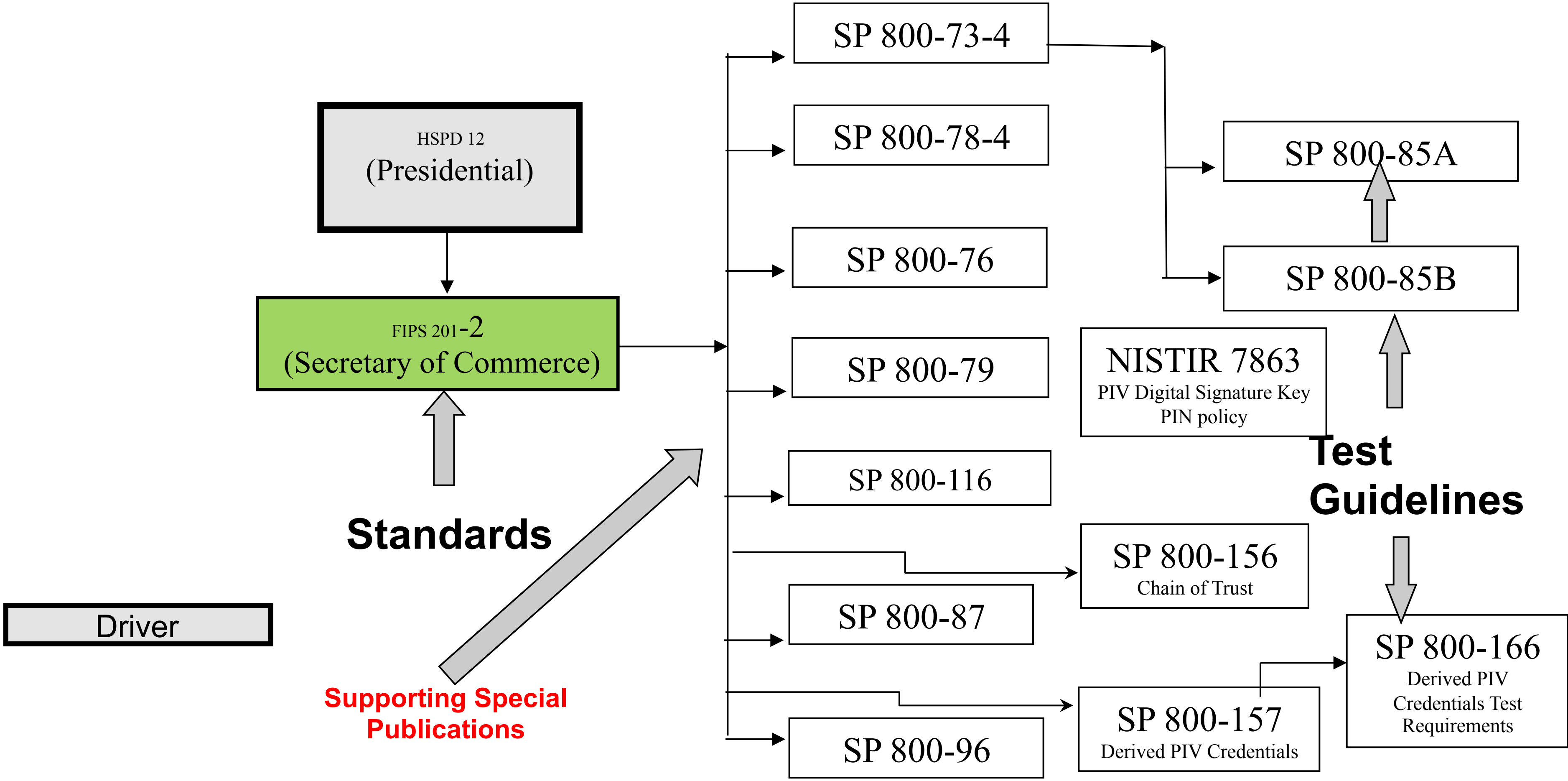
Revision 2 of FIPS 201

and its Associated Special Publications

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

IAB meeting,
December 4, 2013

FIPS 201-2 and Associated Special Publications (SPs)

