Overview of FIPS 201 Revision 3

Hildegard Ferraiolo
PIV Program Lead
National Institute of Standards and Technology
August, 2019
Federal Computer Security Managers' Forum

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

Overview

- Status Quo- The current Standard (R2)
- Where we'll headed: Priority Change Requests
- PIV Authenticators and Federation
- In Closing

HSPD-12

"**There are wide variations in the quality and security of identification used to gain access to secure facilities** where there is potential for terrorist attacks. In order to eliminate these variations, U.S. policy **is to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy** by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees). "

Homeland Security Presidential Directive-12

August 27, 2004

Where We Are:

Status Quo: Revision 2 of FIPS 201

- 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
- 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 Where We Are:

Status Quo: 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

- Signature and encryption Key became mandatory

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

Change Requests

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

Where We Are Headed:

Change Requests for FIPS 201 Revision 3

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

(continued) Change Requests for R3

- Identity Proofing in General
  - The FIPS 201/SP 800-63 alignment
    - Identity Source Documents
  - Remote supervised identity proofing
    - Supervised remotely – is local attendant needed?

(continued) Change Requests for R3

PIV and PACS

- Removal of the CHUID authentication mechanism
- Alternatives for CHUID authentication mechanism
  - desired properties: fast, wireless (touch-and-go), one-factor
  - PKI-CAK, FICAM e-PACS server-based BIO-in-PACS (mixed review), Opacity
- Deprecating VIS (flash pass - guard comparing card photo)
- Addition of Mobile Device (maybe others) for PACS?

Miscellaneous Change Requests…

- Make NACI background investigation indicator on PIV Authentication Certificate optional & deprecate in future
- Considering additional PIV Card Security Features (SF)
  - Currently requires only one SF – strongly recommend three
  - Deprecate PIV card magnetic stripe and bar code

FIPS 201-3 Update:

Derived PIV Credential

Authenticators and Federation

Hildegard Ferraiolo

Computer Security Division

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

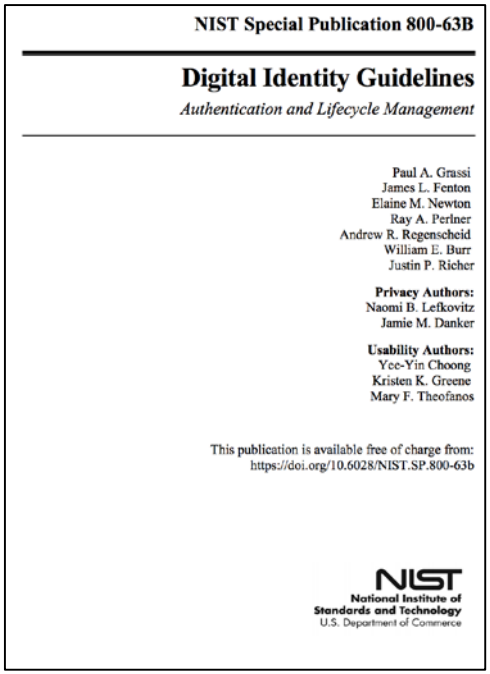
Derived PIV Credential (DPC)

Authenticators

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

Anticipated Changes in FIPS 201-3

- Broadly allow alternative authenticators to be derived from PIV credentials
  - Specify requirements in new Special Publication
  - **AAL2** and **AAL3**
  - Rely on SP 800-63B as the basis for security requirements
  - Facilitate interoperability through federation, not authenticator standards


NIST Special Publication 800-63B

Digital Identity Guidelines

Authentication and Lifecycle Management

Paul A. Grassi
James L. Fenton
Elaine M. Newton
Ray A. Perlner
Andrew R. Regenscheid
William E. Burr
Justin P. Richer

