# UPDATES ON THE PERSONAL IDENTITY VERIFICATION STANDARDS

**David Cooper**
**Hildegard Ferraiolo**

Computer Security Division
NIST ITL

INFORMATION SECURITY AND PRIVACY ADVISORY BOARD Meeting
NIST, Gaithersburg,
May 31th , 2012



National Institute of Standards and Technology

## 2011

**March** Publication of Draft FIPS 201-2

**April** Draft FIPS 201-2 workshop

**June** End of public comment period

- 1K+ comment received from Federal Departments and Agencies, Industry, Private Sector

## 2012

**April** Completed Comment Resolution

**May** Finished Drafting Federal Register Notice to Announce Revised Draft for Public Comments

**July** Estimate for publishing Revised Draft and hold the Revised Draft FIPS 201-2 Workshop (**July 25th**)

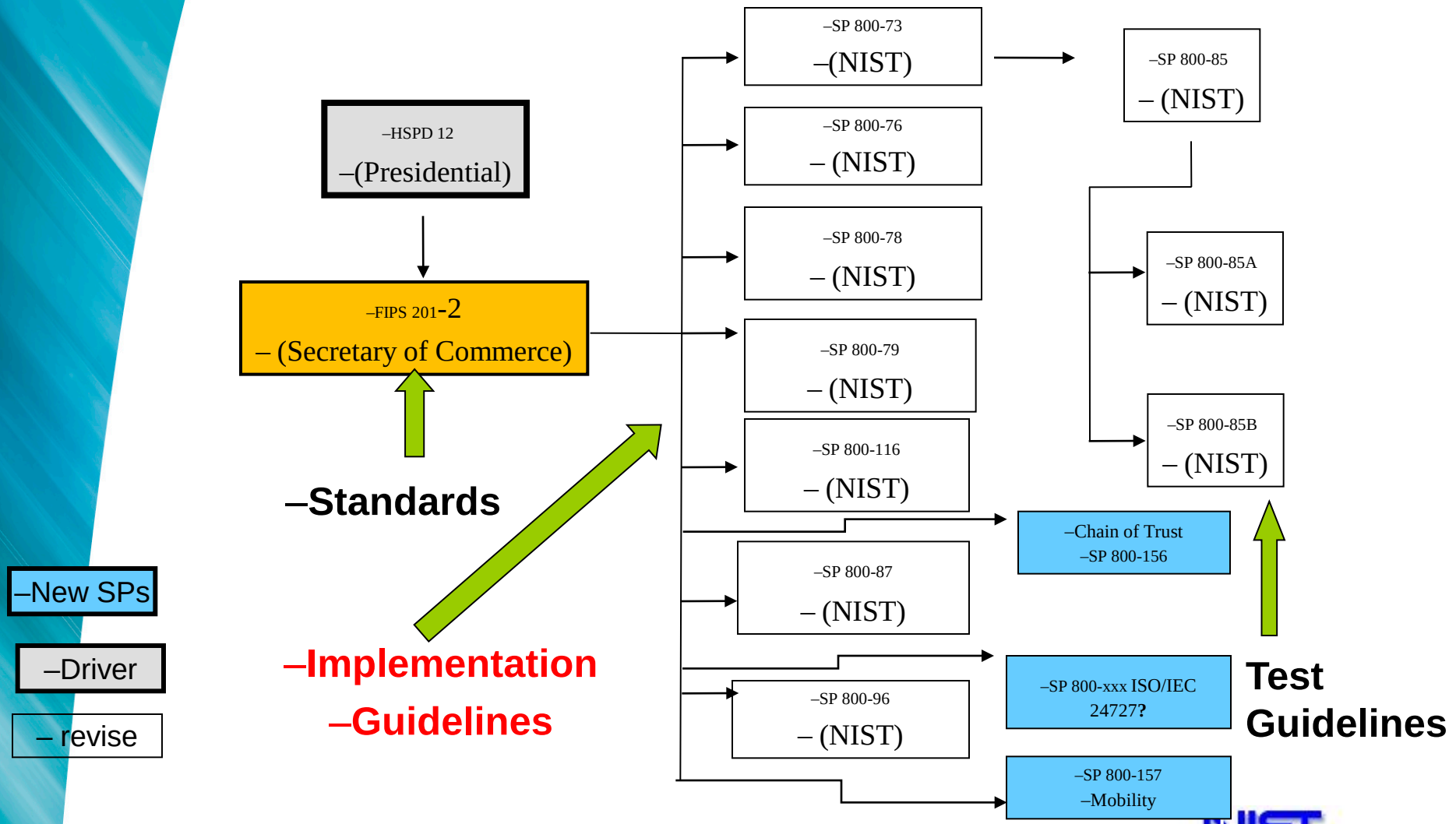
**Aug.** End of public comment period

2012 2013?

# Next Steps…

- Resolve Comments on 2nd Draft FIPS 201-2
- Deliver Candidate FIPS 201-2 to the Secretary of Commerce for consideration
- Announce Final FIPS 201-2 with Federal Register Notice
- Publish Final FIPS 201-2 at csrc.nist.gov
- Publish public comments and resolutions

# HSPD #12
# PIV Document Relationships




National Institute of Standards and Technology

# Representative samples of Received Comments and FIPS 201-2 Revised Draft Walk-through

**categorized by:**

**Clarifications**

**New Requirements**

**New Options and Deprecations**

**The following is not the complete set of changes.**

# PIV-I Cards instead of PIV Card

*Comment*: Federal agencies should be permitted to register PIV–I credentials in lieu of issuing PIV credentials provided that attributes such as successful completion of a NACI can be electronically validated.

HSPD-12 states: "secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees)."

PIV–I credential, as an alternative to issuing a PIV Card, is not consistent with HSPD-12.

# Clarification: Effective Date

- *Comment*: Guidance is needed to distinguish which version of FIPS 201 was used to issue a given card. Guidance is also needed on the adoption/migration of new features.
