FIPS 201-2 Workshop

NIST PIV Team

National Institute of Standards and Technology
US Department of Commerce

Gaithersburg, MD
April 18 – 19, 2011
FIPS 201 EVALUATION PROGRAM
FIPS 201 Evaluation Program

David Temoshok
Director, Federal Identity Management
GSA Office of Governmentwide Policy

NIST FIPS 201-2 Workshop
April 19, 2011
Today’s Discussion

• Overview of FIPS 201 Evaluation Program
• PIV Interoperability
• Evaluation Program Infrastructure and Configuration Management
• Impact of FIPS 201-2 Proposed Changes
GSA FIPS 201 Evaluation Program Status

- GSA administers the FIPS-201 Evaluation Program to determine conformance to normative requirements in FIPS-201 and associated Special Publications.
  - Conformance assessment for **security, interoperability and performance**

- GSA/NIST identified 33 categories of products/services which must comply with specific normative requirements contained in FIPS 201
  - e.g., PIV smart cards, smart card readers, fingerprint scanners, fingerprint capture stations, facial image capture stations, card printing stations, physical access control systems, etc.

- Current product and services approvals:
  - 570+ products on FIPS 201 Approved Product List

- Certified labs:
  - Require NIST accreditation under NVLAP, GSA FIPS 201 EP Certification
  - Atlan Laboratories, InfoGard Laboratories, Atsec Corporation

- Agencies are required to acquire only approved products from GSA APL for the implementation of HSPD-12
The Need for Interoperability

• “For the purposes of this standard, interoperability allows any government facility or information system, regardless of the PIV Issuer, to verify a cardholder’s identity using the credentials on the PIV Card.”
  -- FIPS 201

• Interoperability is the ability:

  “…of two or more devices, components, or systems to exchange information (in accordance with defined interface specifications) and to use the information that has been exchanged in a meaningful way.”
  -- FIPS 201 Evaluation Program

• “Identity Solutions will be interoperable…Technical interoperability refers to the ability of different technologies to communicate and exchange data based on well-defined and testable interface standards.”
  -- National Strategy for Trusted Identities in Cyberspace (NSTIC)
The Starting Gate for Government-wide PIV Interoperability

- PIV Standard data model
- PIV Interoperability, security, and performance standards and requirements
- PIV data interface specifications
- PIV Standard Testing Programs
- Approved Product Lists

• Federal Standard Testing Programs
  - NIST NVLAP – PIV Application, PIV Middleware,
  - NIST MINEX – FP Template Generator, FP Template Matcher
  - FBI – FP scanning equipment
  - GSA FIPS 201 Evaluation Program/NVLAP – 33 Categories of Products on APL
<table>
<thead>
<tr>
<th>PIV Document</th>
<th>Date Issued</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIPS 201-1</td>
<td>Mar 2006</td>
<td>Personal Identity Verification (PIV) of Federal Employees and Contractors</td>
</tr>
<tr>
<td>SP 800-116</td>
<td>Nov 2008</td>
<td>A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)</td>
</tr>
<tr>
<td>SP 800-104</td>
<td>Jun 2007</td>
<td>A Scheme for PIV Visual Card Topography</td>
</tr>
<tr>
<td>SP 800-96</td>
<td>Sep 2006</td>
<td>PIV Card to Reader Interoperability Guidelines</td>
</tr>
<tr>
<td>SP 800-85 B</td>
<td>Jul 2006</td>
<td>PIV Data Model Test Guidelines</td>
</tr>
<tr>
<td>SP 800-85 A-2</td>
<td>Jul 2010</td>
<td>PIV Card Application and Middleware Interface Test Guidelines (SP800-73 compliance)</td>
</tr>
<tr>
<td>SP 800-79 -1</td>
<td>Jun 2008</td>
<td>Guidelines for the Accreditation of Personal Identity Verification (PIV) Card Issuers (PCI's)</td>
</tr>
<tr>
<td>SP 800-78 -3</td>
<td>Dec 2010</td>
<td>Cryptographic Algorithms and Key Sizes for Personal Identity Verification</td>
</tr>
<tr>
<td>SP 800-76 -1</td>
<td>Jan 2007</td>
<td>Biometric Data Specification for Personal Identity Verification</td>
</tr>
<tr>
<td>SP 800-73 -3</td>
<td>Feb 2010</td>
<td>Interfaces for Personal Identity Verification (4 parts): 1- End-Point PIV Card Application Namespace, Data Model and Representation 2- End-Point PIV Card Application Interface 3- End-Point PIV Client Application Programming Interface 4- The PIV Transitional Data Model and Interfaces</td>
</tr>
</tbody>
</table>
GSA FIPS 201 EP -- Product Evaluation Documentation

