NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Personal Identity Verification Webinar:

Derived PIV Credentials and Federation

NIST Information Technology Lab

For closed captioning go to:

https://das.1capapp.com/event/nistnccoe

February 1, 2023

Welcome & Session Overview

Hildegard Ferraiolo, NIST PIV Program Lead

Why are we here today?

Purpose:

- ➢ To kick off the public comment period for new PIV guidelines for derived PIV credentials and federation
- ➢ To describe the new guidelines and related FIPS 201-3 revisions
- ➢ To enumerate the public comment process and timeline

Outcomes:

- ✓ You gain an understanding of the new guidelines and how they fit into the broader PIV program
- ✓ You will have insights into the areas where NIST is seeking specific input for the final versions
- ✓ You will have details on the comment period and how to submit comments to the PIV team

What will we be discussing?

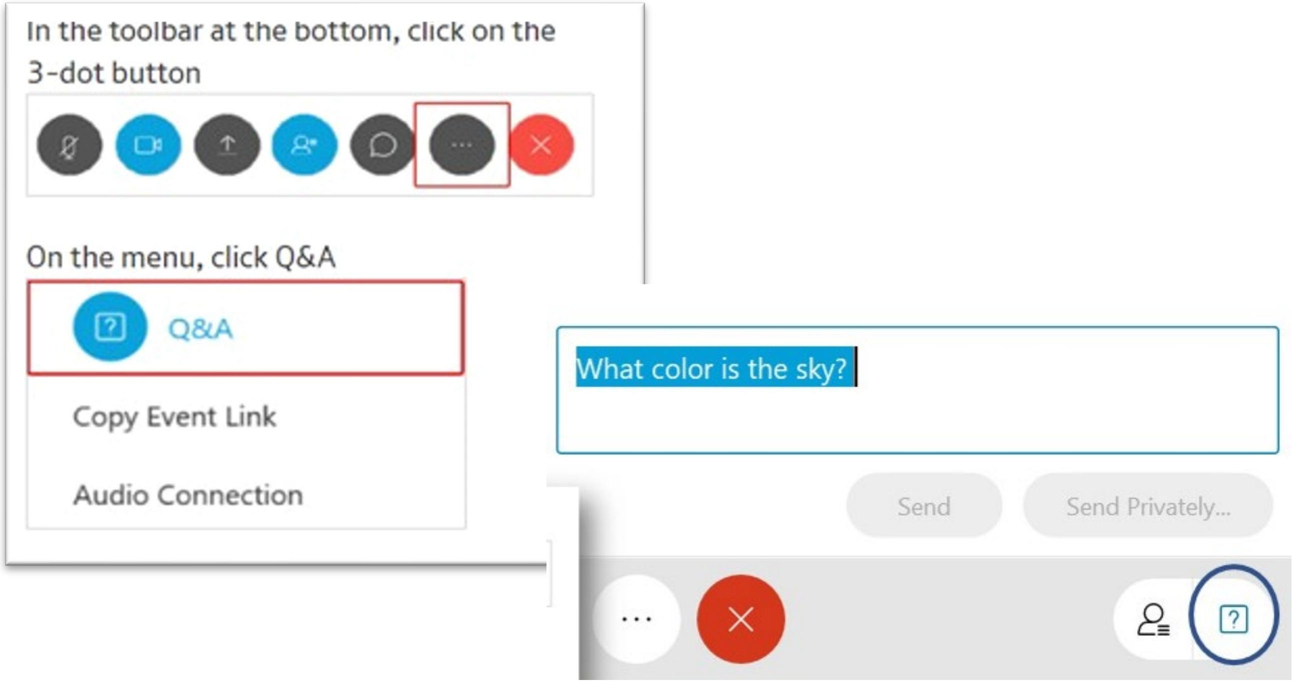
Item	Speaker	Time
Welcome	Hildegard Ferraiolo	5 minutes
Opening Remarks	Matthew Scholl	5 minutes
Introduction to the PIV Standard	Hildegard Ferraiolo	10 minutes
FIPS 201-3 Overview of Revisions	Andrew Regenscheid	15 minutes
Introduction – NIST and the Digital Identity Guidelines	Ryan Galluzzo	15 minutes
	Break 1:50 – 2:00 pm	
Changes to SP 800-157 R1	Andrew Regenscheid Jim Fenton	20 minutes
New Draft SP 800-217	Andy Regenscheid Justin Richer	30minutes
Key Dates & Next Steps	Hildegard Ferraiolo	5 minutes

Have Questions? Please use the Q&A feature on Webex to submit questions. We will address select questions after each session. As time permits, we may also respond via the Q&A feature on Webex.

