PIV Card Specification Update (SP 800-73-4)

Hildegard Ferraiolo, NIST

PIV Project Lead

Slides by David Cooper

March 3, 2015

Alignment with New Requirements in FIPS 201-2

- All features that are newly mandatory in FIPS 201-2 are fully specified in SP 800-73-3:
  - Card Authentication key and certificate
  - Digital signature key and certificate*
  - Key management key and certificate*
  - Facial image data object
  - Card UUID
- Requirements of FIPS 201-2 can (and shall) be met today, without waiting for SP 800-73-4.

* Only required if cardholder has government-issued email account at the time of credential issuance.

New Requirement in SP 800-73-4

- PIN-length enforcement
  - FIPS 201-2 specifies a minimum PIN length of 6 digits.
  - SP 800-73-3 sets maximum PIN length of 8 digits, but no minimum length
  - Under SP 800-73-4, PIV Cards must prevent PIN from being changed to a value whose length is less than 6 digits
  - New cards will need to implement this under SP 800-85A-4 testing.
- Currently approved cards already implement all other requirements of SP 800-73-4.

New (Optional) Features of SP 800-73-4

- Secure messaging (SM)
- On-card biometric comparison (OCC)
  - Card activation
  - Authentication method (OCC-AUTH)
- Virtual contact interface (VCI)

Secure Messaging

- Key-establishment protocol
  - Uses One-Pass Diffie-Hellman, C(1e, 1s, ECC CDH)
  - Includes key confirmation
- Secure Messaging
  - Data fields of commands and responses are encrypted
  - All command and response data, including status words, are integrity protected
  - Includes protection against replay and message reordering.

On-Card Biometric Comparison

- VERIFY command with fingerprint minutia
- Alternative card activation to PIN
  - Enables use of private keys and reading of non-biometric data objects
- Provides two-factor authentication when performed over secure messaging (SM)
  - Key-confirmation step of key-establishment protocol authenticates card (“something you have”)
  - Authenticated response to VERIFY authenticates cardholder (“something you are”)

Secure Messaging ≠ VCI

Secure messaging serves three purposes:

1. One-factor authentication (SM-AUTH)
   - Alternative to PKI-CAK authentication, but because it is optional SM-AUTH is not a candidate for inter-agency access point
   - Key-confirmation step of key-establishment protocol authenticates card
2. Two-factor authentication (OCC-AUTH)
   - SM-AUTH + OCC over SM
3. Virtual Contact Interface
   - Perform all non-card-management functions of PIV Card Application over contactless interface

Authentication over Contactless Interface

Authentication Mechanism	Interface Requirement	PIN needed?
CHUID, PKI-CAK, SYM-CAK, SM-AUTH	Contactless	✗
OCC-AUTH	Contactless / SM	✗
BIO, BIO-A, PKI-AUTH	VCI	✓

- Any use of PIV Card that requires VCI over contactless interface also requires PIN (or OCC) entry.
- VCI primarily enables card use with mobile devices.

Change from Revised Draft

- Pairing code requirement for VCI can be disabled by issuer
  - Indicated by bit in Discovery Object
  - Requires approval of Designated Approving Authority (DAA)
  - Requires compensating controls to ensure PII (i.e., name, email address and organization) will not be skimmed from the PIV Card when in close proximity when the card is outside its protective sleeve.

Thank you!

Questions?

Hildegard Ferraiolo
PIV Project Lead
NIST ITL Computer Security Division
hildegard.ferraiolo@nist.gov