  - *SP 800-73 will specify PIV card versions and/or discovery mechanism for new features*
  - *New features become effective once specified in the associated NIST Special Publication*
  - *OMB* will provide *transition / compliance timetable for features that have become mandatory.*

# New Requirement: PCI Review

- To enhance the trustworthiness of the PIV Card the Revised Draft FIPS 201–2 requires an independent review of the PIV Card Issuer accreditation.

# New Option: Chain-of-Trust

One or more previous cardholder enrollment records (including status of BI –NACI init/complete?) linked/chained via 1:1 biometric match

- Re-use of record to personalize PIV Card at issuance, renewal, re-issuance
  - Re-connect to record via 1:1 biometric match or
  - When biometric match cannot be performed: ID proof with the PCI operator, comparing facial image enrollment image (or new Card) with ID documents and cardholder
  - Eliminates need to re-enroll (identity proofing and registration process)

# Clarification: Renewal / Reissuance

*Comment*: The difference between reissuance and renewal of PIV Cards is unclear.

•Revised Draft FIPS 201-2 specifies:

- *Renewal:*
  - *The PIV card is valid (uncompromised, not revoked nor expired)*
  - *The cardholder is in possession of the PIV card*
- *Reissuance:*
  - *The PIV card is lost, stolen, compromised*
  - *Logical credentials on-card are compromised*

# New Option: Issuance/Reissuance/Renewal

*Comment*: The proposed requirement to implement the iris biometric, as an alternative for individuals from whom fingerprints cannot be collected, is an undue burden. The 2011 Draft is also unclear about how to address applicants from whom neither fingerprints nor iris images can be obtained.

•Revised Draft FIPS 201-2 specifies:

- 1:1 biometric match with iris biometric is optional
- New feature: When an automated biometric match cannot be performed operator compares enrolled image with ID documents and cardholder

# New Option: Secure Messaging

Comments: Secure messaging capability should allow all functionality of the PIV Card to be accessible over the contactless interface of the card.

