VALIDATION, CERTIFICATION, AND ACCREDITATION

Impact of FIPS 201-2 Revisions 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

Overview of 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
- Test (b) is used by GSA for verifying the Card Personalization function

Overview of 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 Status Changes

Change: The asymmetric Card Authentication Key (CAK), the Digital Signature Key (DSK), the Key Management Key (KMK) and Electronic Facial Image are now Mandatory Objects.

Test Impacts:

- Remove these objects from Tool Configuration Option
- Make Associated Tests Mandatory

  - Accessibility from Right Interfaces (Retrieval & Input)

  - Testing for Crypto Key presence (Challenge – Response)

Impact of Proposed FIPS 201-2 Changes on PIV Validation

New Optional Objects

Change: One or Two Iris Images – Optional alternative to fingerprint templates if they are not collectible.

Test Impacts:

- Include these objects in the Tool Configuration Options
- Include the necessary tests

Impact of Proposed FIPS 201-2 Changes on PIV Validation (Contd..1)

Operation/Object Protection Changes

Change: 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 Protected Objects (e.g., Facial Image)

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

Impact of Proposed FIPS 201-2 Changes on PIV Validation (Contd..1)

Object Content Changes:

Change: Mandatory UUID in CHUID, NACI indicator in PIV Authentication Certificate of all cards, Use of OID specific to signing certificate

Test Impacts:

- Data Model Tester should test for correct representation and valid values for these data items.

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

Issuance, Renewal and Reissuance

Change: Changes in Condition for Renewal, Reissuance, and Biometric match requirements during Issuance

PCI Controls & Assessments:

Control and Assessment procedures in the following Accreditation Focus areas will need to be changed:

- Card Activation / Issuance Process
- Maintenance Process

Impact of Proposed FIPS 201-2 Changes on PCI Accreditation

Accreditation Assurance

Change: Independent Review of PIV Card Issuer (PCI) Accreditation

PCI Controls & Assessments:

Add New Controls for:

- Choice of entity for independent review
- Procedures for independent review
- Follow-up action to independent review

Questions (?)