- GSA is Approval Authority and responsible for all product approvals, evaluation requirements, test requirements, test tools, and APL

- Approval Procedures
  - Provide details on all requirements for application package contents and the evaluation criteria for each requirement that applies to a particular product category
  - Product suppliers must ensure that all product evaluation requirements are met

- Test Procedures
  - Provide details on all test requirements and test procedures
  - PIV NVLAP Labs must follow Lab Test procedure explicitly for each product category

- Complete suite of Approval and Test Procedures and Supplier Requirements for all 33 APL product categories
GSA FIPS 201 Evaluation Program Test Tools

• **800-85B Data Conformance Test Tool**
  - Tests conformance to PIV data model and card encoding (Electronic Personalization)
  - Validates content of PIV data objects

• **Cardholder Facial Image Test Tool**
  - Tests conformance of biometric facial image stored on card

• **Server-based Certificate Validation Protocol (SCVP) Client**
  - Allows a product to delegate certificate path discovery and validation to the EP server
  - Supports EP testing using SCVP for products performing cryptographic functions

• **Data Populator Tool**
  - Capable of generating all mandatory PIV data objects: Card Capability Container, Cardholder Unique Identifier, X.509 Certificate for PIV authentication, Cardholder Fingerprint Template, and Security Object
  - Capable of generating all 4 PIV asymmetric key pairs

• GSA Test Tools are available for download at: [http:fips201ep.cio.gov/tools.php](http:fips201ep.cio.gov/tools.php)
GSA FIPS 201 EP Configuration Management

- All Product Evaluation and Testing Documents must be updated to reflect any changes in FIPS 201 requirements (or any associated SP)
  - All EP Approval and Test documentation reflect version status.
- All EP Test Tools must be updated to reflect any changes in FIPS 201 requirements (or any associated SP)
- All products are required to conform to current EP requirements
  - May require re-evaluation and re-testing
- Products from APL determined no longer compliant or no longer commercially available are removed from APL and posted on Removed Product List
  - Products on APL undergoing re-evaluation due to changed/new requirements are highlighted.
## FIPS 201 Proposed Key Changes – EP Impacts

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mandatory Card Auth Key</td>
<td></td>
<td>✓ PIV Cards &lt;br&gt; ✓ Electronic Personalization &lt;br&gt; ✓ CAK Auth System</td>
<td>✓ PIV Cards &lt;br&gt; ✓ Electronic Personalization &lt;br&gt; ✓ Card Reader – Transparent</td>
<td>✓ 800-85B Tool &lt;br&gt; ✓ Data Populator</td>
</tr>
<tr>
<td>New Iris Biometric Modality</td>
<td>✓ IRIS Scanning Equipment &lt;br&gt; ✓ IRIS Matching Equipment &lt;br&gt; ✓ PIV Card Reader(s) Iris</td>
<td>✓ IRIS Scanning Equipment &lt;br&gt; ✓ IRIS Matching Equipment &lt;br&gt; ✓ PIV Card &lt;br&gt; ✓ Electronic Personalization &lt;br&gt; ✓ PIV Card Reader Iris &lt;br&gt; ✓ Bio Auth Readers and Systems</td>
<td>✓ PIV Cards &lt;br&gt; ✓ Electronic Personalization &lt;br&gt; ✓ Bio Auth Readers &amp; Systems</td>
<td>✓ 800-85B Tool &lt;br&gt; ✓ Data Populator</td>
</tr>
<tr>
<td>On Card Biometric Comparison</td>
<td>✓ PIV Card Reader(s) OCC Bio</td>
<td>✓ PIV Card Reader OCC Bio &lt;br&gt; ✓ PIV Card</td>
<td>✓ PIV Card</td>
<td></td>
</tr>
<tr>
<td>Post Issuance Change</td>
<td></td>
<td>✓ Electronic Personalization</td>
<td>✓ Electronic Personalization</td>
<td></td>
</tr>
<tr>
<td>Mandatory DigSig + PDVAL - PIV Data Object Verification</td>
<td></td>
<td>N/A – already required from SP 800-116 changes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

U.S. General Services Administration
For More Information

- Visit our Websites:
  - http://www.idmanagement.gov

- Or contact:
  
  David Temoshok
  
  Director, Federal Identity Management
  
  david.temoshok@gsa.gov
  202-208-7655