- *Revised Draft FIPS 201-2 introduced "virtual contact interface" over which all functionality of the PIV Card is accessible.*

# Biometrics for Authentication

Status Quo (FIPS 201):

- *Two fingerprint templates stored on-card and used for off-card comparison*

- **New Requirements**:
  - *Required on-card electronic facial Image stored on card and used for off-card comparison in operator-attended environment.*
- **New Option:** for electronic storage on-card:
  - *Iris image and*
  - *Biometric on-card comparison*

# New Requirement: Digital Signature Key And Key Management Key

Status Quo (FIPS 201-1):

- The digital signature key and key management key are optionally implemented on-card to support signature and encryption schemes.

**New Requirement**:

Digital signature key and key management key are proposed to be mandatory* in support of the FICAM Roadmap.

- *if the cardholder has a government-issued email account at the time of credential issuance

# New Requirement: UUID

*Comment*: The Universally Unique Identifier (UUID) must be mandatory for interoperability between PIV and PIV–Interoperable (PIV–I) ecosystems.

•Revised Draft FIPS 201–2 specifies the UUID as a mandatory unique identifier for the PIV Card (in addition to the FASC-N).

# Downgrade: CHUID and VIS AuthN

- CHUID and VIS AuthN do not provide LoA 2 “SOME assurance”.

  *CHUID and VIS AuthN will be downgraded in FIPS 201-2 to LoA 1 LITTLE to NO assurance.*

  *-CHUID AuthN proposed to be eliminated in FIPS 201-3*

  ***Note: The CHUID data object remains on-card for PACS ACL Privileges Look-up.***

## New Requirement: CAK (Card Authentication Key & Credential)

- The ‘Alternative’ to CHUID AuthN
- Required CAK credential to be stored on-card
- Available as interoperable interagency AuthN for PACS at “SOME” assurance (PKI-CAK)

# New Option: PIN Reset

*Comment*: Federal agencies should be able to perform PIN resets without requiring cardholders to appear in person before a card issuer.

Status Quo (FIPS 201-1)

In Person or Kiosk-based resets

Revised Draft: Status Quo plus:

- ***New:*** Remote PIN reset Procedure

# New Option: PIN Reset (continued)

PIN reset in the General Computing Environment (desktops, laptops…etc)

*1) cardholder initiates PIN reset with the issuer operator*

*2) operator authenticates PIV cardholder through an out-of-band authentication procedure (e.g., pre-registered knowledge tokens); and*

*3) Cardholder matches live scan with stored biometric through a 1:1 on-card comparison.*

•Remote PIN reset operation via secure mutually authenticated post issuance updates with CMS

.

# Topography

- *Comment*: Information about card topography is currently split between the 2011 Draft and NIST Special Publication 800–104, *A Scheme for PIV Visual Card Topography*. It would be clearer if all of this information is consolidated in one document.

- Revised Draft specifies:
  - *New Requirement: employee affiliation color-coding*
  - *New Requirement: large expiration date in the upper right-hand corner of the card*
  - *Option: Federal Emergency Response Official designation restricted to the bottom of the card*
  - *Option: Country of Citizenship, if implemented located in the bottom of the card*
  - *I-9 list of Identity Source document*
  - *SP 800-104 to be withdrawn.*

# Mobility

*Comment*: In order to accommodate the federal government's movement towards mobile devices, the standard needs to permit other form factors apart from the current ISO/IEC 7816 (credit-card) form factor.

Revised Draft FIPS 201-2:

•Continues to require every cardholder to be issued PIV Card, but

- *Recognizes mobile devices as an <u>additional</u> computing environment for accessing PIV-enabled applications.*
- *<u>Goal</u>: Maintain HSPD-12's 'common identification' (a set of common credentials) and support OMB-11-11 guidance with mobile devices*

# PIV Derived Credentials

- HSPD-12's "**Common Identification**" on mobile devices:
  - *"A set of common credentials on mobile devices"*
  - *Created by agencies' issuance systems (MDMs) for their employees/contractors' mobile devices*
  - *Omits FIPS 201-2 "identity proofing" (SP800-63-1 Derived credential concept – issuer of derived and primary credential is the same entity)*
    - *Cardholder demonstrates possession and control of card (remotely authenticates) -> agency can provision up to LoA 3 PIV derived credentials*
    - *Cardholder demonstrates possession of card and appears in-person → agency can provision up to LoA 4 PIV derived credentials*

# Question?

Thank you!