Interagency Advisory Board

Meeting Agenda, Wednesday, April 24, 2013

1. **Opening Remarks**

2. **A Security Industry Association (SIA) Perspective on the Cost and Methods for Migrating PACS Systems to Use PIV and PKI as Relying Parties** *(Steve Van Till, SIA)*

3. **Update on FIPS 201-2 and Associated Publications** *(Hildy Ferraiolo NIST)*

4. **What the SCA is Doing to Increase Adoption of Strong Credentials - Government ID Training, PIV-I Implementation, and Interoperable Credentials** *(Panel Discussion of SCA membership)*

5. **Closing Remarks**

An Update on FIPS 201 and Associated Special Publications

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

IAB
April 24th, 2013

FIPS 201 History and Projection

- 2011 –Draft FIPS 201-2 & Workshop
- 2012 – Revised Draft FIPS 201-2 & Workshop
- 2013 – Estimate for publishing final FIPS 201-2

2012 2013

Next Steps…

- Done: Resolve Comments on 2nd Draft FIPS 201-2 and produce Candidate Final FIPS 201-2
- Almost Done: Approval Package
- Deliver Candidate FIPS 201-2 to the Secretary of DoC for consideration
- Announce Final FIPS 201-2 with Federal Register Notice (FRN ready and approved)
- Publish Final FIPS 201-2 at csrc.nist.gov
- Publish public comments and resolutions

Candidate Final FIPS 201-2

What is different* from FIPS 201-1 (Standard in Effect)?

* A partial list of differences

PIV Data Model / Credentials

FIPS 201-1

Mandatory

- PIV Authentication
- CHUID
- Biometric (fingerprints)

Optional

- CAK
- Digital Signature Key
- Key Management Key,
- Facial Image

Candidate Final FIPS 201-2:

Mandatory

- PIV Authentication
- CHUID
- Biometric fingerprints)
- asymmetric CAK
- Digital Signature Key,
- Key Management Key
- Facial Image

Optional:

- OCC, Biometric(iris), symmetric CAK

Candidate Final FIPS 201-2 Authentication Mechanisms

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

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

•Yellow font constitutes a change from FIPS 201-1.

•Underlined: Authentication methods suitable for inter-agency use – all PIV cards have (or will have) the credential (associated with authentication method) on-card.

•Signature validation required on all signed credential (i.e., BIO, BIO-A, CHUID, Certs….)

Candidate Final FIPS 201-2

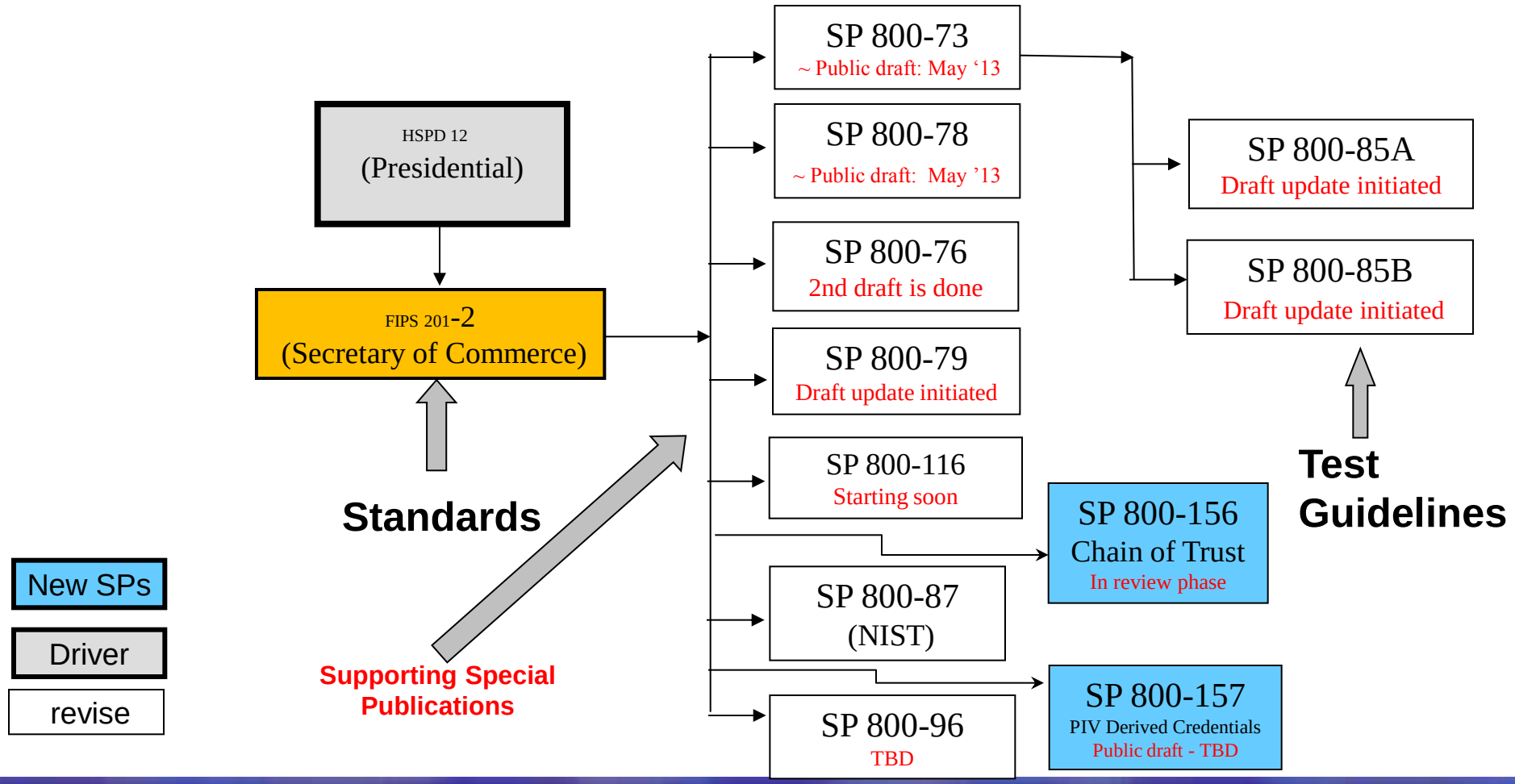
PIV Card Interface:

Contact, Contactless and now optionally virtual contact interface (VCI) and SM

Form Factor:

- PIV Card remains mandatory
- Optionally derived PIV credentials on mobile device to enable remote IT access with mobile.

HSPD #12
PIV Document Relationships



Questions (?)

Thank you!

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