General Plan:

Hildegard Ferraiolo
PIV Standard Program Lead
Computer Security Division

NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

Overview

- Logistics
- The Agenda
- Priority Change Requests
- The FIPS Process and BRM
- Context in-scope/out-of-scope
- PIV Team and Steering Comittee
- Revision Principles and Lessons Learned

Logistics – The Business Requirements Meeting (BRM)

- Presentations followed by discussions, Q&A
- We have a large remotely attending audience:
  - Please use the microphone to comment and/or ask questions
  - Remote Attendees use piv_comments@nist.gov to comment and/or ask questions
- We cannot cover all –
  - Opportunity to comment after the meeting (deadline 3/31/19) – government only

The Agenda Today

8:30-8:50	**Welcome Remarks – Donna Dodson (NIST)**
8:50-9:30	**Digital Identity Policy - Jordan Burris (OMB)**
9:30-10:10	**General Plans - Hildegard Ferraiolo (NIST)**
10:10-10:30	**Break**
10:30-11:30	**Identity Proofing – Jim Fenton (Altmode Networks) and David Temoshok (NIST)**
11:30-12:30	**Authenticators & Derived Credentials – Andy Regenscheid (NIST)**
12:30 - 1:30	**Lunch**
1:30 - 2:30	**Federation for Logical Access – Justin Richer (Bespoke) and David Temoshok (NIST)**
2:30-3:10	**PACS - Hildegard Ferraiolo (NIST) and Andy Regenscheid (NIST)**
3:10-3:30	**Break**
3:40-4:10	**Other Topics - Hildegard Ferraiolo (NIST)**
4:10-4:30	**Wrap up**

Background - FIPS 201 Revision 2

- Addition of Derived PIV Credentials – as an optional authenticator for platforms that do not support smartcards (currently restricted in SP 800-157 to mobile devices)
- Virtual Contact Interface – secure communication for wireless authentication
- Chain of Trust – enables binding and reconnection to enrollment record. Its XML schema in SP 800-156 enables inter-agency data exchange of enrollment record – avoids re-enrollment
- Biometrics:
  - addition of iris as an option for enrollment/binding to enrollment record
  - Made facial image template mandatory as an on-card biometric – can be used at enrollment/re-issuance
  - Option for match on card fingerprint authentication

- Green text indicate that the R2 revision items play a role in R3

continued Background - FIPS 201 Revision 2

- Deprecated the CHUID authentication mechanism and indicated its removal from a future FIPS
- Made *PKI-CAK* cryptographic key mandatory for PIV Cards, intended use for 1 factor wireless authentication and as one of the replacement of the CHUID authentication mechanic
- On-card NACI indicator remains a requirement. Major purpose of Revision 1 was to include the indicator.

- Signature and encryption Key became mandatory

- Green items indicate that the R2 revision item plays a role in R3.

Priority Change Requests for R3

- Addition of other Form Factors not just smartcards because…
  - Some platforms do not support smartcards
- Additional non-PKI PIV Credentials because…
  - We use alternatives, especially where smartcards are not supported
- Federation
  - shifting interagency interoperability requirement of HSPD-12 to Federation

(continued) Priority Change Requests for R3

- Identity Proofing in General
  - The FIPS 201/SP 800-63 alignment
  - Remote supervised identity proofing
  - Remote AAL-3 authenticator derivation
- PIV and PACS
  - Removal of the CHUID authentication mechanism
  - Alternatives for CHUID authentication mechanism
  - Addition of Mobile Device (maybe others) for PACS

Looking Ahead…

- No major re-write of FIPS expected. Focus should be in amending/adding high level context/requirements in the major topic area (change requests)

- Major effort should concentrate on technical updates to NIST Special Publications for the major topic areas, while shepherding FIPS 201 through the revision fairly quickly.
  - SP development/edits will follow FIPS development

The Federal Information Processing Standard (FIPS) Process

A pre-established, formal process

https://www.nist.gov/itl/procedures-developing-fips-federal-information-processing-standards-publications

