FIPS 201-2 Workshop

NIST PIV Team

National Institute of Standards and Technology
US Department of Commerce

Gaithersburg, MD
April 18 – 19, 2011

OVERVIEW

Overview

- Goals and format of the workshop
- The FIPS 201-2 PIV Team
- Revision Process
- Summary of proposed Changes

Workshop Goals and Format

Goals

- Introduce Draft FIPS 201-2
- Elicit Questions, Comments and Feedback
- Note: Official comments via piv_comments@nist.gov

Format

- For each topic, we present the changes first
- Followed by QA/Feedback from participants (on-site or from webcast)

The PIV Team

- William MacGregor, Program Manager
- David Cooper – PIV Cryptographic Capabilities
- Ketan Mehta – FIPS 201-2 Editor
- Patrick Grother – PIV Biometrics
- Salvatore Francomacaro – Change Management
- Annie Sokol – Visual PIV Card Topography
- Ramaswamy Chandramouli: PIV Validation and Accreditation
- Hildegard Ferraiolo – PIV Card Capabilities

PIV REVISION PROCESS

FIPS 201 History and Excerpts

- **February 2005**: FIPS 201 published
- **March 2006**: FIPS 201-1 Change Notice 1

Because a standard of this nature must be flexible enough to adapt to advancements and innovations in science and technology, the NIST will review this standard within five years to assess its adequacy.”

- FIPS 201-1, p. vi

- **February 2010** – The 5 year anniversary

Revision Process

- We determine a revision necessary based on:
  a. comments received during the 5 years from USG and industry
  b. Business Requirement Meeting
  c. standards based technology advancements
- We prepared Draft FIPS 201-2 to include a), b), c)

Revision Process

- March 8th 2011, announced Draft FIPS 201-2 with a Federal Register Notice including Summary of Change and the announcement of this workshop
- At the same time, published Draft FIPS 201-2 at NIST website (http://csrc.nist.gov/publications/PubsFIPS.html)
- comment period 90 day, ending June 6th
- Today: Holding a workshop April 18th &19th 2011

Next Revision Steps

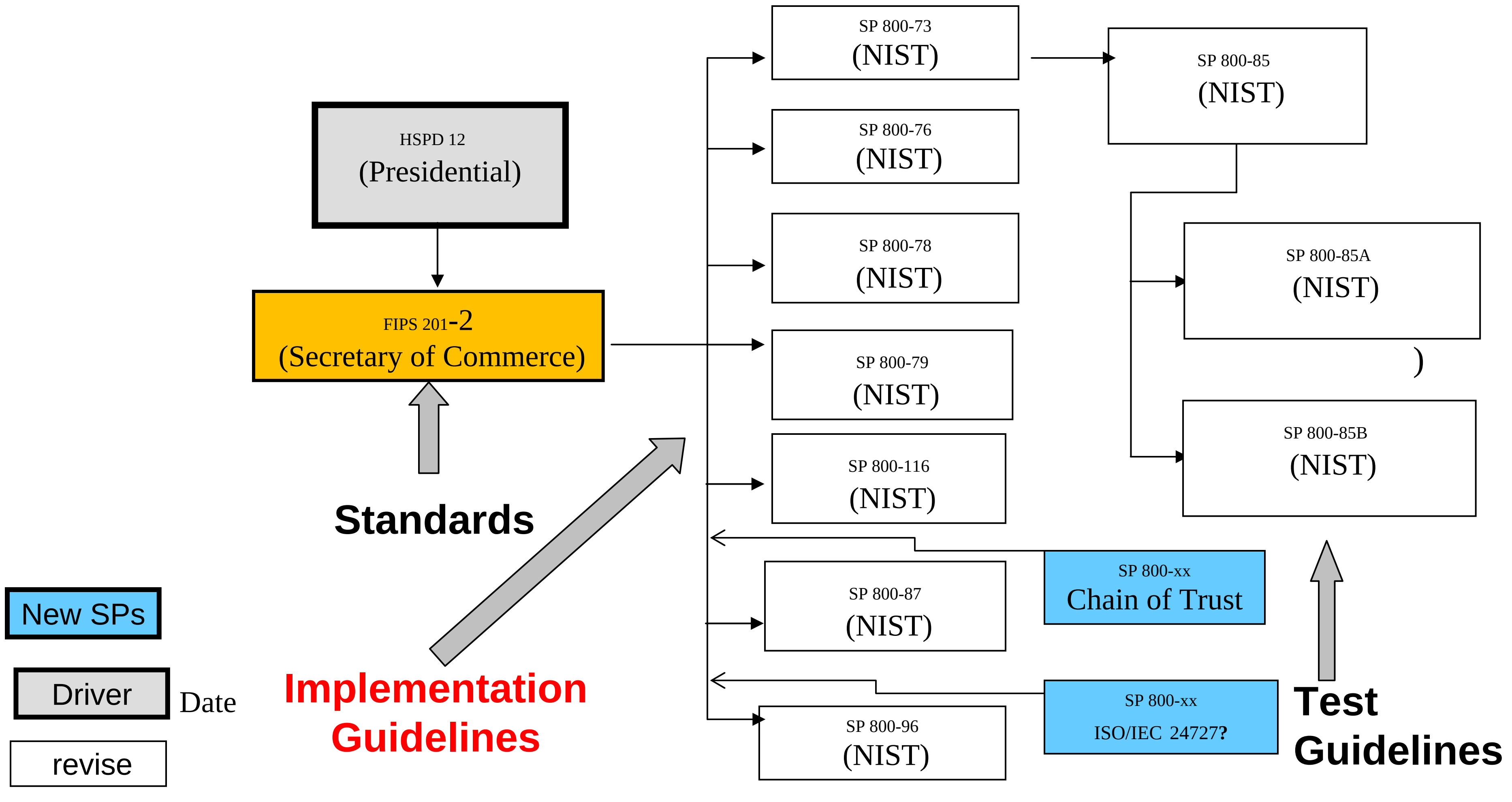
- After June 6th, NIST will start the comment resolution period
- Prepare Final FIPS 201-2
- Promulgate Final FIPS 201-2 to the Secretary of DoC for approval and signature
- Announce Final FIPS 201-2 with Federal Register Notice
- Publish Final FIPS 201-2 at csrc.nist.gov
- Publish public comments and resolution

