Status Report On Personal Identity Verification Standards and HSPD#12

Topics

- HSPD-12 Requirements and Timeline
- FIPS 201 Requirements
- SP 800-73 Requirements
- SP 800-78 Requirements
- SP 800-79 Requirements
- Emerging Guidelines

HSPD-12 Presidential Policy Driver

Home Security Presidential Directive 12 (HSPD-12):

"*Policy for a Common Identification Standard for Federal Employees and Contractors*"

Dated: **August 27, 2004**

HSPD 12 Requirements

Secure and reliable forms of personal identification that is:

- Based on sound criteria to verify an individual employee's identity
- Strongly resistant to fraud, tampering, counterfeiting, and terrorist exploitation
- Rapidly verified *electronically*
- Issued only by providers whose reliability has been established by an official accreditation process

HSPD 12: Requirements (cont.)

- Applicable to *all* government organizations and contractors except identification associated with National Security Systems
- Used for access to Federally-controlled facilities and logical access to Federally-controlled information systems
- Flexible in selecting appropriate security level – includes graduated criteria from *least* secure to *most* secure
- Implemented in a manner that protects citizens' privacy

FIPS 201 Requirements

Phased-Implementation
In Two Parts

- Part 1 – Common Identification and Security Requirements
  - HSPD 12 Control Objectives
  - Identity Proofing, Registration and Issuance Requirements
  - Effective October 2005
- Part 2 - Common Interoperability Requirements
  - Detailed Technical Specifications
  - No set deadline for implementation in PIV standard
- Migration Timeframe (i.e., Phase I to II)
  - Agency implementation plans to OMB before July 2005
  - OMB has issued schedule for other elements (OMB M-05-24)

PIV Identity Proofing and Registration Requirements

- Organization shall adopt and use an approved identity proofing and registration process.
- Process shall begin with initiation of a National Agency Check with Written Inquiries (NACI) or other Office of Personnel Management (OPM) or National Security community investigation required for Federal employment.
- Before issuing the credential, agencies should receive notification of the resulte of the National Agency Checks (NAC). If the agency does not receive the results of the NAC within five days, the identity credential can be issued based on the FBI National Criminal History Check (fingerprint check). Note: a completed National Agency Check is sufficient for credential issuance; however, the required National Agency Check with Written Inquiries must still be completed.
- Applicant shall be required to provide two forms of identity source documents in original form. Source documents must come from the list of acceptable documents included in *Form I-9, OMB No. 1115-0136, Employment Eligibility Verification*. At least one document shall be a valid State or Federal government-issued picture identification (ID).
- Applicant must appear in-person at least once before the issuance of a PIV credential.

PIV Issuance and Maintenance Requirements (Cont.)

- The organization shall issue PIV credentials only through systems and providers whose reliability has been established by the agency and so documented and approved in writing (i.e., accredited).

Identity Proofing and Card Issuance Requirements

- No single individual shall be capable of issuing a PIV card
- Role Based Model
  - Roles of PIV Applicant, Sponsor, Registrar, and Issuer are mutually exclusive (I.e. no individual shall hold more than one of these roles in the identity proofing and registration process.)
  - PIV Issuer and PIV Digital Signatory roles may be assumed by one individual or entity.
- System-Based Model
  - Requires highly developed personnel management system and remotely accessible database (e.g., DoD DEERS/RAPIDS)
  - No cards issued to individuals not in the database

Privacy Requirements

- HSPD 12 requires that PIV systems are implemented with all privacy controls specified in this standard, as well as those specified in Federal privacy laws and policies including but not limited to the E-Government Act of 2002, the Privacy Act of 1974, and Office of Management and Budget (OMB) Memorandum M-03-22, as applicable.

- All agencies must:
  - have a privacy official role
  - conduct Privacy Impact Assessment (PIA) in accordance with standards
  - have procedures to handle Information in Identifiable Form (IIF)
  - have procedures to handle privacy violations
  - maintain appeals procedures for denials/revocation of credentials.

Part 2
PIV
Requirements

Functional Components

- PIV Front-End Subsystem — PIV Card, card and biometric readers, and personal identification number (PIN) input device. The PIV cardholder interacts with these components to gain physical or logical access to the desired Federal resource.

- PIV Card Issuance and Management Subsystem — the components responsible for identity proofing and registration, card and key issuance and management, and the various repositories and services (e.g., public key infrastructure [PKI] directory, certificate status servers) required as part of the verification infrastructure.

- Access Control Subsystem — the physical and logical access control systems, the protected resources, and the authorization data.