- Shares many similarity with regulatory rule making process
- Business Requirements meeting
- **FRN** to announce intention to develop/revise a FIPS and that starts commenting period and announces workshop/next steps
- Incorporate additional feedback solicited by additional **FRNs**
- **FRN** announcing revised draft (if needed), contains resolution of all comments of first draft, starts comment period and announces workshop
- Department of Commerce Secretary approval and **FRN** announcing final FIPS and also documents all comments/resolutions

- Maintaining traceability to business requirements

Collaborators/Contributors:

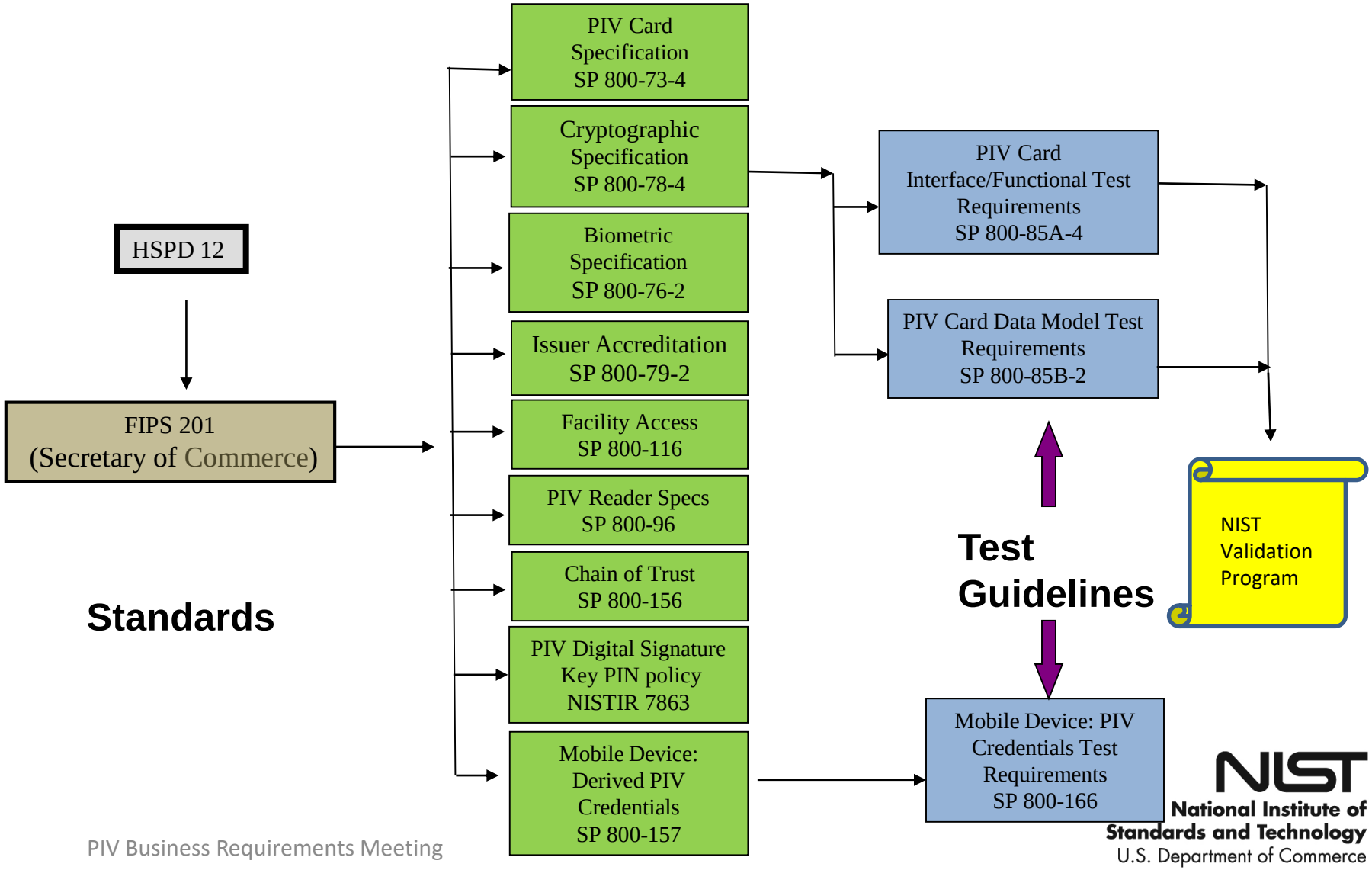
Part of HSPD-12 Steering Committee:

