Changes to SP 800-73

(SP 800-73-4)

Ketan Mehta
NIST PIV Team
NIST ITL Computer Security Division
mehta_ketan@nist.gov

Smart Card Alliance, Government Conference
October 30, 2014

Draft SP 800-73-4

- Removed Part 4, The PIV Transitional Data Model and Interfaces - as discussed with DoD.
- Added Section 1.3 “Effective Date”. This aligns with OMB’s coordinated language in FIPS 201-2.
- Made asymmetric Card Authentication key mandatory.
- Made digital signature key and key management key conditionally mandatory.
- Made the facial image data object mandatory.

Draft SP 800-73-4

- Introduced specifications for optional secure messaging.
- Introduced specifications for optional virtual contact interface over which all non-card-management functionality of the PIV Card is accessible.
- Added support for optional pairing code that is used to establish virtual contact interface.
- Added PIV card level PIN length enforcement requirements for the PINs, pairing code and PUK.

Draft SP 800-73-4

- Made Card UUID mandatory.
- Added optional Cardholder UUID as a cardholder unique identifier.
- Added optional on-card biometric comparison mechanism as a means of performing card activation and as a PIV authentication mechanism.
- Expanded Part 1, Appendix C (PIV Algorithm Identifier Discovery) to include an Algorithm Identifier discovery for Secure Messaging.
- Expanded Part 2, Appendix A (GENERAL AUTHENTICATE examples) to illustrate use of VCI.

Draft SP 800-73-4 Introduces

- Key Establishment Protocol
- Secure Messaging (SM)
- Virtual Contact Interface (VCI)
  - Protocols in SP 800-73-4 are only for non-card-management operations
  - Secure messaging for card management is out-of-scope for SP 800-73-4

Key-Establishment Protocol

- Establishes session keys for SM
- Based on One-Pass Diffie-Hellman – C(1e, 1s, ECC_CDH)
- One-way authentication scheme – card is authenticated by the host
- Any host can establish a secure channel with a card

Secure Messaging

- Uses session keys to:
  - Encrypt (AES-CBC) data fields in commands and responses
  - Integrity protect (cipher-based MAC) command and response data, including status words in response
- Command and responses are protected from integrity of message sequences

On-Card Biometric Comparison Authentication

- Perform VERIFY command with OCC data over SM
- Key-establishment protocol authenticates card
- Encryption protects card holder's biometrics from eavesdroppers
- Integrity protection of response status, combined with response sequencing ensure that "successful execution" response from card can be trusted

Virtual Contact Interface

- Establish Secure Messaging Session
- Optionally, it is strongly recommended, submit Pairing Code using VERIFY command
- Discovery mechanism is provided to find out if the card requires Pairing Code to establish VCI
- Perform any non-card-management operation, just as if communicating over contact interface

Pairing Code

- Protects personally identifiable information from Skimming
- Prevents attacker from locking the PIN
- An optional threshold mechanism is provided to protect against the card from getting locked over contactless interface
- Pairing code is on by default and compensating controls need to be implemented if Pairing Code is not used

Pairing Code (cont'd)

- Provides authorization, not authentication
  - One pairing code per card, shared by all "authorized" hosts
- May be permanently cached on the host system
  - Enter pairing code into a device once
  - Device caches pairing code for life of card and submits it to card whenever a card requires it to establish VCI
- Shall be stored on the card if required for VCI establishment
- Consist of eight decimal digits and it shall be generated at random by the PIV Card Issuer

Thank you

Questions?

Ketan Mehta
NIST ITL Computer Security Division
mehta_ketan@nist.gov