Privacy Authors:
Naomi B. Lefkovitz
Jamie M. Danker

Usability Authors:
Yee-Yin Choong
Kristen K. Greene
Mary F. Theofanos

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63b

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

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

Authenticator Assurance Levels

	AAL2	AAL3
Types	Combinations providing multifactor authentication: OTP, Out-of-Band, Look-up Secrets, software crypto	Hardware cryptographic authenticators (multifactor authenticators or combinations)
Examples	Passwords with: • Push notifications, • OTP/SecureID • FIDO U2F Software-based Derived PIV	PIV cards* Hardware-based Derived PIV* FIDO with Token Binding + password
MitM Resist.	**Required**	**Required**
Verifier Impersonation Resist.	Not Required	**Required**
Verifier Compromise Resist.	Not Required	**Required**
Auth. Intent	Recommended	**Required**

Authenticator Interoperability

- **Objectives**
  - Support interagency reuse and acceptance
  - Facilitate technical interoperability with applications
- Many non-PKI authenticators are for use with a single CSP/Verifier
  - Limits need for authenticator-based interoperability
- **Shift interoperability focus to federation**
  - **Provides abstraction layer to support multiple authenticators**
  - **Can simplify authenticator management**
- WebAuthn/FIDO
  - FIDO/WebAuthn guidance could promote security, facilitate compatibility between gov't servers and industry authenticators

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

Authenticator Challenges: The Link to PIV Cards

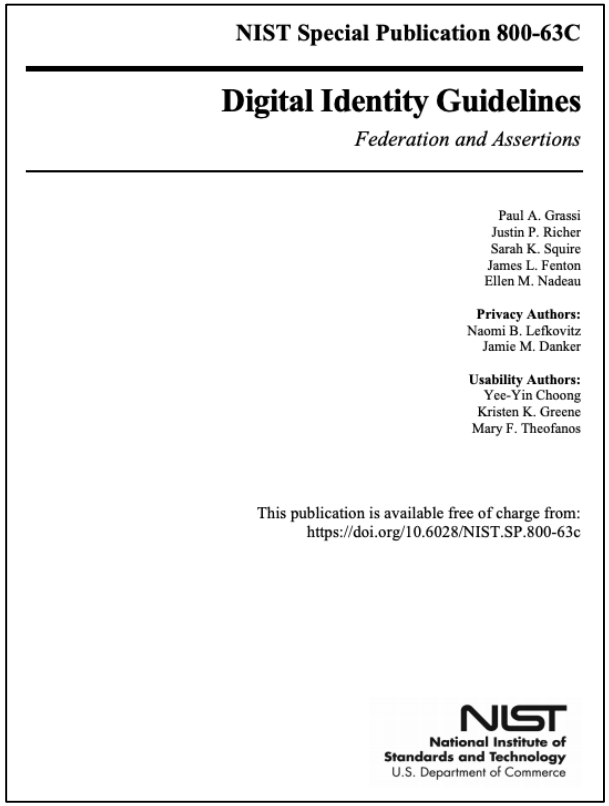
- PIV Card and DPC authenticator are tightly linked.
  - Authenticators need to be terminated if eligibility to hold a PIV Card ends/is terminated
  - Requires links to PIV Card issuer
    - Easier to maintain if issuer of DPC authenticator and PIV Card is the home agency (the same issuer) – IDMS maintains it.
    - Hard to maintain/communicate if DPC authenticator and PIV Card issuer are different
  - NIST to restrict issuance of Derived PIV Credential (authenticators) to home agency to facilitates termination of authenticators

Federation

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

Anticipated Changes in FIPS 201-3

- Encourage federation to facilitate interoperability and flexibility
  - Specify requirements in new Special Publication
  - Rely on SP 800-63C as the basis for security requirements at FAL1-3.
  - Identify/develop profiles of common federation protocols
  - Develop guidelines for IdPs/CSPs



