Special Publication 800-73: Interfaces for Personal Identity Verification

Jim Dray

NIST NPIVP Workshop

March 3, 2006

PIV Special Publications

- SP800-73: Interfaces for Personal Identity Verification
- SP800-76: Biometric Data Specification for Personal Identity Verification
- SP800-78: Cryptographic Algorithms and Key Sizes for Personal Identity Verification
- SP800-79: Issuer Organization Accreditation Guidance (comment draft 17 June)

NIST
National Institute of Standards and Technology

Special Publication 800-73

- "Interfaces for Personal Identity Verification" 8 April 2005
- Technical specifications for PIV card interface, client API, and data model
- Based on evolution of GSC concepts:
  - Unified card interface
  - Technology neutral (VM card, file system card)
  - Standards compliant (ISO)

NIST
National Institute of Standards and Technology

SP800-73 Document Structure

- Part 1: Architectural model
- Part 2: Transition specification
- Part 3: Endpoint specification

NIST
National Institute of Standards and Technology

SP800-73 Part 2

- Optional transition path for agencies with existing GSC-IS deployments
- Provided by Government Smart Card Interagency Advisory Board
- Based on commonality of data model
- Will be superceded by endpoint systems at the close of each agency's deployment

SP800-73 Part 3

- Endpoint PIV card application specification
- Tighter than GSC-IS and transition of necessity, to support PIV interoperability
- Mandatory full deployment of Part 3 cards at the end of Phase II
- Reference implementation available
- Conformance test program SP800-85

Part 3 Card Architecture

- PIV card behavior is defined at the card interface (“black box”)
- Internal implementation details are not addressed
- Independent of card platform
  - file system vs. object based
  - Native OS vs. Virtual Machine vs. ?

Card Management Framework

- GSC-IAB Policy Group recommendation
  - No requirement for interoperability of card management systems across agencies
  - Common initial state for mandatory data objects
- Some ‘credential initialization and administration’ functions included at card edge interface
  - PUT DATA
  - GENERATE ASYMMETRIC KEYPAIR
- NISTIR 7284: PIV Card Management Report

PIV Card Data Model (I)

- Five mandatory objects
  - Card Capability Container
  - Cardholder Unique Identifier (CHUID)
  - PKI Certificate for PIV Authentication
  - Cardholder Fingerprint (formerly 2)
  - Security Object (ICAO signed hash table)

PIV Card Data Model (II)

- Five optional data objects:
  - Cardholder Facial Image
  - Printed Information
  - PKI Certificate for Digital Signature
  - PKI Certificate for Key Management
  - PKI Certificate for Card Authentication

Namespace Management

- PIV Registered Application Provider Identifier ‘A0 00 00 03 08’
- Object Identifiers at the PIV Client API
  - PIV subarc of the Computer Security Object Register
- BER-TLV tags at the card interface
- Namespace management white paper on PIV website

Physical Access Control

- All PIV cards contain a CHUID as defined in [PACSv2.2]
- PIV card functionality is restricted to CHUID retrieval in contactless mode
  - Optional Card Authentication Key may also be used
- All agencies must be able to read and parse the CHUID at a minimum – expiration date check

SP800-73-1 Update

- Proposed changes
  - Incorporate Errata
  - Biometrics – SP800-76
  - Remove PIN protection on certificates
  - Stability – No major architectural changes!
- Public comment period closed March 1

Additional Topics

- PIV Data Set Generator
- Migration to ISO 24727
- Contactless interoperability

Contact Details

james.dray@nist.gov: GSC Chief Architect

teresa.schwarzhoff@nist.gov: GSC Standards Program Manager

william.barker@nist.gov: PIV Program Manager

PIV Website: http://csrc.nist.gov/piv-project

NIST
National Institute of Standards and Technology