GSA FIPS 201 Evaluation Program

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

NIST/DHS/TSA TWIC QPL Workshop
April 21, 2010

HSPD-12 Government-wide Implementation and Acquisition Strategy

- NIST provides HSPD-12 process and technical requirements (FIPS 201 and associated Special Publications).
- Government-wide interoperability is required. Implementation is controlled through acquisition process.
- GSA designated as "Executive Agent for Acquisition" for Information Technology for the implementation of HSPD-12. GSA is designated to establish an evaluation program to ensure that products/services conform to HSPD-12 (FIPS 201) requirements and to maintain an Approved Products List for products determined conformant to FIPS 201.
- Agencies are required by policy (M-05-24) and regulation (FAR Amendment 2005-17) to acquire only products from GSA-approved APL for the implementation of HSPD-12.

The PIV Document Suite (NIST)

PIV Document	Date Issued	Title
FIPS 201-1	Mar 2006	**Personal Identity Verification (PIV) of Federal Employees and Contractors**
SP 800-116	Nov 2008	**A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)**
SP 800-104	Jun 2007	**A Scheme for PIV Visual Card Topography**
SP 800-96	Sep 2006	**PIV Card to Reader Interoperability Guidelines**
SP 800-85 B	Jul 2006	**PIV Data Model Test Guidelines**
SP 800-85 A-1	Mar 2009	**PIV Card Application and Middleware Interface Test Guidelines (SP800-73 compliance)**
SP 800-79 -1	Jun 2008	**Guidelines for the Accreditation of Personal Identity Verification (PIV) Card Issuers (PCI's)**
SP 800-78 -2	Feb 2010	**Cryptographic Algorithms and Key Sizes for Personal Identity Verification**
SP 800-76 -1	Jan 2007	**Biometric Data Specification for Personal Identity Verification**
SP 800-73 -3	Feb 2010	**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

PIV Authentication Factors

PIV Authentication Mechanism	Have	Know	Are	PIV Assurance Level	Interface
Card Auth Key (CAK) + BIO (BIO, BIO-A or BIO AUTH)	x	x	x	4 – Very High confidence	Contact
BIO Authentication (digital signature validation of BIO Object)	x	x	x	4 – Very High confidence	Contact
BIO Attended	x	x	x	4 – Very High confidence	Contact
BIO – Biometric match off-card	x	x	x	3 - High confidence	Contact
PKI – cryptographic challenge - response	x	x		3 - High confidence	Contact
CHUID Authentication (digital signature validation of CHUID)	x			3 - High confidence	Contact/ Contactless
CAK -- cryptographic challenge - response	x			2 – Some confidence	Contact/ Contactless
CHUID + Visual	x			2 – Some confidence	Contact/ Contactless

The Need for Interoperability

Interoperability is defined as the ability:

- *"…of any government facility or information system, regardless of PIV issuer, to verify a cardholder's identity using the credentials on the PIV card."* FIPS 201-1
- *"…to use any PIV Card with any PACS application performing one or more PIV authentication mechanisms."* SP 800-116
- *"…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."* GSA FIPS 201 Evaluation Program

The Starting Gate for Interoperability

- Standard data model
- Interoperability and security standards
- PIV data interface specifications
- Standard Testing Programs - Products
- Reference Implementations - data interface specifications
- Standard Testing Program - data interface specifications
- **Federal Approved Product Lists**

- FIPS 201 and associated NIST Special Publications
- PIV Interface Specifications
- Federal Bridge Certificate Policy
- FPKI Audit requirements
- FICAM Profiles and Architecture suite
- Standard Testing Programs - Products
  - **GSA FIPS 201 Evaluation Program**
  - **NIST**
  - **FBI**
  - **NVLAP**
  - **FPKI**

GSA FIPS 201 Evaluation Program Status

- GSA administers the FIPS-201 Evaluation Program to determine conformance to FIPS-201 normative requirements.
  - Accredited laboratories perform all FIPS 201 compliance evaluations
  - Approved Product List posted at http://fips201ep.cio.gov/
- GSA/NIST identified 32 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:
  - 450+ products on FIPS 201 Approved Product List
- GSA and NIST partner to use NVLAP for FIPS-201 (PIV) testing
- Current certified labs:
  - Require NVLAP accreditation, GSA FIPS 201 EP Certification
  - Atlan Laboratories, InfoGard Laboratories, Atsec Corporation

GSA FIPS 201 Evaluation Program Document Suite

- Lab Documentation
  - Lab Specification
  - Laboratory Qualification Requirements
  - Configuration Management Plan
- Suppliers Handbook
- Approval Procedures
  - Specific approval procedures for all 34 categories of products on FIPS-201 APL
  - Vendor test requirements, lab test requirements, specific approval requirements
- Lab Test Procedures
  - Specific test procedures for all categories of products on FIPS-201 APL 450+ requiring testing through NVLAP-accredited labs.
- Standard Forms and Agreements