NIST Special Publication 800-63C

Digital Identity Guidelines

Federation and Assertions

Paul A. Grassi
Justin P. Richer
Sarah K. Squire
James L. Fenton
Ellen M. Nadeau

Privacy Authors:
Naomi B. Lefkovitz
Jamie M. Danker

Usability Authors:
Yee-Yin Choong
Kristen K. Greene
Mary F. Theofanos

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63c

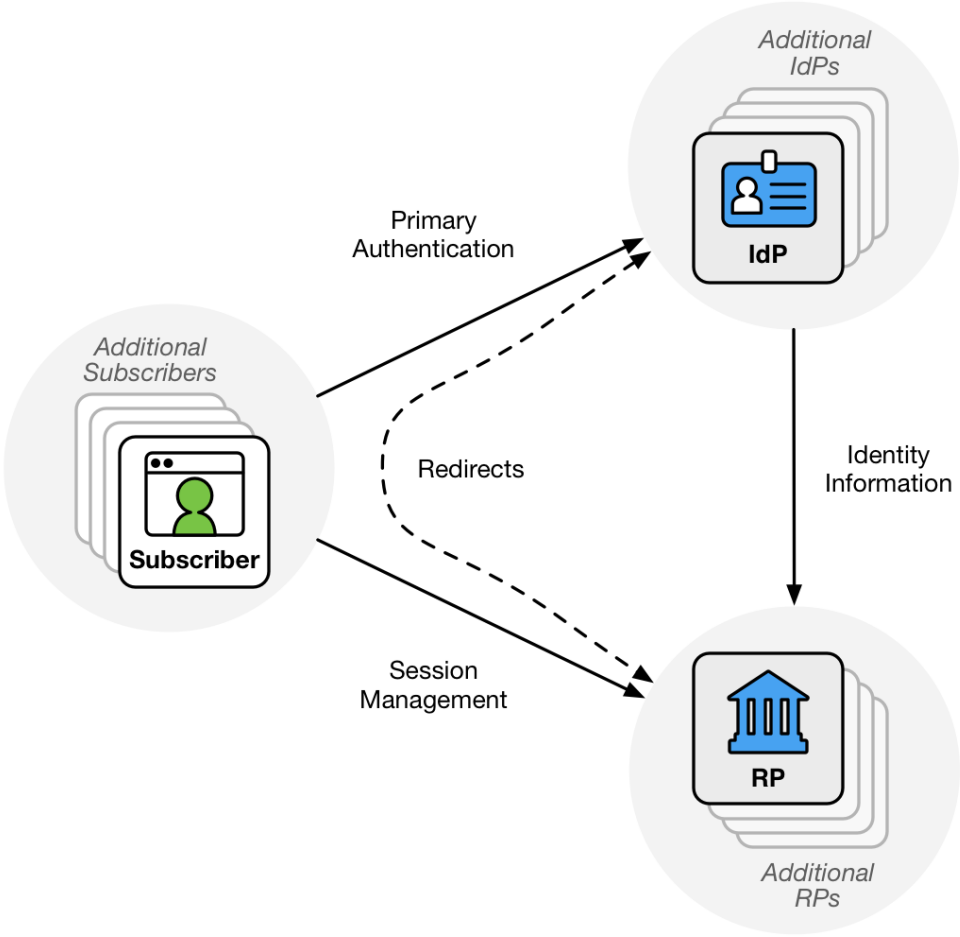
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

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

What is federation?

A process that allows the conveyance of identity and authentication information across a set of networked systems.

