Derived PIV Application and Data Model Test Guidelines (NIST SP 800-166 Draft) – Status Update

Ramaswamy Chandramouli (Mouli)
Information Technology Lab (ITL), NIST
March 4, 2015

FIPS 201-2 Associated Special Publication’s Workshop
Derived PIV Application & Data Model Test Guidelines – Status Update

• Derived PIV Application & Data Model Tests – Objectives

• Scope of the SP 800-166 Document

• Overview of Contents

• Publication Process Timeline
Derived PIV Application & Data Model Test Guidelines - Objectives

• Provide Test Requirements and Test Assertions for testing conformance of:
  (a) Derived PIV Application
  (b) Derived PIV Application Data Model

• TO THE FOLLOWING SPECIFICATIONS
  - Derived PIV Credentials (SP 800-157)
  - Interfaces for Personal Identity Verification (SP 800-73-4)

• ON NON-EMBEDDED TOKENS SUCH AS
  - microSD
  - USB &
  - Universal Integrated Circuit Cards (UICC)
SP 800-166 (Derived PIV Application & Data Model Test Guidelines) - Scope

- Derived PIV Application Conformance Tests
  - Derived PIV Application Object Access & Storage Tests
  - Derived PIV Application Interface Conformance Tests

- Derived PIV Application Data Model Conformance Tests
  - BER-TLV Format Conformance
  - Digital Signature Conformance
  - PKI Profile Conformance
Derived PIV Application & Data Model Conformance Test Configuration
Overview of Contents (Generic Token Requirements)

- UICC shall implement the Global Platform Card Secure Element Configuration v1.0
- USB ICCDs (Secure Element) used shall comply with USB Device Class – Smart Card Specification [ICCDSPEC]
- The APDUs for Derived PIV Application shall be transported to Secure Element using Bulk-out command pipe and responses be received using Bulk-in command pipe.
- USB Tokens with cryptographic modules shall be compliant with “APDU Support for contact card readers” specification in SP 800-96.
SP 800-166 – Overview of Contents (Derived PIV Application Conformance Tests)

• I. Object Access & Storage Tests
  • Accessibility of Mandatory object and any optional object specified in the documentation using BER-TLV tags of the corresponding PIV application objects of Section 4 of SP 800-73-4 Part 1 based on mapping in Table B-1 of SP 800-157.
  • Usage of all key references based on references to corresponding keys in Table 4 of SP 800-73-4 Part 1 & Table 6-1 of SP 800-78-4 based on mapping in Table B-2 of SP 800-157.
I. Object Access & Storage Tests.. Contd

- Usage of Cryptographic algorithm identifiers as per Tables 6.2 & 6.3 of SP 800-78-4 and Cryptographic mechanism identifiers as per Table 5 of SP 800-73-4

- Allocation of right container size for objects

- Access of data objects & private key usage based on access rule (Password – its size & wrong attempts)

- Satisfaction of Security condition for Update/Storage of data objects
II. Interface Conformance Tests

• Testing the following commands: SELECT, GET DATA, VERIFY, CHANGE REFERENCE DATA, RESET RETRY COUNTER, GENERAL AUTHENTICATE, PUT DATA & GENERATE ASYMMETRIC KEY PAIR - for

• Right precondition for use

• Expected Return/Status codes

• Right post condition (e.g., State Variable value)
SP 800-166 – Overview of Contents (Derived PIV Application Data Model Conformance Tests)

I. BER-TLV Conformance

- Derived PIV Authentication Certificate (*Mandatory*)
- Digital Signature Certificate
- Key Management Certificate
- Discovery Object
- Key History Object
- Retired Certificates for Key Management
- Security Object
SP 800-166 – Overview of Contents (Derived PIV Application Data Model Conformance Tests)

II. Digital Signature Conformance

• Security Object (Only Signed Object)
  - Presence of Discovery Object & Key History Object Hashes
  - Asymmetric Digital Signature for conformance to Cryptographic Message Syntax – RFC 5652
  - Digest Algorithm & Signature Algorithms in accordance with SP 800-78-4 specification
SP 800-166 – Overview of Contents (Derived PIV Application Data Model Conformance Tests)

III. PKI Profile Conformance

- Derived PIV Authentication Certificate
- Digital Signature Certificate
- Key Management Certificate
- PIV Credential Issuer Certificate (Data Object Signing Certificate)
## SP 800-166 – Publication Timeline

<table>
<thead>
<tr>
<th>Milestone</th>
<th>Planned Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Public Comment Draft</td>
<td>4/24/2015</td>
</tr>
<tr>
<td>Public Comment Period - Closing Date</td>
<td>5/22/2015</td>
</tr>
<tr>
<td>Publication of Final Document</td>
<td>10/06/2015</td>
</tr>
</tbody>
</table>
Thank you

Questions?

Ramaswamy Chandramouli (Mouli)
NIST ITL Computer Security Division
mouli@nist.gov