

Update of NIST PIV Standards and Specifications

Hildegard Ferraiolo

PIV Project Lead

NIST ITL Computer Security Division

hildegard.ferraiolo@nist.gov

Smart Card Alliance, Government Conference

October 30, 2014

NIST FIPS 201 Standards and Specifications

- 9/2013 -- Publication of FIPS 201-2 – The PIV Standard
 - 12 month implementation timeline
- 9/2014 Issuance of FIP 201-2 PIV Cards
 - Include the previous optional (now mandatory) features on PIV Card. (These types of cards have been available for a while).
 - Issuer Accreditation:
 - No action if accredited under SP 800-79-1 that include controls for previous optional (now mandatory) features of PIV Card
 - Otherwise use –SP 800-79-1 / -2 to include control for previously optional (now mandatory) PIV Card features
 - 3 year re-authorization cycle: Use SP 800-79-2
 - Moved Non-Compliant PIV Card Applications and PIV Middleware to Removed Products List (RPL) at NIST PIV Validation site.

NIST FIPS 201 Standards and Specifications

- 5/14 – Published Revised Draft SP 800-73-4 PIV Card Application, PIV Middleware and associated interfaces
 - Goal: To add new optional features specified in FIPS 201-2 (Secure Messaging, VCI, OCC, Iris)
 - **Final Publication targeted before End of 2014**
 - Published with Final SP 800-78-4 (PIV Cryptographic Specification)
- 8/14 -- Published Draft SP 800-85B-4, *PIV Data Model Test Guidelines*
 - Goal: To include test cases for new optional credentials/Data Object introduced in SP 800-73-4 (OCC, iris. Pairing Code Reference Data, etc.)
 - FIPS 201-2, SP 800-73-4 DERIVED Test Requirements for PIV Card Credentials/Data Model

NIST FIPS 201 Standards and Specifications

- Draft SP 800-85A: Derived PIV Card Application and PIV Middleware Test Requirements
 - Goal: To include test cases to exercise new optional functionality introduced in FIPS 201-2 and SP 80073-4 (VCI, SM, OCC, iris, PIN length enforcement among others)
 - **Targeted to be published shortly after SP 800-73-4 is final**
- NIST Validation Program (PIV Card Application and Middleware)
 - Update to Test Runner is initiated
 - To be distributed to 3rd Party NPIVP Laboratories once complete
 - SP 800-73-4-based (new optional features) testing in approx. late 2015

NIST FIPS 201 Standards and Specifications

- 7/2014 -- Published draft SP 800-79, *Guidelines for the Accreditation of Personal Identity Verification (PIV) Card Issuers (PCIs)*.
 - Goal 1: To include issuer controls for new optional features introduced in FIPS 201-2 (grace period, pseudonymous identity, post-issuance updates, chain of trust, among others)
 - Goal 2: To include a new set of issuer controls for Derived PIV Credentials Issuers

NIST FIPS 201 Standards and Specifications

- **Draft SP 800-157, Guidelines for Derived Personal Identity Verification (PIV) Credentials**
 - Contains the technical details for implementing and deploying derived PIV credentials on mobile devices, such as smart phones and tablets.
 - **Target FINAL publication: November 2014**
- **Draft NIST IR 7981, Mobile, PIV, and Authentication,**
 - analyzes and summarizes various current and near-term options for remote authentication with mobile devices that leverage both the investment in the PIV infrastructure and the unique security capabilities of mobile devices.
 - **Target FINAL publication date: November / December 2014**
- **Draft SP 800-166 Derived PIV Credential Test Requirements**
 - Specifies derived test requirements for the Derived PIV Credential and its security token (Data Model and Interfaces)
 - Portability: Removable security tokens (USB, SD, UICC) should be portable from one device to another.

New Work Items to Begin in 2015

- Draft SP 800-116-1
 - *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*
- Draft SP 800-156
 - *Representation of PIV Chain-of-Trust for Import and Export*
- Draft SP 800-96-1
 - *PIV Card to Reader Interoperability Guidelines*

Thank you

Questions?

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