- NIST SP 800-63-3

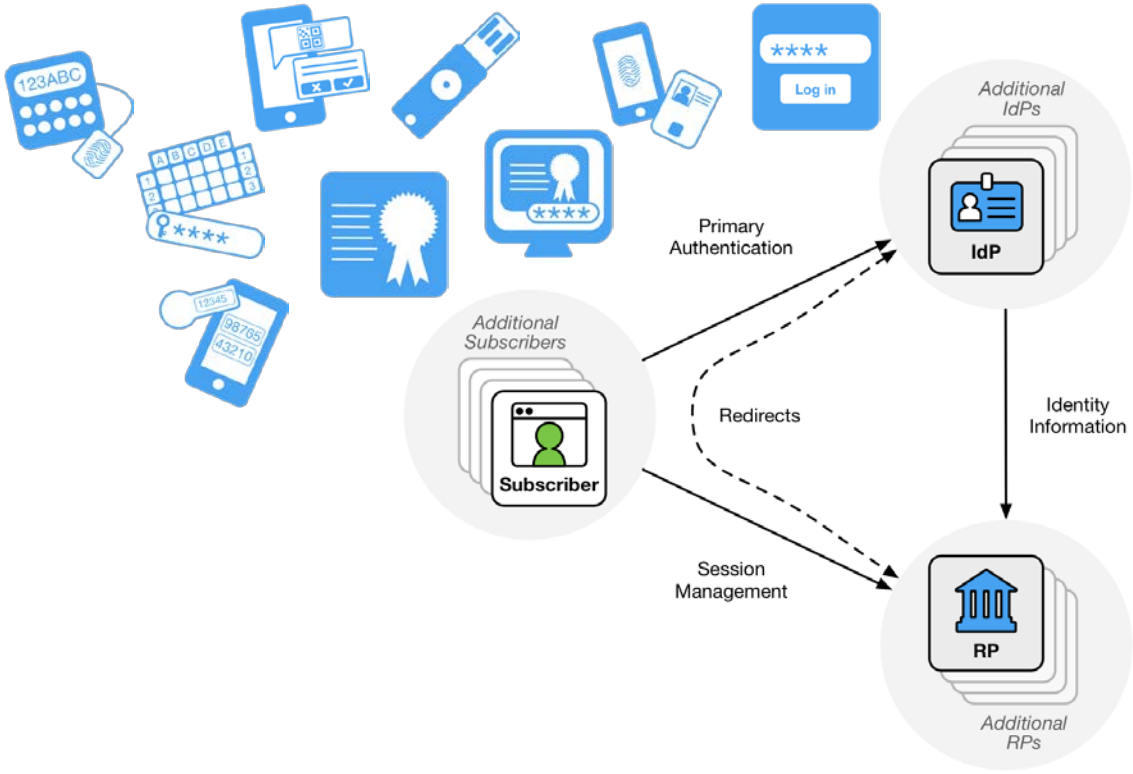


National Institute of Standards and Technology
U.S. Department of Commerce

Why federate?

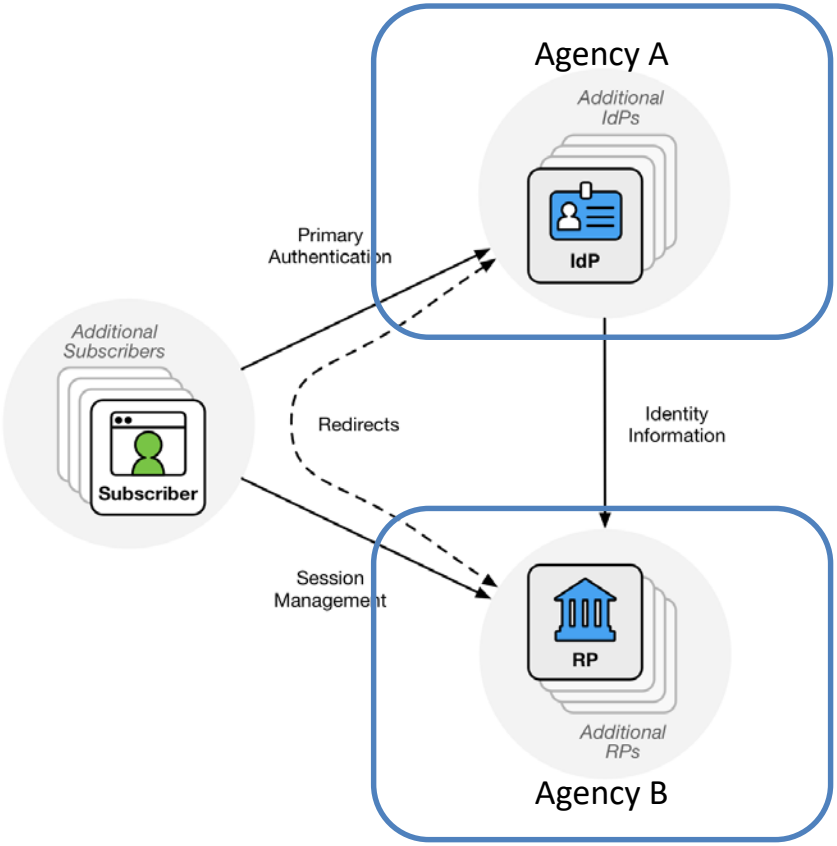
- Abstraction layer for authenticators
- Attribute disclosure
- Timeliness of assertions/attributes
- Cross-boundary acceptance and use
- Relying Party maintains control of sessions