Audience Engagement

Please use the Q&A window to enter your questions for today's event.

1. On the right side, click on the 3-dot button.
2. Click the Q&A header to open the Q&A panel.
3. Type your question in the box, along with your name and organization.
4. Click **send**.



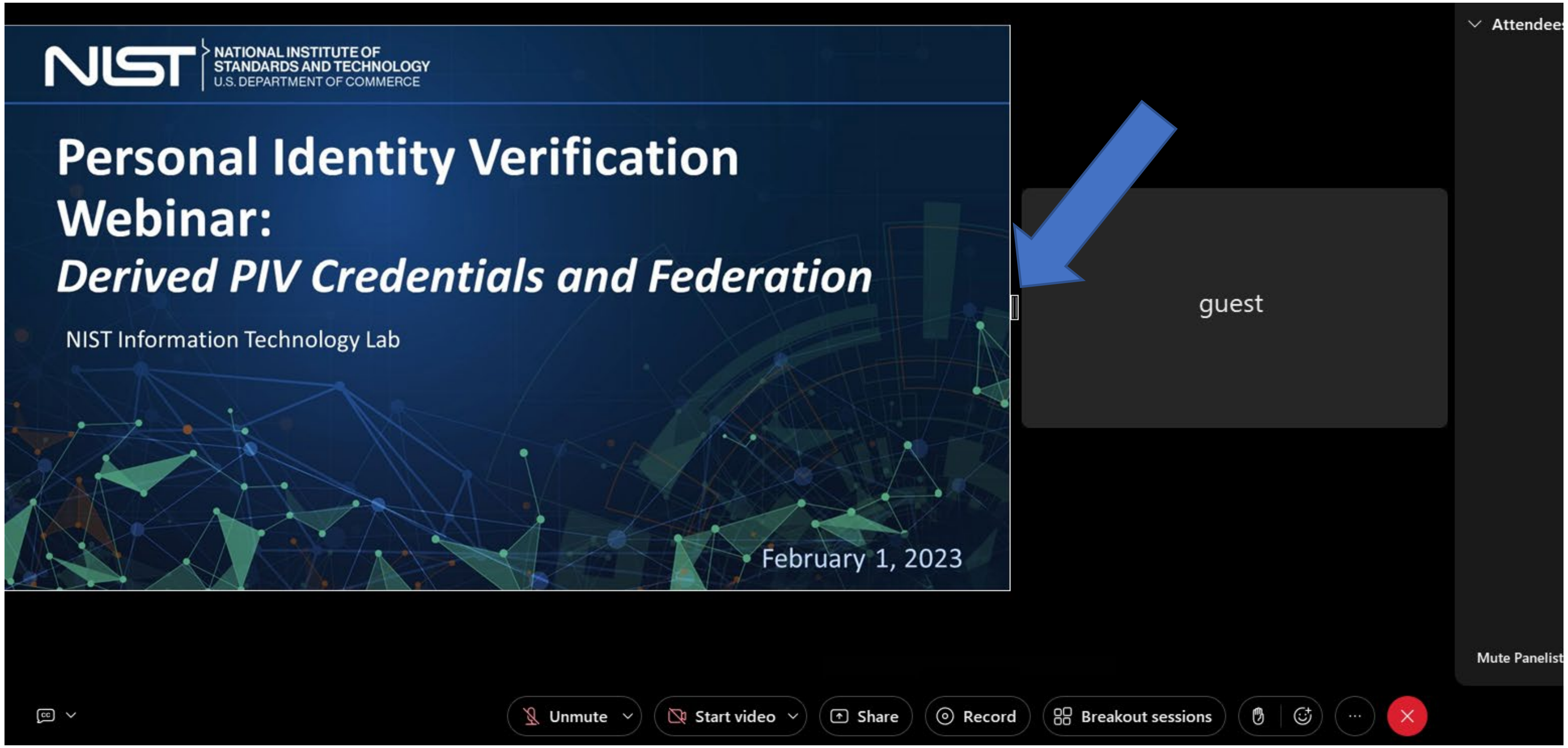
In the toolbar at the bottom, click on the 3-dot button

On the menu, click Q&A

What color is the sky?