FIPS 201 REQUIREMENTS

- Mandatory and Optional PIV Card Visual Data
- Mandatory and Optional PIV Card Electromagnetic Elements
- Mandatory and Optional PIV Electronically Stored Data
- Card Information Available for “Free Read”

PIV Card Management

FIPS201 specifies:

- PIV Card Issuance
- PIV Card Maintenance
- PIV Card Renewal
- Card Re-issuance
- Card PIN Reset
- Card Termination

Interfaces for Personal Identity Verification

SP 800-73 specifies:

- PIV Data Model (Mandatory and Optional Data Elements)
- Optional Transition Card Interfaces (APIs, Object Naming Structure and Mapping Mechanism, Data Formats and Structures, Card Commands)
- Mandatory End-Point Card Interfaces Card Re-issuance
  - Data Objects
  - Data Types
  - Client Application Programming Interfaces
  - PIV Card Application Card Command Interface

Cryptographic Algorithms and Key Sizes for Personal Identity Verification

SP 800-78 specifies:

- Mandatory PIV Authentication Data (asymmetric key pair and corresponding PKI certificate)
- Optional Keys
  - Asymmetric key pair and corresponding certificate for digital signatures
  - Asymmetric key pair and corresponding certificate for key management
  - Asymmetric or symmetric card authentication keys for supporting additional physical access applications
- Cryptographic Algorithms and Key Sizes
- Authentication Information Stored on the PIV Card

Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations

SP 800-79 specifies:

- Certification & Accreditation Fundamentals
  - C&A Phases (Initiation, Certification, Accreditation, Monitoring)
  - Accreditation Decisions (Authorization, Interim Authorization, Denial)
  - Accreditation Package and Supporting Documentation
- Attributes of PIV Card Issuers (PCI) and Assessment Methods
- PCI Functions and Operations (Plan, Document, Implement, Operate)
- PIV Services and Operations
  - Applicant ID Proofing and Registration
  - PIV Card Issuance
  - PIV Card Life Cycle Management

Draft PIV Tools and Guidelines

- SP 800-73 Reference Implementation (Mandatory SP 800-73 elements)
- SP 800-85 PIV Middleware and PIV Card Application Conformance Test Guidelines
  - Test Plan, Test Set-up, and Test System Configuration
  - Test Suite Elements (Middleware Tests, Card Command Interface Tests and Data Object Representation Tests)
  - Derived Test Requirements
  - Test Assertions
  - Test and Compliance Documentation
  - Acceptance Criteria
  - Test and Compliance Process
- SP 800-87 Codes for the Identification of Federal and Federally-Assisted Organizations (Replaces Withdrawn FIPS 95-2)
- NPIVP Laboratory Designation for PIV Conformance Testing
- PIV Services and Operations

Some Issues and Questions

- Additional Issuer Accreditation Criteria/Procedure Needed?
- Basis for Accrediting Individuals for PIV Roles Needed?
- Need for Special Interest Groups
  - Issuer Organization Accreditation?
  - Acquisition?
  - PIV II Implementation/Migration?
  - Interoperability and Other Testing?
- Physical Security Implementation Support
  - Readers
  - Cryptographic Integration
  - Other?
- Resolution of Biometrics Formats (Image vs Template, 128K Cards?)
- Other?

Back-Up

HSPD-12 Milestones

Timeline	Agency/Department Requirement/Milestone
August 27, 2004	**Directive signed and issued**
Not later than 6 months (February 25, 2005)	**Issued standard**
Not later than 4 months following issuance of standard (June 25, 2005)	**Program in place to ensure that identification issued by organizations meet the PIV Standard (Part-1)**
Not later than 6 months following issuance of standard. (August 25, 2005)	**Identify additional applications that could benefit from conformance to the standard**
Not later than 8 months following issuance of standard (October 27, 2005)	**Compliance with standard (Part-1)**

PIV Card Visual Data

Mandatory

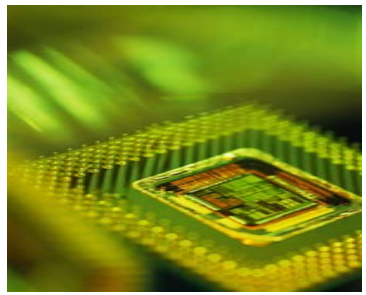
- Name
- Employee Affiliation
- Card Expiration Date
- Card Serial Number (Unique to Issuer)
- Issuer Identification

Optional

- Card Holder's Written Signature
- Pay Grade
- Rank
- Agency Name and/or Department
- Agency Seal
- Issue Date
- Information for Returning Lost Card
- Color codes
- Federal Emergency Official Designation

