FIPS 201-2 and NIST Special Publications Update

- Smart Card Alliance Webinar
- November 6, 2013
Today’s Webinar Topics & Speakers

- **Introductions:** Randy Vanderhoof, Executive Director, Smart Card Alliance
- **FIPS 201-2 Update:** Hildegard Ferraiolo, NIST
- **SP 800-73:** Ketan Mehta, NIST
- **SP 800-73 Secure Messaging:** David Cooper, NIST
- **SP 800-157:** Sal Francomacaro, NIST
- **Q&A:** Randy Vanderhoof, Smart Card Alliance
Revision 2 of FIPS 201
(FIPS 201-2)

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

Smart Card Alliance Post Govt Conference Webinar,
November 6, 2013
From FIPS 201-1 to FIPS 201-2

- 2011 – Draft FIPS 201-2 & Workshop
- 2012 – Revised Draft FIPS 201-2 & Workshop
- 2013 – September 5th, FIPS 201-2 published
What is different from FIPS 201-1?
PIV Card Issuer’s Perspective
# PIV Issuer Viewpoint – The Next Gen PIV Card

<table>
<thead>
<tr>
<th>FIPS 201-1 (superseded)</th>
<th>FIPS 201-2 (in effect):</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mandatory</strong></td>
<td><strong>Mandatory</strong></td>
</tr>
<tr>
<td>- PIV Authentication</td>
<td>- PIV Authentication</td>
</tr>
<tr>
<td>- CHUID</td>
<td>- CHUID</td>
</tr>
<tr>
<td>- Biometric (fingerprints)</td>
<td>- Biometric (fingerprints)</td>
</tr>
<tr>
<td><strong>Optional</strong></td>
<td></td>
</tr>
<tr>
<td>- CAK</td>
<td>- CAK</td>
</tr>
<tr>
<td>- Digital Signature Key</td>
<td>- Digital Signature Key</td>
</tr>
<tr>
<td>- Key Management Key</td>
<td>- Key Management Key</td>
</tr>
<tr>
<td>- Facial Image</td>
<td>- Facial Image</td>
</tr>
<tr>
<td></td>
<td><strong>Optional</strong></td>
</tr>
<tr>
<td></td>
<td>- OCC, Biometric (iris)</td>
</tr>
</tbody>
</table>
In Depth Technical Details

- SP 800-73-4 (Revision in process)
- SP 800-78-4 (Revision in process)
- SP 800-76-2 (Revision complete)
- SP 800-85 A / B (Revision in process)
- SP 800-79-2 (Revision TBD)
Compliance Perspective
Effective Date and Implementation Schedule of FIPS 201-2
(as coordinated with OMB)

• **Effective Date:**
  
  “This Standard is effective immediately and supersedes FIPS 201-1 (Change Notice 1). New *optional* features of this Standard that depend upon the release of new or revised NIST Special Publications are effective upon final publication of the supporting Special Publications.”

• **Implementation Schedule:**
  
  “This Standard mandates the implementation of some PIV Card features that were optional to implement in FIPS 201-1. To comply with FIPS 201-2, all new and replacement PIV Cards shall be issued with the *mandatory* PIV Card features no later than 12 months after the effective date of this Standard.”
Relying Party’s Perspective
FIPS 201-2 - A Relying Party’s Viewpoint
Authentication Mechanisms

<table>
<thead>
<tr>
<th>PIV Assurance Level Required by Application/Resource</th>
<th>PACS</th>
<th>LACS Local Workstation Environment</th>
<th>LACS Remote/Network System Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>LITTLE or NO confidence</td>
<td>VIS*, CHUID*</td>
<td>CHUID*</td>
<td></td>
</tr>
<tr>
<td>SOME confidence</td>
<td>PKI-CAK, SYM-CAK</td>
<td>PKI-CAK</td>
<td>PKI-CAK</td>
</tr>
<tr>
<td>HIGH confidence</td>
<td>BIO</td>
<td>BIO</td>
<td></td>
</tr>
<tr>
<td>VERY HIGH confidence</td>
<td>BIO-A, OCC-AUTH, PKI-AUTH</td>
<td>BIO-A, OCC-AUTH, PKI-AUTH</td>
<td>PKI-AUTH</td>
</tr>
</tbody>
</table>

Yellow font constitutes a change from FIPS 201-1.