Adjusting Slide Size

To adjust the size of the slides on your screen, drag the bar in-between the slides and presenter to the left or right.



NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

Personal Identity Verification Webinar:

Derived PIV Credentials and Federation

NIST Information Technology Lab

February 1, 2023

Opening Remarks

Matthew Scholl, Chief of the Computer Security Division

Introduction:

Personal Identity Verification Program

Hildegard Ferraiolo, NIST PIV Program Lead

HSPD-12 -> FIPS 201

Homeland Security Presidential Directive 12 was issued in 2004 to create a common identification standard for federal employees and contractors for accessing federally-controlled facilities and federal information systems.

Results:

- A standard, interoperable credential: the PIV Card
- Consistent processes for identity vetting and proofing
- A common, secure approach for accessing facilities and networks
- An increased level of government efficiency

Refresh via FIPS 201 Revisions

The PIV Standard needs to be agile.

- Incorporate Lessons Learned from stakeholders
  - Department/Agencies, Vendors, Integrators
- Update based on Technological Advancements
  - E.g., remote supervised id proofing/enrollment
- Align with New Policy
  - (i.e., OMB, OPM)

Example: FIPS 201-2 →FIPS 201-3

FIPS 201 - Revision 2:

- Allows for Derived PIV Credentials on mobile devices
  - Embedded or removable Derived PIV Credential
  - A PKI-Credential – 2 factor
  - One platform – mobile device
  - Specified in SP 800-157

FIPS 201 - Revision 3:

- Expands Derived PIV Credentials
  - PKI and non-PKI credentials
  - Platform agonistic
  - Specified in draft SP 800-157 R1
- Adds PIV Federation – draft SP 800-217

Scope of PIV Standards & Guidelines

In Scope:

Enrollment and Credential Issuance

→ Evidence and biometric requirements supporting policies

→ Enrollment records

Credential Lifecycle Management

→ Reissuance/renewal procedures

→ Termination procedures

Credential Security

→ Authenticator requirements

→ Cryptography specifications

→ Biometric specifications

Credential Interoperability

→ Card/application interface specifications

→ PIV Reader specifications

→ *Federation (new with FIPS 201-3)*

Trust enablement

→ PIV Issuer accreditation guidelines

Privacy

→ Requirements for PIV issuers and implementers

Scope of PIV Standards & Guidelines

In Scope:

Enrollment and Credential Issuance

→ Evidence and biometric requirements supporting policies
→ Enrollment records

Credential Lifecycle Management

→ Reissuance/renewal procedures
→ Termination procedures

Credential Security

→ Authenticator requirements
→ Cryptography specifications
→ Biometric specifications

Credential Interoperability

→ Card/application interface specifications
→ PIV Reader specifications
→ *Federation (new with FIPS 201-3)*

Trust enablement

→ PIV Issuer accreditation guidelines

Privacy

→ Requirements for PIV issuers and implementers

Out of Scope:

Who needs to obtain a PIV credential?

→ OPM, Credentialing Standards Procedures (2020)

Who is eligible for a PIV credential?

→ OPM Credentialing Standards Procedures (2020)

