FIPS 201 Validation and Test Support Activities at NIST

Dr. R. Chandramouli (Mouli)

National Inst. Of Standards & Technology

mouli@nist.gov

FIPS 201 Evaluation Program Information Day

GSA, June 19, 2006

NIST Validation and Test Support Activities – FIPS 201 Components Covered

1. Validation

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

2. Test Support

- **Personalized Data on the PIV Card – covers Card Management System, Cryptographic Modules, PKI System outputs**
- **Biometric Software – Template Generators and Matchers**

NIST Validation and Test Support Activities – Documents, Toolkits & Operations

1. Validation

- ***Document***
  - **SP 800-85A – Test Guidelines for PIV Card and Middleware Interfaces**
- ***Toolkit***
  - **Card & Middleware Interface Test Runner**
- ***Operations***
  - **Accreditation of NPIVP Labs**
  - **Validation of Test Reports from Labs**
  - **Issuance of Certificates**

NIST Validation and Test Support Activities – Documents, Toolkits & Operations (Cont.)

2. Test Support

- *Document*
  - SP 800-85B – PIV Data Model Test Guidelines
  - MINEX Test Report
- *Toolkit*
  - PIV Data Model & Content Test Runner
- *Operations*
  - Process for including Template Generators and Matchers from new vendors into the Interoperability Matrix

FIPS 201 Validated Components – Testing Organizations and 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)

FIPS 201 Validated Components – 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 & Content Tests

Test Type	Basis Specs
BER-TLV Conformance	*SP 800-73-1 – Appendix A*
Biometric Objects – Format & Profile	*SP 800-76*
Signed Objects Conformance	FIPS 201-1, RFC 3852, SP 800-78
PKI Certificate Profiles Conformance	FICC – SSP PKI Certificate Profiles, SP 800-78

PIV Data Model and Content Tests (BER-TLV Conformance)

- **Conformance to Data Model specified in Appendix A of SP 800-73-1**
  - 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 (Biometric Objects – Format & Profile- SP 800-76)

- **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 (Cryptographically Signed Objects – FIPS 201-1, RFC 3852 & SP 800-78)

- **Signed Objects Conformance**
  - Signature Blocks Conform to FIPS 201-1 Specs
  - Signature Encoding as per RFC 3852
- **Algorithm Usage & Signature Integrity**
  - SP 800-78 Specified Algorithms Used
  - Signature Content Verifies for included data

PIV Data Model and Content Tests (PKI Certificate Profiles – FICC SSP PKI Profiles)

- Certificate Format and Encoding should conform to Profiles in “X.509 Certificate and CRL Extensions Profile for the SSP Program”
- Certificates are:
  - PIV Authentication Certificate
  - Digital Signature Certificate
  - Key Management Certificate
  - Card Authentication Certificate

Biometric Data Interoperability Tests - MINEX

- **Fingerprint Template (Minutiae) Performance Testing (for Interoperability)**
  - Tests Vendors' Minutiae Extractor and Matcher Algorithms for matching performance
  - Matrix based MINEX Tests developed by NIST

MINEX Test -Types of Templates

- Proprietary templates
  - Individual vendor's representation of images
- Standard templates: INCITS 378 format
  - MIN:A templates
    - codes minutiae coordinates (x, y), angle (θ), type, & quality
  - MIN:B templates
    - MIN:A data plus ridge count, core, and delta information

MINEX Test - Largest Biometric Test to Date…

- 4 datasets:
  - POEBVA, DHS2, POE, and DOS
- Number of Samples
  - 60,000 matched fingerprint pairs
  - 120,000 non-match fingerprints
- 14 vendors
  - Six participants in MIN:B testing
- 4.4 billion comparisons resulting in >45 GB of data

MINEX Test – Vendors in Initial Round

A. Cogent Systems Incorporated
B. Dermalog Identification Systems GMBH
C. Bioscrypt Incorporated
D. Sagem Morpho Incorporated
E. Neurotechnologija
F. Innovatrics
G. NEC Corporation
H. Technoimagia Corporation
I. Identix Incorporated
J. Biologica Sistemas
K. SPEX Forensics
L. Secugen Corporation
M. NITGen Corporation
N. Cross Match Technologies

MINEX Test - Questions

- Does the template give accuracy comparable with proprietary (image-based) implementations?
- Can template data be generated and matched by different vendors without attendant increase in error rates?

MINEX Test - Types of Tests

- Single- v. Two- Finger
- Proprietary v. Native
- Native v. Interoperable
- Scenarios 1,2,3,&4
- Four dataset of different quality

MINEX Test - Results 1

- Proprietary templates are superior to MIN:A templates in accuracy.
- The enhanced MIN:B template performed only marginally better than the basic MIN:A template.

MINEX Test - Results 2

- As with most recent tests (by NIST and others), the error rates between matching algorithms vary by an order of magnitude.
- Two-finger authentication with standard templates can achieve the accuracy of single-finger authentication with proprietary templates.

MINEX Test - Results 3

- The leading vendors in template generation are not always the leaders in matching and vice-versa.
  - Some template generators produce standard templates that are matched more accurately than others. Some combination of templates fail completely.
  - Some matchers compare templates more accurately than others.

MINEX Test - Results 4

- Certification of an interoperable group of products requires some prior specification of the required accuracy.
  - More products will interoperate when the accuracy requirement is low and vice versa.
  - More products can be certified if the group's mean error rate is below a threshold than if their worst interoperable pair is used for certification.

MINEX Test - Results 5

- Performance is sensitive to the quality of the dataset.
  - Applies to both proprietary and interoperable templates.
  - Two higher quality datasets (POEBVA and POE) provide reasonable interoperability. Two lower quality datasets (DOS and DHS2) do not.