

PIV Test Guidelines Revisions

Dr. R. Chandramouli (Mouli)

mouli@nist.gov

(Director NPIVP)

NPIVP Workshop

March 3, 2006

Red Auditorium, NIST, Gaithersburg

Scope of SP 800-85

DTRs and Test Assertions Cover the testing of the following for Conformance to SP 800-73 Specs:

- 1. PIV Middleware Interface – Client Application Programming Interface (Chapter 6)**
- 2. PIV Card Application Interface – Card Application Card Command Interface (Chapter 7)**
- 3. PIV Data Model (Chapter 4 & Appendix A)**

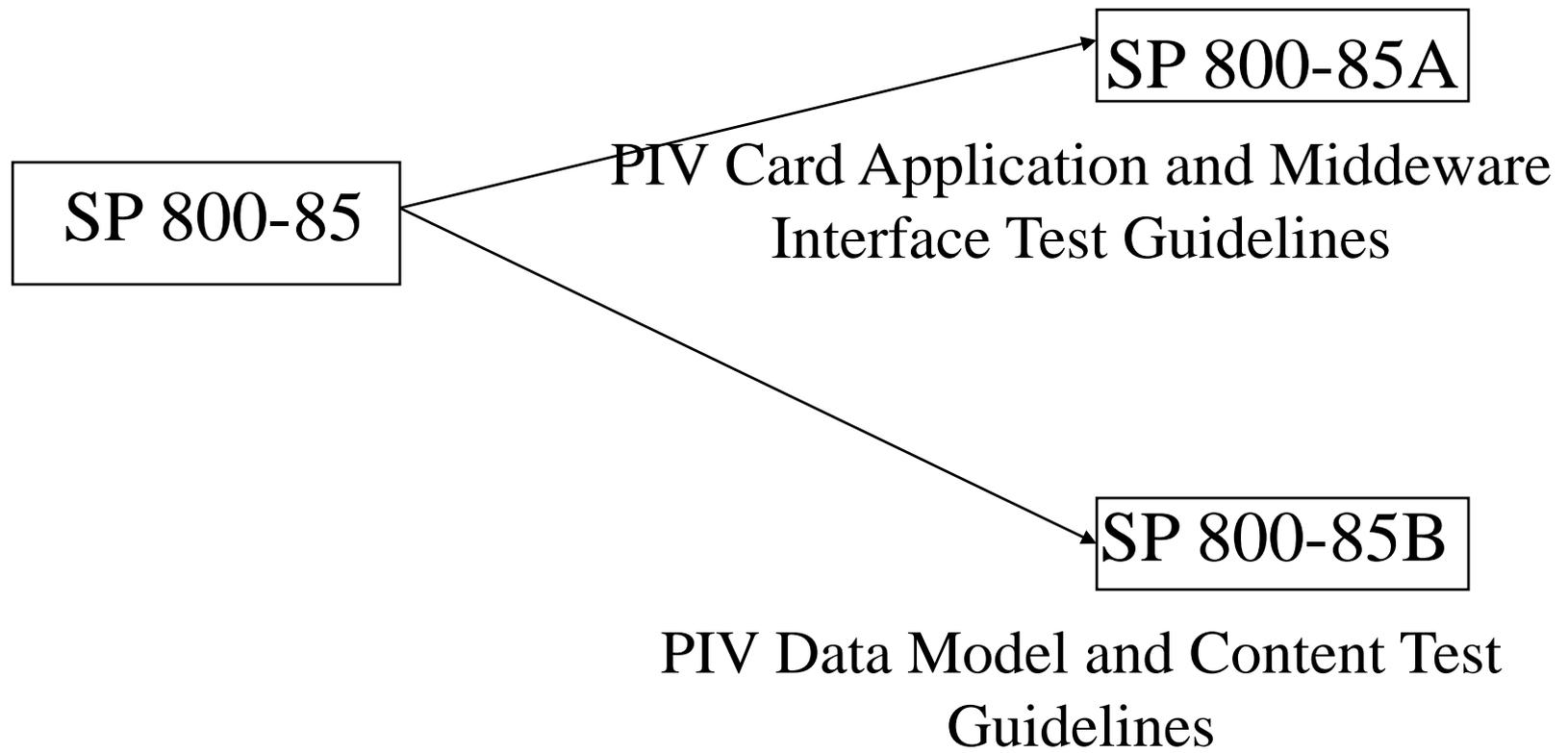
PIV Conformance Testing Process Overview

Test Type	By whom	When
PIV Middleware Interface	Accredited NPIVP Lab	Prior to Agency Procurement
PIV Card App. Interface	Accredited NPIVP Lab	Prior to Agency Procurement (Card Pre-Personalization)
PIV Data Model (On-card Content)	Agencies (or Sys. Integrator)	During Card Issuance (Personalization)

PIV Conformance Testing Guidelines Documents Overview (Revised)

Test Type	By whom	Document
PIV Middleware Interface	Accredited NPIVP Lab	SP 800-85A
PIV Card App. Interface	Accredited NPIVP Lab	SP 800-85A
PIV Data Model and Content	Agencies (or Sys. Integrator)	SP 800-85B

PIV Conformance Testing Guidelines Document Titles



PIV Card Application and Middleware Interface Test Guidelines (SP 800-85A)

- Scope

- **PIV Middleware Interface Tests**
 - 9 Functions
 - 81 Test Cases
- **PIV Card Application Interface Tests**
 - 8 APDU_s
 - 97 Test Cases
 - 68 Contact, 29 Contactless Interface

What is “New” and “Out” in SP 800-85A

Out

- Appendix D – PIV Data Objects Representation Test Assertions
- Appendix E - PIV Authentication Use Case Test Assertions
- Appendix F.3 – Data Objects Representation Test Results Summary
- Appendix F.4 – Authentication Use Case Test Results Summary
- Appendix F.5 – To be renamed to “Test Discrepancy Cases Reporting Template” and re-numbered.

What is “New” and “Out” in SP 800-85A

New

- Appendix D – DTRs to Test Assertions Mapping Table
- Testing Integrity of Data Objects storage based on BER-TLV tags – WHAT IS IN = WHAT WE GET
- Tests Modified to capture 800-73-1 changes
e.g., Removal of PIN requirement for Certificate buffers
- Testing of GENERAL AUTHENTICATE command for all three types of authentication – INTERNAL, EXTERNAL and MUTUAL.

PIV Data Model and Content Test Guidelines (SP 800-85B) - Scope

- **BER-TLV Format Conformance Tests**
 - All data Objects
 - Appendix A of SP 800-73
- **Biometric Data Format Conformance Tests**
 - Fingerprint and Facial Objects
 - SP 800-76
- **Cryptographic Objects Tests**
 - Certificates, Signature Blocks
 - SP 800-78, FIPS 201-1

Publication Dates

- **SP 800-85A – March 10th, 2006**
- **SP 800-85B - April 3th, 2006**