Next Revision Steps

- FIPS 201-1 is superseded / retired
- The new standard in effect is FIPS 201-2

- Wait, there is more….

HSPD #12
PIV Document Relationships



HSPD 12
(Presidential)

FIPS 201-2
(Secretary of Commerce)

Standards

Implementation Guidelines

SP 800-73
(NIST)

SP 800-76
(NIST)

SP 800-78
(NIST)

SP 800-79
(NIST)

SP 800-116
(NIST)

SP 800-87
(NIST)

SP 800-96
(NIST)

SP 800-xx
Chain of Trust

SP 800-xx
ISO/IEC 24727?

SP 800-85
(NIST)

SP 800-85A
(NIST)

)

SP 800-85B
(NIST)

Test Guidelines

New SPs

Driver

Date

revise

Summary of Proposed Changes

A “Top Ten” List of Proposed Changes

……(there are more…)

Top 10 #1

The asymmetric Card Authentication Key is now Mandatory

4 Used in 1 Factor authentication for Physical access control – to access federal buildings and facilities

4 It is used over the card’s contactless interface (touch and go).

4 By making this Card Authentication Key mandatory, it can be deployed government-wide in an interoperable manner

4 Better alternative to the CHUID, which can be sniffed / copied and replayed.

Top 10 -- #2

Introduction of enrollment record (Chain of Trust)

- Maintained by issuer and contains the documentary evidence of identity proofing, Background Investigation (BI) and the biometric data
- Enables cardholder to re-connect to the record by matching against the record’s fingerprint.

  4 Eliminates complete re-enrollment for lost, stolen, compromised card.

  4 Eliminates recapturing biometrics -- use the record’s biometric instead to personalize the card.

  4 BI status: repeating BI in the event of a lost, stolen, or damaged card is not needed.

Top 10 -- #3

Iris Recognition:

- Included iris biometric to re-connect to the enrollment record, when fingerprints cannot be enrolled with issuer
- At the same time, included iris as an optional authentication method

Top 10 -- #4

Standards based technological advancements:

In 2005, some open standards were promising, but immature. Now, these standards are mature and thus incorporated in Draft FIPS 201-2 draft.

- Added optional On Card Biometric Comparison (OCC) authentication
- The cardholder's fingerprint biometric representation is captured by the reader and transferred to the card, where it is matched against the cardholder's stored biometrics.
- OCC also enabled as an optional Card activation mechanism in addition to PIN –based card activation.

Top 10 -- #5

Option to support of ISO/IEC 24727

Added ISO/IEC 24727 based standards technology to improve reader resilience and flexibility.

ISO/IEC 24727 offers a suite of authentication mechanisms used be used in a consistent and repeatable manner for Identification, Authentication and signature (IAS) application with a smart cards.

4 We are also interested in ISO/IEC 24727 for the secure Channel feature, for example to secure communication between the card-to-PC or PIN-pad-to-PC paths. (needed for on card comparison)

Top 10 -- #6

Add optional feature for card orientation

4 *To comply with Section 508* of the Rehabilitation Act

4 strives to make electronic and information technology accessible to people with disabilities

4 Improved usability of the card for visually challenged cardholder

4 The card now has orientation features to help orientate the card to insert it in the card reader the correct way

Top 10 -- # 7

Extend the maximum length of the printed name

4 Eliminate name truncation, if possible, and the resulting irritation and inaccuracies that result.

Top 10 -- # 8

Add online Background Investigation (BI) verification and remove on-card NACI Indicator

4 Once there is a government-wide, online BI status service, the NACI Indicator can become optional and deprecated, as advised by OMB.

Top 10 -- #9

Enabled remote post issuance update to the PIV Card in cases where none of the printed information on the surface of the card is changed.

Top 10 -- #10

Bring I-9 Identity Source Document specifications into FIPS 201-2:

- Define the permitted combinations of I-9 Identity Source documents in FIPS 201-2, reducing confusion and mistakes.

Thank you

Hildegard Ferraiolo

hferraio@nist.gov