Abstraction layer across authenticators



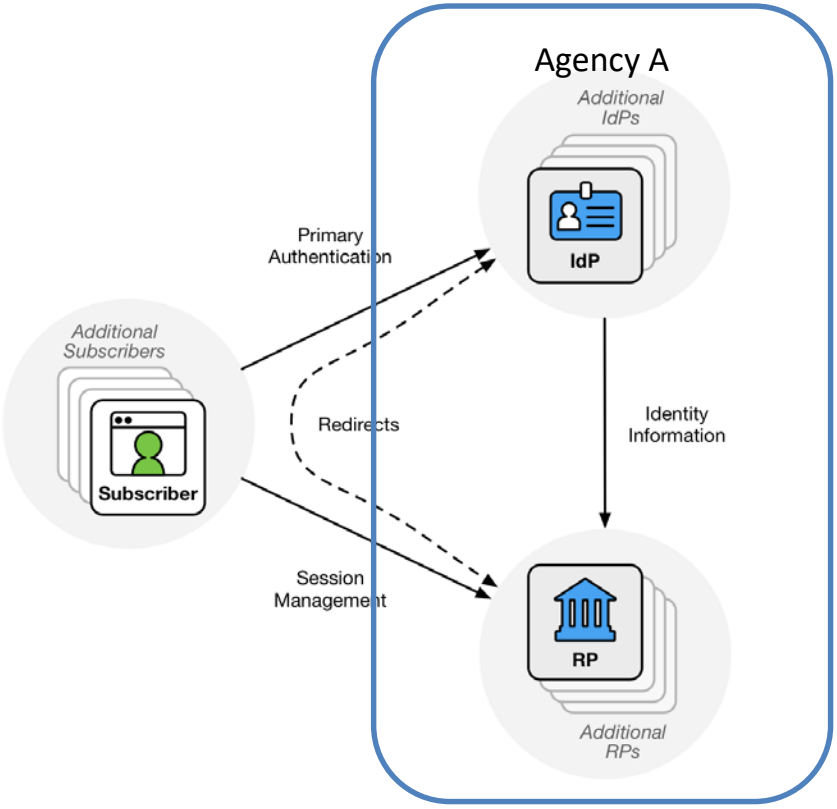
National Institute of Standards and Technology
U.S. Department of Commerce

Can cross boundaries



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

Can work internally



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

Federation Assurance Level (FAL)

	FAL1	FAL2	FAL3
Assertion type	Signed	Signed & Encrypted	Signed, Encrypted, & Holder-of-Key
Subscriber attributes	Yes (if backchannel)	Yes	Yes
Examples	OIDC SAML artifact binding	OIDC with encrypted ID token SAML with encrypted assertion	OIDC or SAML plus secondary key-based authenticator (certificate, FIDO, etc)

- **FAL1 is good for most use cases**
  - Requires signatures, audience restriction, replay protection, etc.
  - Especially when subscriber attributes are sent in the backchannel, separate from the assertion
- **FAL3 requires token binding and/or client authenticated TLS**

Federation protocols

- OpenID Connect (OIDC)
  - Supports browser and mobile
  - iGov profile from OIDF
- Security Assertion Markup Language (SAML)
  - Profile available for browsers
  - eGov profile from Kantara