* Downgraded to Little or No Confidence (LoA-1)

• Signature validation required on all signed credentials (i.e., BIO, BIO-A, CHUID, Certs….)
• Underlined: Authentication methods suitable for inter-agency use – all PIV cards have (or will have) the credential associated with authentication method on-card.
In Depth Technical Details .....  

- SP 800-116 (Revision TBD)  
- SP 800-73-4 (Revision in process)  
- SP 800-78-4 (Revision in process)  
- SP 800-76-2 (Revision complete)
FIPS 201-2

PIV Card Interface:
Contact, Contactless and now optionally virtual contact interface
– Technical Details in SP 800-73-4, SP 800-78-4, SP 800-85A-2

Form Factor:
• PIV Card remains mandatory
• Optionally derived PIV credentials on mobile device to enable remote IT access with mobile.
  - Technical Details in SP 800-157 (new), SP 800-166 (new)
FIPS 201-2

- Optional Chain-of-Trust and Grace Period for PIV card reissuance processes  (Technical details in SP 800-156 (new), SP 800-79 )
- Relaxation of PIV Card termination requirements and specifically certificate revocation  (Technical details in SP 800-79 )
- Facial image match as option for 1:1 match at re-issuance,
- New options for physical card characteristics to help agencies achieve Section 508 compliance for PIV card orientation,
- A UUID as a mandatory unique identifier for the PIV Card.  (Technical details in SP 800-73-4 )
HSPD #12
PIV Document Relationships

HSPD 12
(Presidential)

FIPS 201-2
(Secretary of Commerce)

SP 800-73-4
Public draft: May ‘13

SP 800-78-4
Public draft: May ‘13

SP 800-76
2 draft is done

SP 800-79
Draft update initiated

SP 800-116
TBD

SP 800-87
(NIST)

SP 800-96
To commence

SP 800-156
Chain of Trust
Draft update initiated

SP 800-157
PIV Derived Credentials
Public draft - TBD

SP 800-85A
Draft update initiated

SP 800-85B
Draft update initiated

SP 800-166
PIV Derived Credentials TEST REQUIREMENT
Public draft - TBD

New SPs
Driver

revision in process
revision complete

Supporting Special Publications

Test Guidelines

Standards
FIPS 201-2 Revision Team:

From A to Z:

- Ramaswamy Chandramouli – PIV Validation and Accreditation
- David Cooper – PIV Cryptographic Capabilities
- Hildegard Ferraiolo – PIV Program Lead and PIV Card Capabilities
- Salvatore Francomacaro – Change Management
- Patrick Grother – PIV Biometrics
- Ketan Mehta – PIV Authentication Mechanisms
- Annie Sokol – Visual PIV Card Topology
Final FIPS 201-2 Released

• Announce Final FIPS 201-2 with Federal Register Notice

• Publish Final FIPS 201-2 at csrc.nist.gov

• Publish public comments and resolutions
  – 2011 Draft comments:
  – 2012 Draft comments
Standards - FIPS 201-2

Working together = close alignment. Are all parties equally satisfy?

- NIST received 1,800+ comments during the revision including:
- U.S. federal government organizations,
- State government organizations,
- Private sector organizations, and
- Private individuals

Thank you!
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 Post Govt Conference Webinar,
November 6, 2013
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.
NIST Special Publication
800-73-4 Secure Messaging Capabilities

David Cooper
Computer Security Division
NIST ITL
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)
- Card-to-host authentication only
- Any host can establish a secure channel with a card
  - even hosts that shouldn't be trusted
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 response chaining used to protect 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 words, combined with response chaining ensures that "successful execution" response from card can be trusted
Virtual Contact Interface

Contact (Wire) Channel

RF Channel
Encrypted Channel
Virtual Contact Interface

1) Establish secure messaging
2) Submit pairing code using VERIFY command
3) 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
Pairing Code

