FIPS 201-2 Workshop

NIST PIV Team

National Institute of Standards and Technology
US Department of Commerce

Gaithersburg, MD
April 18 – 19, 2011

PIV VALIDATION, CERTIFICATION, AND ACCREDITATION

Impact of FIPS 201-2 Changes on PIV Validation & Card Issuer Accreditation - Outline

- Overview of PIV Validation
- Impact of Proposed FIPS 201-2 changes on PIV Validation
- Overview of PIV Card Issuer (PCI) Accreditation Guidelines
- Impact of Proposed FIPS 201-2 changes on PCI Accreditation Guidelines

Current PIV Validation

- PIV Conformance Tests

  (a) PIV Card Interface Conformance Testing

  (b) PIV Card Data Model Conformance Testing

  (c) PIV Middleware (API) Conformance Testing

- Tests (a) & (c) are done by NVLAP accredited Labs using NIST supplied Toolkits on Commercial Product submissions
- NIST NPIVP Program validates the tests and issues certificates

Current PIV Validation (contd…)

- PIV Card Interface Conformance Testing
  - 100+ Positive & Negative Tests
  - Tests the Behavior of Card Commands (APDUs)
    - Based on the type of Interface
    - Configuration Values (e.g., PIN Reset counter)
    - Supported Cryptographic Algorithms
    - Mandatory and Optional Objects
    - Protection Requirements for Privileged Operations
  - Tests for accessibility of objects using correct OIDs

Impact of Proposed FIPS 201-2 changes on PIV Validation

Object Level Changes

Change -1: One or Two Iris Images – Alternate to fingerprint templates if they are not collectible.

Change -2: Asymmetric Card Authentication Key – now made mandatory instead of optional

Change-3: On-card biometric comparison data - optional

Test Impact: Accessibility from right interfaces

– Contact for Change-1 & Change-3 and

– Contact/Contactless for Change-2

Impact of Proposed FIPS 201-2 changes on PIV Validation (contd 1)

Operation Protection Changes

Change -4: PIV Card Activation for privileged operations can be done using equivalent verification data (e.g., biometric data) in addition to PIN

Test Impact: Ability to use alternate activation mechanism should be demonstrated for

– Accessing all Protected Objects other than Biometric Data

– Using Cryptographic Keys (e.g., PIV Authentication Key)

Impact of Proposed FIPS 201-2 changes on PIV Validation (contd 2)

Changes in Authentication Mechanisms

Change -5: Requirements for signature verification and certificate path validation made mandatory in – CHUID, BIO and BIO-A authentications.

Test Impact: Conformance Tests for above authentication mechanisms in PIV Data Model Testing should include path validation for embedded cert as well as signature verification

Impact of Proposed FIPS 201-2 changes on PIV Validation (contd 3)

Changes in Authentication Mechanisms

Change -6: Two Additional (optional) Authentication Mechanisms: (a) On-card Biometric Comparison & (b) Symmetric Card Authentication Key

Test Impact: Conformance Tests for the new authentication mechanisms in PIV Data Model Testing should be added

Overview of PIV Card Issuer (PCI) Accreditation

- Methodology Published in SP 800-79-1 (June 2008)
- Based on Assessment of Controls and Issuance of ATO
- There are 79 Controls under 13 Accreditation Focus Areas which in turn are organized under 4 Accreditation Topics
- The Four Accreditation Topics are:
  - Organizational Preparedness
  - Security Management and Data Protection
  - Infrastructure Elements
  - (PIV) Processes

Impact of Proposed FIPS 201-2 changes on PCI Accreditation

Reference to OPM directive on Credentialing Standards

Change -7: Explicit reference to OPM Memo dated July 31, 2008 under "Credentialing Requirements"

PCI Controls & Assessments:

(a) Written Policies & Procedures relating to enrollment/identity proofing (DO-2), PIV Card Issuance (DO-3) under "Preparation & Maintenance of Documentation".

Impact of Proposed FIPS 201-2 changes on PCI Accreditation

Changes in Enrollment Record Collection & Retention

Change -8: Retention of the most recent biometric data as part of the enrollment data set to create a "chain of Trust" to avoid expensive re-enrollment in situations such as Reissuance and Transfers.

PCI Controls & Assessments:

(a) Written Policies & Procedures relating to enrollment/identity proofing (DO-2), PIV Card Issuance (DO-3) & Re-issuance (DO-6) under "Preparation & Maintenance of Documentation".

Impact of Proposed FIPS 201-2 changes on PCI Accreditation

Specification of Identity Source Documents

Change -9: Extraction of content from I-9 form that is relevant to FIPS 201 and listing of Primary and Secondary Identity Source Documents

PCI Controls & Assessments:

(a) Checking of Identity Source documents for Employment Eligibility Verification (EI-3) under "Enrollment/Identity Proofing Process"

Impact of Proposed FIPS 201-2 changes on PCI Accreditation

Change in Re-issuance process Requirements

Change -10: Use of "Chain of Trust" record for 1-to-1 biometric match for re-issuance of compromised, lost, stolen or damaged PIV Cards.

PCI Controls & Assessments:

(a) "PCI Facility performs the entire identity proofing and enrollment/identity proofing process prior to re-issuing a PIV card (EI-5)" under "Enrollment/Identity Proofing Process" – Needs to be modified

Impact of Proposed FIPS 201-2 changes on PCI Accreditation

Issuance of Cards to a previous Holder

Change -11: Coverage of Issuance guidelines to include use cases where a previous PIV card holder is issued a card again within a grace period

PCI Controls & Assessments:

(a) Written Policies & Procedures relating to Card Issuance (DO-3).

Questions (?)