PIV Conformance Testing – Scope and Process

Dr. R. Chandramouli (Mouli)

National Inst. Of Standards & Technology

mouli@nist.gov

5th Annual Smart Cards in Government Conference

April 18-20, 2006

PIV Conformance Testing – Artifacts Covered

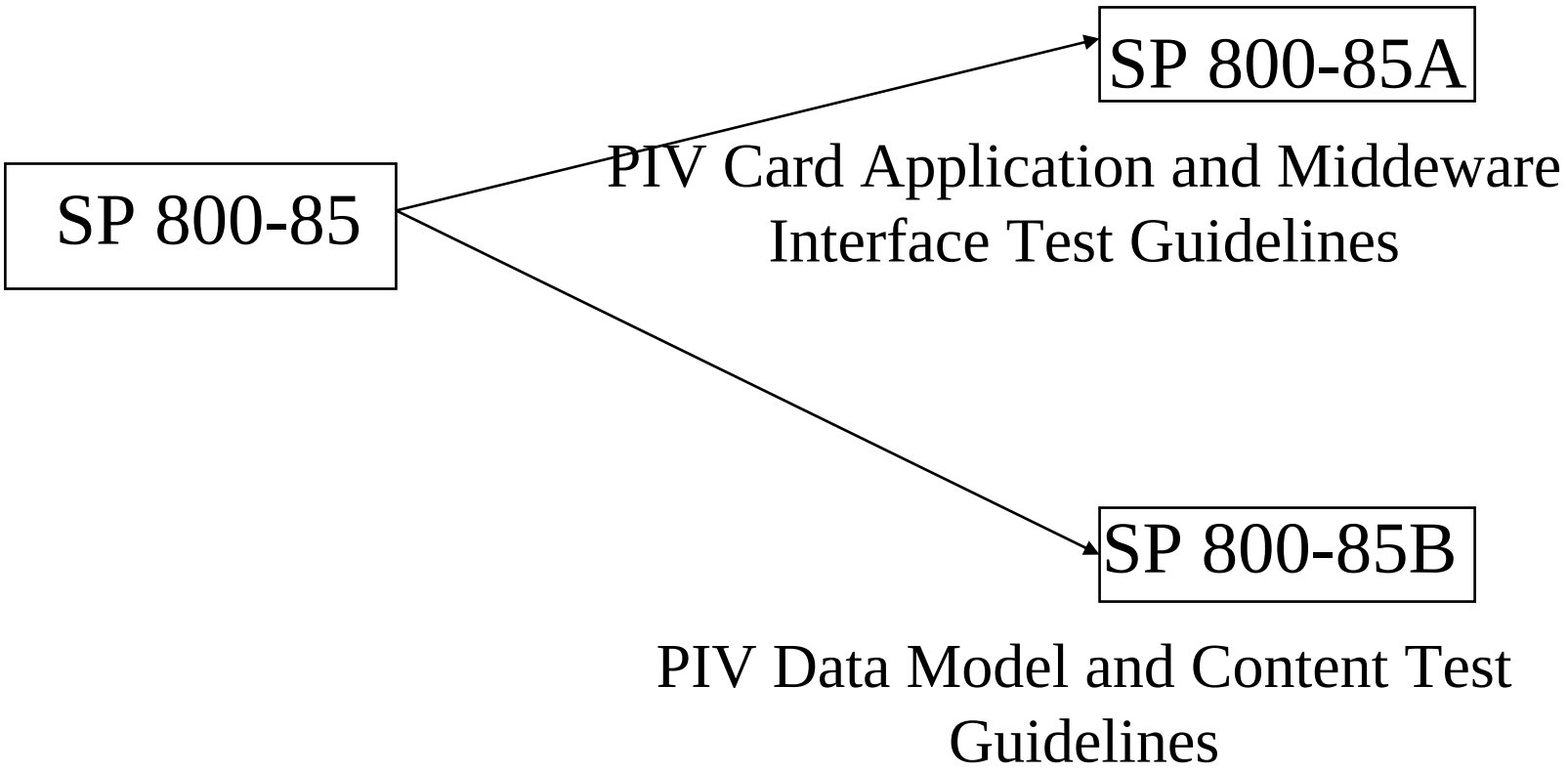
Interfaces (Guidelines – SP 800-85A)