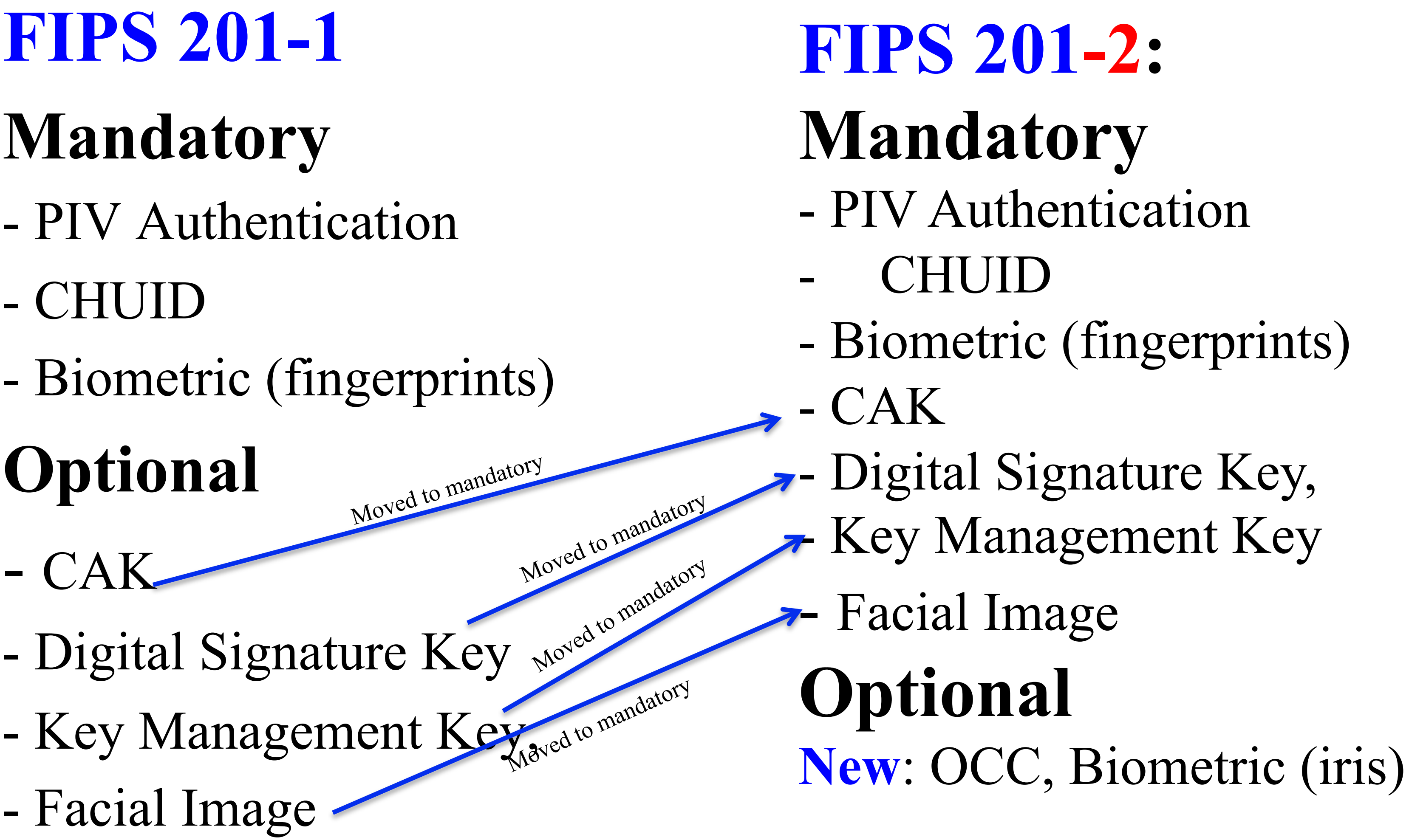


2013

- September 5th, FIPS 201-2 was approved and published
- May 13th, published drafts SP 800-73-4 and SP 800-78-4 for public commenting
- July 2013, published final SP 800-76-2

A Roadmap to Aligning Special Publications with FIPS 201-2

The Next Generation PIV Card



FIPS 201-1

Mandatory

- PIV Authentication
- CHUID
- Biometric (fingerprints)

Optional

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

FIPS 201-2:

Mandatory

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

Optional

New: OCC, Biometric (iris)

PIV Card Interfaces: Contact, Contactless and **new** optional Virtual Contact Interface (VCI)

In Depth Technical Details …..