In Closing

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

Looking Ahead…

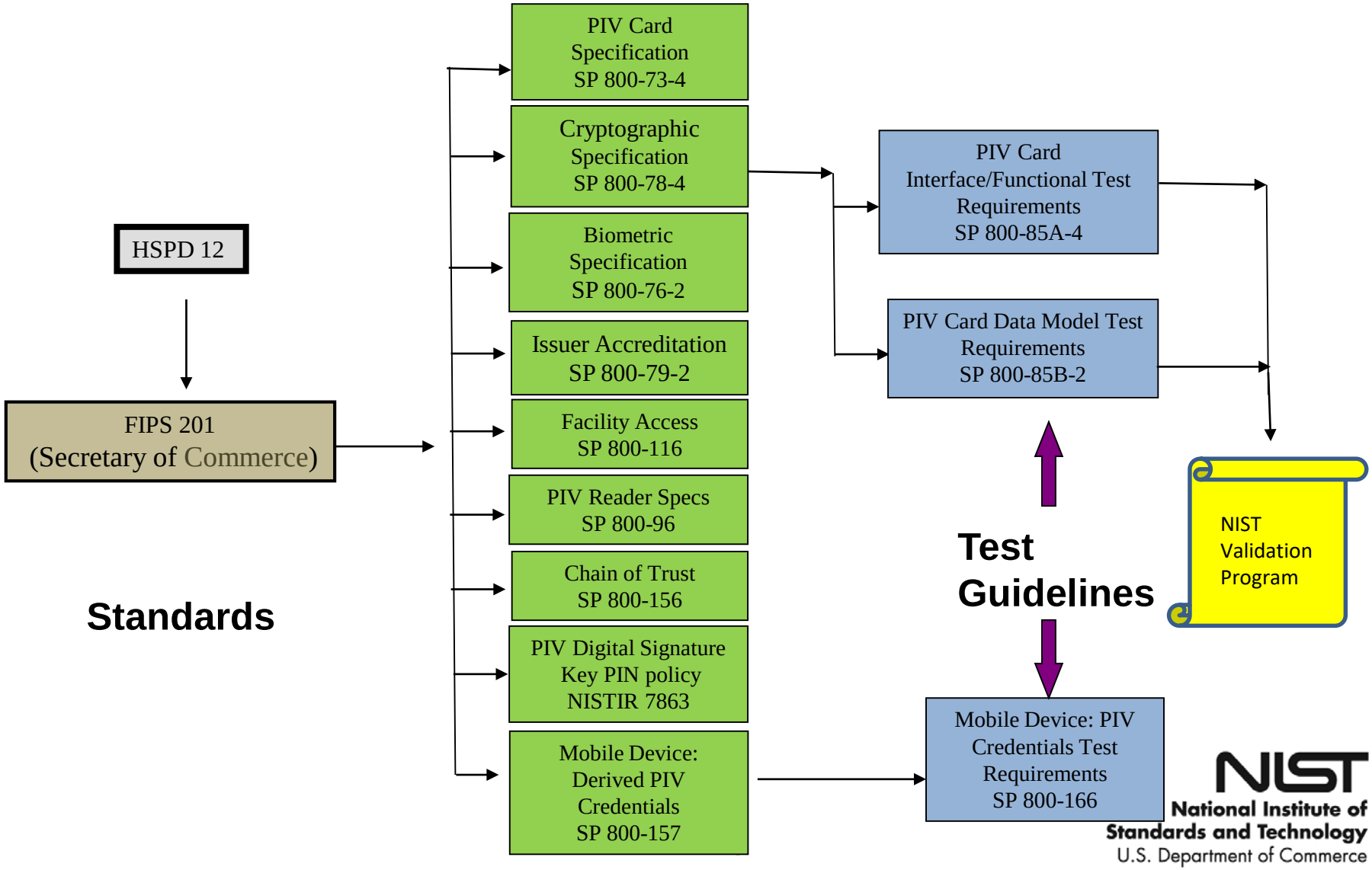
- No major re-write of FIPS expected. Focus should be in amending/adding high level context/requirements in the major topic area (change requests)

- 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

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 Overall Process



Tentative Timeline/Milestones

Project Milestone	Date
Government-only Business Requirements Meeting	March 2019
Draft updates to FIPS 201 materials	~November 2019
Workshop	~December 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

HSPD-12 Steering Committee

- OMB
- GSA
- DoD
- DHS
- DoJ
- 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

Questions?

Contact Information

PIV PoC:

Hildegard Ferraiolo

PIV Standard Program Manager

hildegard.ferraiolo@nist.gov