- **PIV Card Application Interface**
- **PIV Middleware Interface**

Data Objects (Guidelines – SP 800-85B)

- **PIV Card Application Objects**
- **Cryptographic Objects**
- **Biometric Data**

PIV Conformance Testing Guidelines Document Titles



PIV Conformance Testing – Testing Entities & Basis Specs

Test Type	By whom	Basis Specs
PIV Middleware Interface	Accredited NPIVP Lab	SP 800-73-1 (Chapter 6)
PIV Card Application Interface	Accredited NPIVP Lab	SP 800-73-1 (Chapter 7)
PIV Data Model and Content	Agencies (or Sys. Integrator)	SP 800-73-1 (Appendix A) SP 800-78 SP 800-76

PIV Conformance Testing – Lifecycle Context &Validated Entity

Test Type	When	Validated Entity
PIV Middleware Interface	Prior to Agency Procurement	*Product* (Software)
PIV Card Application Interface	Prior to Agency Procurement (Card Pre-Personalization)	*Product* (Card with a loaded program)
PIV Data Model and Content	Prior to Card Issuance	*System* (Card Issuance)

PIV Conformance Testing – Interfaces Testing Process

- **Tests enabled by a NIST-developed Toolkit**
  - PIV Middleware – 9 Functions, 65 Test Cases
  - PIV Card Application – 8 APDUs
    (Contact) – 73 Test Cases
    (Contactless) – 29 Test Cases
- **Formal Certification & Validation Program- NPIVP (http://www.nist.gov/npivp)**
  - Tests done by accredited NPIVP Labs
  - NIST validates results & Issues Certificates

PIV Data Model and Content Tests (SP 800-85B) – Card Application Objects

- **Conformance to Data Model specified in**

  Appendix A of SP 800-73-1 (BER-TLV)

  - Correct tag identifiers
  - Correct representation of Tag Lengths
  - Length of Data field consistent with Length indicated in Length field

PIV Data Model and Content Tests (SP 800-85B) – Cryptographic Objects

- **Certificate Conformance**
  - The 4 certificates conform to profiles specified in "X.509 Certificate and CRL Extensions Profile for the SSP Program"
- **Signed Objects Conformance**
  - Signature Blocks Conform to FIPS 201 Specs
- **Algorithm Usage & Signature Integrity**
  - SP 800-78 Specified Algorithms Used
  - Signature Content Verifies for included data

Biometric Data Testing - Taxonomy

- **Fingerprint Template (Minutiae) Performance Testing (for Interoperability)**
  - Tests Vendors' Minutiae Extractor and Matcher Algorithms for matching performance
  - Matrix based MINEX Tests developed by NIST
- **Fingerprint Template (Minutiae) Representation on the Card**
  - Formats for various components of the representation tested for Conformance to Specs in SP 800-76.

PIV Data Model and Content Tests (SP 800-85B) – Biometric Data

- **CBEFF Patron Format Conformance**
  - Allowed Values
  - Content Integrity (e.g.,) – BDB length matches the value in the CBEFF Header
- **ANSI INCITS 378 Profile Conformance**
  - Required Fields, Allowed Values & Encodings
  - Content Integrity (e.g.,)
    - Number of Minutiae Records matches the value in View Header

PIV Data Model and Content Tests – Planned Process

- **Guidelines Document - SP 800-85B**

  - To be published for public comments on May 12, 2006

- **Beta Version of Data Model & Content Tester**

  - Made Available to Agencies on May 19,2006

- **Questions**

  - **Mouli (mouli@nist.gov)**