PIV Card Requirements

- Mandatory
  - Integrated Circuit to Store/Process Data



- Optional
  - Magnetic Stripe
  - Bar Code
  - Linear 3 of 9 Bar Code

- Interfaces:
  - Contact (ISO/IES 7816)
  - Contactless (ISO/IES 14443)

PIV Electronically Stored Data

Mandatory:

- PIN (used to prove the identity of the cardholder to the card)
- Cardholder Unique Identifier (CHUID)
- PIV Authentication Data (asymmetric key pair and corresponding PKI certificate)
- Two biometric fingerprints

Optional:

- An asymmetric key pair and corresponding certificate for digital signatures
- An asymmetric key pair and corresponding certificate for key management
- Asymmetric or symmetric card authentication keys for supporting additional physical access applications
- Symmetric key(s) associated with the card management system

Card Information Available for "Free Read"

- Federal Agency Smart Card Number (FASC-N)
  - Card-unique number
  - Agency-assigned number for card holder
  - Affiliation category (Employee, contractor, etc.)
  - Employer identification code
- Card Expiration Date
- Digital Signature
- Optional Information (i.e. Information not required by FIPS 201)
  - Data Universal Numbering System Number (DUNS)
  - Optional Global Unique Identifier (GUID)
  - Other optional information added at discretion of Issuing Agency

Authentication Mechanisms

- Three Identity Authentication Assurance levels
- Authentication using PIV Visual Credentials
- Authentication using the PIV CHUID
- Authentication using PIV Biometric
- Authentication using PIV Asymmetric Cryptography (PKI)

Graduated Assurance Levels for Identity Authentication

Authentication for Physical and Logical Access

PIV Assurance Level Required by Application/Resource	Applicable PIV Authentication Mechanism **Physical Access**	Applicable PIV Authentication Mechanism **Logical Access** Local Workstation Environment	Applicable PIV Authentication Mechanism **Logical Access** Remote/Network System Environment
SOME confidence	VIS, CHUID	CHUID	PKI
HIGH confidence	BIO	BIO	PKI
VERY HIGH confidence	BIO-A, PKI	BIO-A, PKI	PKI

Further Guidance

- Supporting Publications
  - SP 800-73 – *Interfaces for Personal Identity Verification* (card interface commands and responses)
  - SP 800-76 – *Biometric Data Specification for Personal Identity Verification*
  - SP 800-78 – *Recommendation for Cryptographic Algorithms and Key Sizes*
  - SP 800-79 – *Issuing Organization Accreditation Guideline*
- NIST PIV Website (http://csrc.nist.gov/piv-project/)
  - Draft Documents
  - Frequently Asked Questions (FAQs)
  - Comments Received in Original Format
- Additional Guidance
  - OMB Guidance (Policy) {http://www.whitehouse.gov/omb/inforeg/hspd-12_guidance_040105.pdf}
  - FICC Guidance (Implementation – *Identity Management Handbook*) {http://www.cio.gov/ficc/documents/FedIdentityMgmtHandbook.pdf}
  - NIST Guidance on Certification and Accreditation

Current Fiscal Year 2005 FIPS 201 Schedule

Scheduled Deliveries

Homeland Security Presidential Directive Signed	August 27, 2004
DoC Promulgation of FIPS 201	February 25, 2005
[GSA Federal Identity Management Handbook v0.2	March 8, 2005]
NIST SP 800-73, Interfaces for Personal Identity Verification	April 8, 2005
NIST SP 800-78, Crypto Algorithms for Personal Identity Verification	April 8, 2005
Draft SP 800-79, PIV Card Issuing Organization Accreditation Guidelines	June 17, 2005
Publish FIPS 201 Reference Implementation	June 25, 2005
[FIPS 201 Implementation Plans Due to OMB	June 27, 2005]
NIST SP 800-76, Biometric Data Specification for Personal Identity Verification	July 11, 2005*
Draft SP 800-79 Comments Due	July 15, 2005
Final SP 800-79, PIV Card Issuing Organization Accreditation Guidelines	July 25, 2005

Other FY 2005 Activities

- FIPS 201/FIPS 140-2 Derived Test Requirements
- FIPS 201 Conformance Test Suite
- FIPS 201 Compliance Test Facility Accreditation Guideline
- FIPS 201 Test Implementation Guidelines
- FIPS 201 Pre-Issuance Specification
- [Standard Common Software Platform – Facilitation of FIPS 140-2 Validation]
- [FIPS 201 Component and System Developer's Handbooks]
- Training Documentation [Testing, Developer, Issuer, User]

* Dependent on Homeland Security Council Action