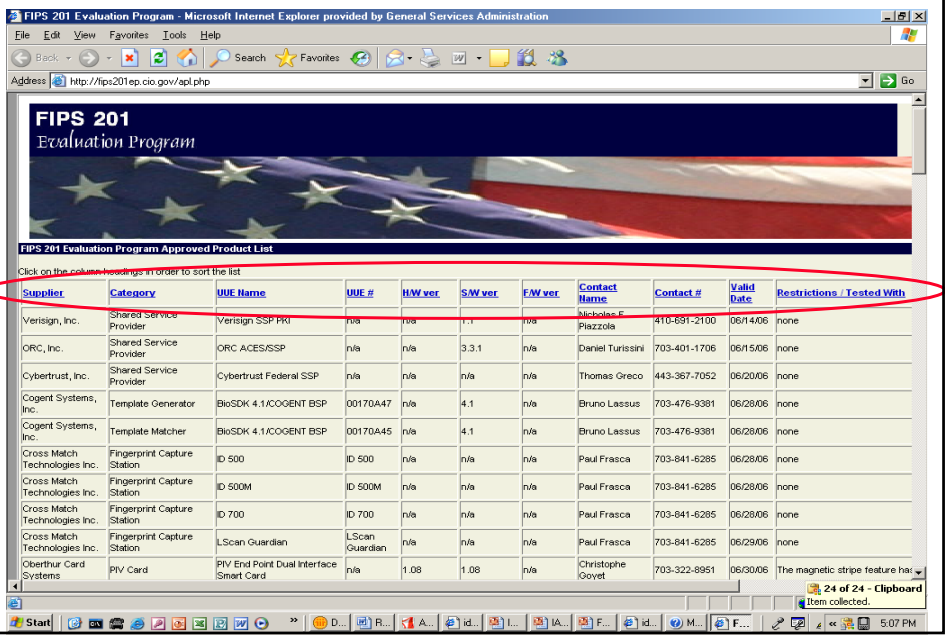
http://fips201ep.cio.gov/

GSA FIPS 201 Evaluation Program Test Tools

- 800-85B Data Conformance Test Tool
  - Tests conformance to PIV data model and card encoding
  - Validates data objects
- Cardholder Facial Image Test Tool
  - Test biometric facial image stored on card
  - Tests compliance with NIST SP 800-76-1 requirements – Biometric Data Specification for PIV
  - INCITS 385-2004
- Server-based Certificate Validation Protocol (SCVP) Test Tool
- Data Populator Tool
- GSA Test Tools are available for download at:

  http:fips201ep.cio.gov/tools.php

Accessing the FIPS 201 Approved Products List

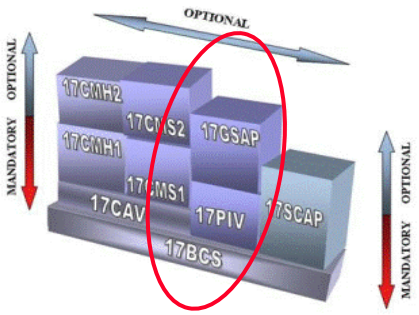


Schematic for GSA FIPS 201 EP Lab Accreditation and Certification

NIST built lab accreditation for GSA EP on Basic Cryptographic and Security Testing and PIV applet and middleware testing accreditation programs.

Steps for GSA EP Lab Certification:

1. Accreditation under NVLAP as a Basic Cryptographic and Security Testing (17BCS) laboratory.
2. Accreditation under NVLAP as a NIST Personal Identity Verification Program (NPIVP) Testing (17PIV) Laboratory.
3. Accreditation under NVLAP for all GSA FIPS 201 test methods (17GSAP).
4. Certification under GSA FIPS 201 Evaluation Program for all test, evaluation, and laboratory requirements.



Key Lessons Learned

- Carefully plan and standardize requirements and guidance documents for all users – suppliers, test labs, approval authority.
- Rigorously plan for configuration management
  - Document updates
  - Changes to requirements
  - Product/version changes
  - New use cases
- Facilitate product development, testing and conformance through development and maintenance of test tools.
- Actively engage the user community – suppliers, laboratories, implementers – in ongoing operation of evaluation program.
- Leverage other conformance and interoperability testing programs.

For More Information

- Visit our Websites:
  http://www.idmanagement.gov
  http://fips201ep.cio.gov/index.php

- Or contact:

David Temoshok
Director, Federal Identity Policy and Management
202-208-7655
david.temoshok@gsa.gov

April Giles, CISM, CISA, CISSP
FIPS 201 Evaluation Program Chief Architect
202-501-1123
april.giles@gsa.gov