenges and Opportunities

Dr. Sarbari Gupta
sarbari@electrosoft-inc.com
703-437-9451 ext 12

8th Symposium on Identity and Trust on the Internet (IDtrust 2009)
April 14-16, 2009
HSPD-12 requires Federal agencies to issue PIV Cards to all employees and contractors

State/Local governments and commercial entities are issuing PIV-like Cards

Immense opportunity to use PIV Cards (and PIV-like cards) as federated identities
  - Challenges
  - Strategies to promote federation
HSPD-12 Background

  - Issued August 2004
  - Mandates Federal Agencies to issue common form of identification to Federal employees & contractors

- FIPS 201 - Personal Identity Verification (PIV) of Federal Employees and Contractors
  - PIV Card: Smart Card based digital identity container with a set of identity credentials
  - PIV Card Issuers are required to be accredited by Agency Official
    - SP 800-79-1 – Accreditation Guide
PIV Card Credentials

- **Mandatory Credentials:**
  - Cardholder Unique Identifier (CHUID)
  - PIV Authentication Private Key and X.509 Certificate (PKI)
  - Cardholder Fingerprints in Biometric Object (BIO)

- **Optional Credentials:**
  - PIV Card Authentication Key (CAK)
  - PIV Digital Signature Private Key & X.509 Certificate
  - PIV Key Management Private Key & X.509 Certificate
  - Cardholder Facial Image

Pictures courtesy www.fedidcard.gov
Identity federation can be defined as ‘the agreements, standards and technologies that make identity and entitlements portable’ across otherwise autonomous security domains [Burton Group]

Goal: Enable users of one domain to securely access data or services of another domain
PIV-Interoperable & PIV-Compatible Cards

- Defined to promote *identity federation* between Federal and non-Federal Organizations

- Issued to personnel not eligible for PIV Cards
  - State and Local Government
  - Commercial Organizations

- PIV Compatible:
  - Meets technical specifications for PIV Card
  - Issuance process does not assure trust by federal relying parties

- PIV Interoperable:
  - Meets technical specifications for PIV Card
  - Issuance process assures trust in PKI Certificate
    - E-Authentication Level 4 Registration Requirements
    - PKI certificate issued under policy mapped to FBCA *Medium-HW* policy
## FIPS 201 & FBCA Medium-HW Policy

<table>
<thead>
<tr>
<th><strong>FIPS 201-1</strong></th>
<th><strong>FBCA Medium-HW policy</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>NACI has to be completed for full scope PIV card.</td>
<td>NACI not required for regular applicants.</td>
</tr>
<tr>
<td>FBI fingerprint check required.</td>
<td>Fingerprint check not required.</td>
</tr>
<tr>
<td>Facial image collected at registration.</td>
<td>Facial image not collected.</td>
</tr>
<tr>
<td>The applicant must appear in person at Registrar at least once prior to issuance.</td>
<td>Remote registration of applicant possible; applicant may avoid in-person encounter prior to issuance.</td>
</tr>
<tr>
<td>Two forms of original identity source documents. At least one must be a government issued picture ID.</td>
<td>One Federal government issued picture ID or two non-Federal IDs one of which is a picture ID.</td>
</tr>
<tr>
<td>Only designated sponsors can submit request for PIV card for an applicant.</td>
<td>No requirement for a sponsor for an applicant.</td>
</tr>
<tr>
<td>Identity proofing and registration process approved by head of agency.</td>
<td>Third party audit required for authorization to operate CA.</td>
</tr>
</tbody>
</table>
### PIV Federation - Risks and Mitigations

<table>
<thead>
<tr>
<th>RISK</th>
<th>MITIGATION</th>
</tr>
</thead>
</table>
| PIV Card Agency B (SSP PKI) | PKI – OK  
BIO – OK  
CHUID – OK  
Review Accreditation Package |
| PIV Card Agency C (Legacy PKI) | PKI – OK  
BIO – Explicitly trust Signer Cert  
CHUID – Explicitly trust Signer Cert  
Review Accreditation Package |
| PIV-Interoperable Card Organization D (Non-Fed SSP) | PKI – OK  
BIO – Explicitly trust Signer Cert  
CHUID – Explicitly trust Signer Cert  
Require Independent Assessment |
| PIV Compatible Card Organization E (Org PKI) | PKI – Explicitly trust Issuer  
BIO – Explicitly trust Signer Cert  
CHUID – Explicitly trust Signer Cert  
Require Independent Assessment |
Suggestions:

- OMB Memo: Federal Relying Party can accept PIV-Interoperable Cards only from issuers that are accredited/assessed using SP 800-79-1.

- Update Certificate Profiles for FBCA Medium-HW policy to indicate authority of PIV Object Signers
  - E.g., Common Policy supports `id-PIV-content-signing` certificate extension.

- Align the requirements of FIPS 201, Common Policy and FBCA Medium-HW Policy.

- Establish 3rd party audit regime for compliance with FIPS 201 requirements.
- Immense opportunity to use PIV Cards (and PIV-like cards) as federated identities

- QUESTIONS??