- Provides authorization, not authentication
  - One pairing code per card, shared by all “authorized” hosts
- May be permanently cached
  - Enter pairing code into a device once
  - Device caches pairing code for life of card and submits it to card whenever a VCI is needed
## Access Rules

<table>
<thead>
<tr>
<th></th>
<th>Contactless</th>
<th></th>
<th>Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No SM</td>
<td>SM</td>
<td>VCI (SM + pairing code)</td>
</tr>
<tr>
<td>Read CHUID</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Read Card Auth Cert</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Use Card Auth Key</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Read other X.509 Certs</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Use other private keys</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Read biometric data</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>VERIFY PIN</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>VERIFY OCC</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>PUT DATA</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
FIPS 201-2 and Mobility
(SP 800-157 - Derived PIV Credentials)

Sal Francomacaro
NIST PIV Team
NIST ITL Computer Security Division
salfra@nist.gov

Smart Card Alliance Webinar,
November 6, 2013
“Mobile Revolution”

- **Always-on, Always-connected**
- Rapid innovation driven by intense competition and consumer demand
- Different constraints, abilities than desktop/laptop computers
- More and more Federal systems accessed by mobile devices, increasing need for strong assurance of identity
FIPS 201-2 and Mobility

FIPS 201-2 recognizes and directly supports new Mobility trends:

“Valid PIV Cards may be used as the basis for issuing derived PIV credentials in accordance with NIST Special Publication 800-157, Guidelines for Derived Personal Identity Verification (PIV) Credentials”

While SP 800-157 will provide guideline on Derived PIV credential, it will not preclude the use of different technique (i.e. NFC) for the Mobile PIV ecosystem
The scope of the Derived PIV Credential guideline is to provide PIV-enabled authentication services for high-level applications on the mobile device to authenticate the credential holder to remote systems.

The guideline specifies the use of tokens with alternative form factors to the PIV card that may be inserted into mobile devices.
SP 800-157 - Derived PIV Credentials

• Derived PIV Credentials are based on the general concept of derived credential in SP 800-63

• Identity proofing and vetting processes do not have to be repeated to issue a Derived PIV Credential

• Possession of a valid PIV card is the basis to issue derived PIV credential for mobile devices
SP 800-157 - Derived PIV Credentials

• The guideline specifies and supports both LOA-3 and LOA-4 Derived PIV Credentials
• The guideline doesn’t preclude the issuance of multiple Derived PIV Credentials to the same Applicant on the basis of the same PIV Card
• The Derived PIV Credential is unaffected by loss, theft or damage to the Subscriber’s PIV Card
SP 800-157 - Derived PIV Credentials

- Derived credentials may be issued to a variety of cryptographic tokens available for use on mobile devices. These tokens may be hardware or software-only implementations.

- Federal PKI Policy Authority will issue fpki common policies for both LOA-3 and LOA-4 Derived PIV Credential.
SP 800-157: Cryptographic Token Types

- SD Memory card*
- USB token*
- UICC (next Gen SIM card)
- Embedded Hardware secure element
- Software token

* With an embedded HW crypto controller
PIV and Mobility: A different approach than Derived PIV Credentials

Near Field Communication (NFC)

- A mobile device, that supports the Near Field Communication (NFC) capability, can directly interact with the PIV card contactless interface
- The user would need to hold or place the card next to the mobile to initiate the interaction between PIV card and Mobile device
- FIPS 201-2 and Draft SP 800-73-4 specifications have introduced the concept of Virtual Contact Interface (VCI) to support this contactless scenario.
Questions & Answers
• Randy Vanderhoof, rvanderhoof@smartcardalliance.org
• Hildegard Ferraiolo, hildegar.ferraiolo@nist.gov
• Ketan Mehta, ketan.mehta@nist.gov
• David Cooper, david.cooper@nist.gov
• Sal Francomacaro, salvatore.francomacaro@nist.gov

Smart Card Alliance
191 Clarksville Rd. · Princeton Junction, NJ 08550 · (800) 556-6828
www.smartcardalliance.org