- SP 800-73-4 *Interfaces for PIV (Parts 1-3)*
- SP 800-78-4 *Cryptographic Algorithms and Key Sizes for PIV*
- SP 800-76-2 *Biometric Data Specification for PIV*
- SP 800-85B-2 *PIV Data Model Conformance Test Guidelines*
- SP 800-85A-3 *PIV Card Application and Middleware Interface Test Guidelines*
- SP 800-79-2 *Guidelines for the Accreditation of PIV Card Issuers (PCI's)*

FIPS 201-2 Alignment in Associated SPs:
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

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 *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems*
  SP 800-73-4 *Interfaces for PIV*
- SP 800-85A-3 *PIV Card Application and Middleware Interface Test Guidelines*
- SP 800-85B-2 *PIV Data Model Conformance Test Guidelines*

FIPS 201-2 Alignment in SPs

PIV Card Interface:

Contact, Contactless and now optionally Virtual Contact Interface(VCI)

- VCI use case:
  - A mobile device's protected interaction (authN, sign, decrypt) with the PIV card's contactless interface using Near Field Communication (NFC)
  - Expanded contactless use-cases in PACS / LACS applications
- Security is important – VCI's secure messaging feature is being evaluated and vetted through NIST, NSA as well as the public comment processes.
- In Depth Technical Details in….
  - SP 800-73-4, SP 800-78-4, SP 800-85A-2
  - NOT covered in SP 800-157

FIPS 201-2 Alignments in SPs

Form Factor:

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

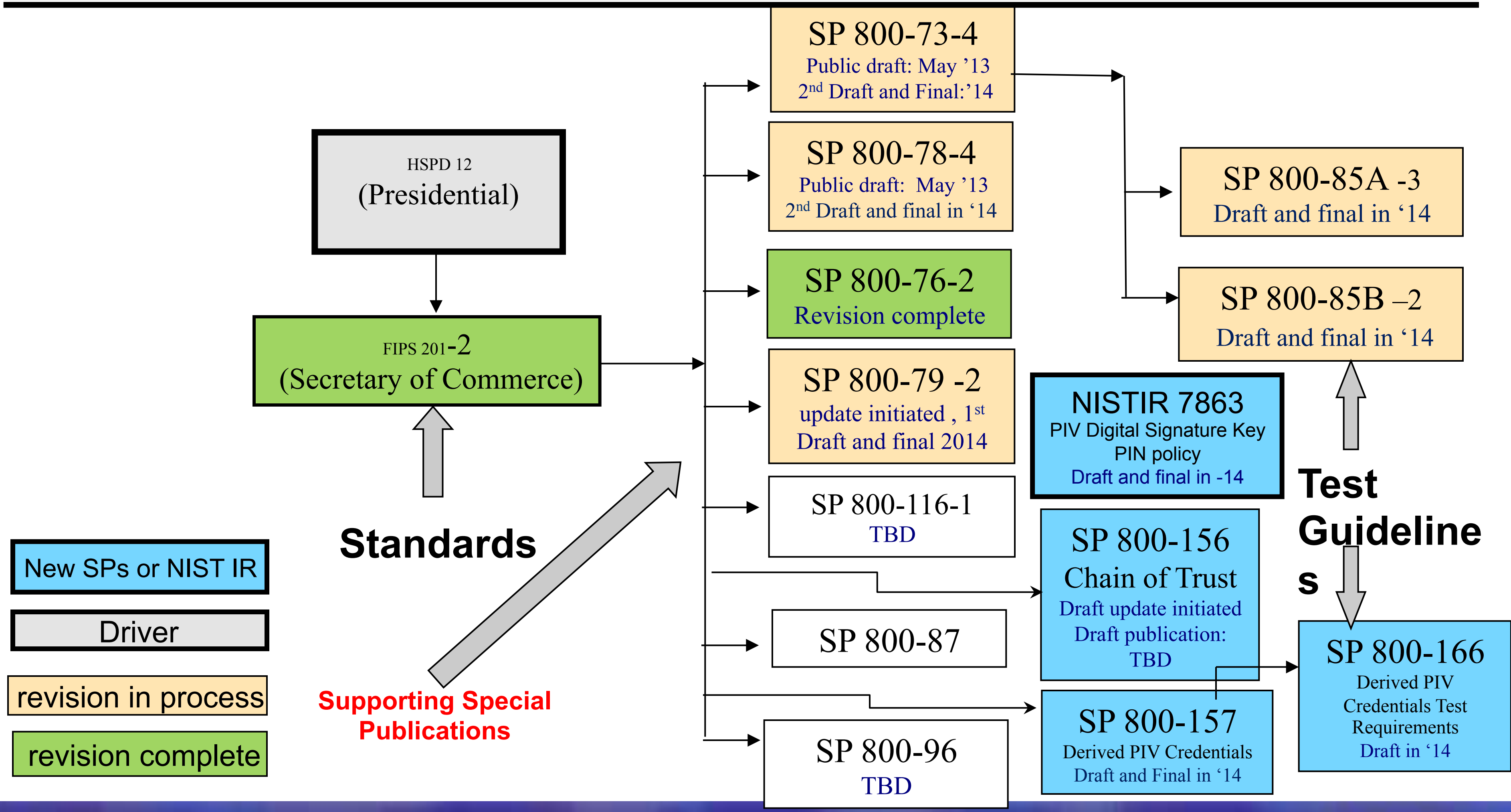
– In Depth Technical Detail in…
  - – SP 800-157 *Derived PIV Credentials*
  - - SP 800-166 *Derived PIV Credentials Test Requirements*
  - - SP 800-79 *Guidelines for the Accreditation of PIV Card Issuers and Derived PIV Credential Issuers*

FIPS 201-2 Alignments in SPs

- Optional Chain-of-Trust and Grace Period for PIV card reissuance processes
  - Technical details in SP 800-156 (new) and SP 800-79

- Relaxation of PIV Card termination requirements and specifically certificate revocation
  - Technical details in SP 800-79

FIPS 201-2 and Associated Special Publications (SPs)



HSPD 12
(Presidential)

FIPS 201-2
(Secretary of Commerce)

Standards

Supporting Special Publications

SP 800-73-4
Public draft: May ’13
2nd Draft and Final:’14

SP 800-78-4
Public draft: May ’13
2nd Draft and final in ‘14

SP 800-76-2
Revision complete

SP 800-79 -2
update initiated , 1st Draft and final 2014

SP 800-116-1
TBD

SP 800-87

SP 800-96
TBD

SP 800-85A -3
Draft and final in ‘14

SP 800-85B –2
Draft and final in ‘14

NISTIR 7863
PIV Digital Signature Key PIN policy
Draft and final in -14

SP 800-156
Chain of Trust
Draft update initiated
Draft publication: TBD

SP 800-157
Derived PIV Credentials
Draft and Final in ‘14

Test Guideline s

SP 800-166
Derived PIV Credentials Test Requirements
Draft in ‘14

🟦 New SPs or NIST IR

⬜ Driver

🟧 revision in process

🟩 revision complete

The NIST PIV Crew (from A to Z)

Ramaswamy Chandramouli (mouli@nist.gov)
David Cooper (david.cooper@nist.gov)
Hildegard Ferraiolo (hferraio@nist.gov)
Salvatore Francomacaro (salfra@nist.gov)
Ketan Mehta (mehta_ketan@nist.gov)

Thank you

Questions?

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