- OMB – policy guidance
- DHS – HSPD-12 implementation / PACS ISC
- GSA – FPKI, APL, GSA MSO
- OPM – Suitability, Vetting, Identity Source Documents of I-9
- DoD, DoJ

FIPS 201 Overall Process

- Top Down Approach
  - HSPD-12 -> FIPS 201 -> SPs
- FIPS specifies high level processes and requirements to satisfy HSPD-12
  - Supporting Special Publications (SP) detail the technical ‘how-to’

FIPS 201 R2



NIST National Institute of Standards and Technology U.S. Department of Commerce

Tentative Timeline/Milestones

Project Milestone	Date
Government-only Business Requirements Meeting	March 2019
Approval for revision package	August 2019
Draft updates to FIPS 201 materials	October 2019
Workshop	November 2019
2nd Draft package (if needed)	April 2020
2nd Draft Workshop (if needed)	May 2020
Final Package	August 2020
Associated Special Publication update/create complete	May 2021

In Comparison to Actual timeline for R2

Project Milestone	Date
Government-only Business Requirements Meeting	2010
Draft Published	March 2011
Workshop	April 2011
2nd Draft Published (if needed)	July 2012
2nd Draft Workshop (if needed)	August 2012
Final Published	Sep 2013
Associated Special Publication update/create complete	Ongoing from September 2013 - 2015

Revision Principles and Lessons Learned

FIPS 201 suited for high level requirements

- >Special Publications (SPs) for the details

Five year review cycle of FIPS 201

- 7-8++ years for the entire process – FIPS revision, SP update/creation
- Only well established/mature standards references and content in the FIPS (e.g, id proofing, PIV card lifecyle and its authentication mechanism)
- Add newer/emerging standards/concepts via SP while aiming for high level functional descriptors in the FIPS (e.g., new PIV authenticator, federation etc)
  - Current text in FIPS 201 on Derived PIV Credential should already cover new authenticator.

Team NIST Topic Leads

Topic	Lead
PIV Card (visual card topography, electronic components):	Ketan Mehta (ketan.Mehta@nist.gov)
Identity Proofing	David Temoshok, Jim Fenton(ctr)
Generalized Derivation	Hildegard Ferraiolo
Authenticator Profiles	Andrew Regenscheid
Federation Profile	David Temoshok, Justin Richer (ctr)
Facility Access with PIV card and alternatives PIV authenticators	Hildegard Ferraiolo, Andrew Regenscheid
Biometric Capabilities	Gregory Fiumara
Issuer Accreditation:	Ramaswamy Chandramouli
Jonathan Gloster	Project Support/PM

In/Out of Scope

NIST's HSPD-12 responsibility:

"established the requirements for a **common identification standard for identity credentials** issued by Federal departments and agencies to Federal employees and contractors (including contractor employees) for gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems." HSPD-12

- Out of scope (No Authority to):
  - Everything else (E.g., authorization, access control policies, other types of non-PIV authenticators (PIV-I, CIV), temporary cards)

HSPD-12 Steering Committee

- OMB: Jordan Burris, Carol Bales, Robert Hankinson, Marie LaSalle
- GSA: Jim Sheire, LaChelle LeVan
- OPM: Lisa Loss, Colleen Crowley
- DoD: Col. Clancy, Tim Baldridge
- DHS: Tom McCarty, Gregory Steven, William Windsor, Mark Vita, Daryle Hernandez
- DoJ: Nicole Arbuckle
- Participants by invitation depending on the topic of discussion

Committee::

- Consists of representatives from federal department/agencies with a role specified in HSPD-12.
- Gives high level directions/goals on the revision within the scope of HSPD-12.
- on-going meeting as needed as direction adjust based on business requirement meeting / comments received.
- Review/Agree on Draft and Finals to be published

To provide comment:

- How: piv_comments@nist.gov with subject line "FIPS 201 BR comments"
- By when: 3/31/2019
- What:
  - Comments from government-only stakeholders
  - High-level business requirements comments

  Comment on:
  - FIPS 201-2
  - Priority Change Requests
  - Questions contained in today's slides