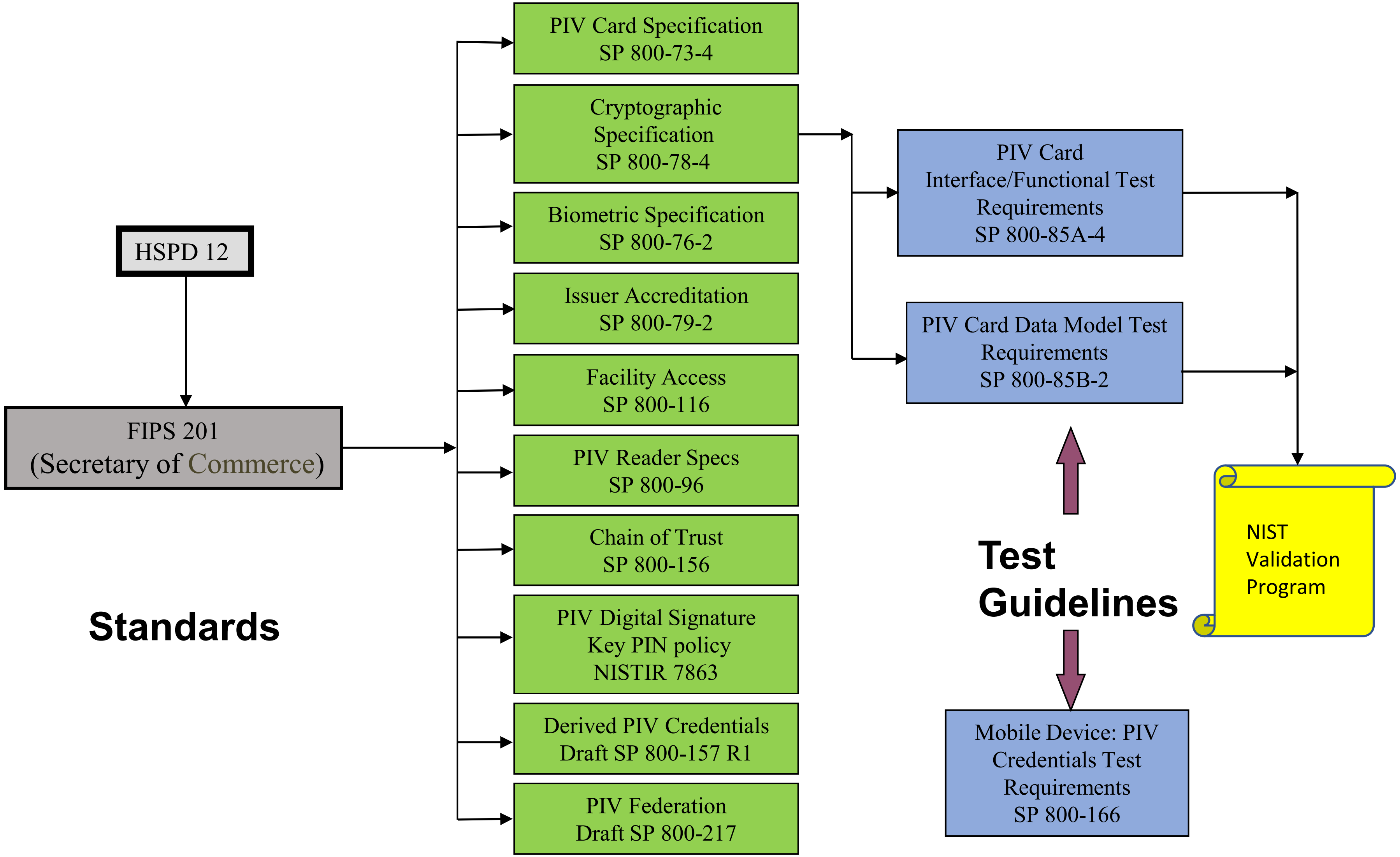
Where must PIV credentials be used?

→ OMB, e.g., A-130, M-05-24, M-19-17
→ CISA/Interagency Security Committee (Facilities)

What products and services are approved?

→ GSA, e.g., Approved Products List, Trust Services program
→ Federal PKI Shared Service Providers

FIPS 201 and Supporting Special Publications



HSPD 12

FIPS 201
(Secretary of Commerce)

Standards

PIV Card Specification
SP 800-73-4

Cryptographic Specification
SP 800-78-4

Biometric Specification
SP 800-76-2

Issuer Accreditation
SP 800-79-2

Facility Access
SP 800-116

PIV Reader Specs
SP 800-96

Chain of Trust
SP 800-156

PIV Digital Signature Key PIN policy
NISTIR 7863

Derived PIV Credentials
Draft SP 800-157 R1

PIV Federation
Draft SP 800-217

PIV Card Interface/Functional Test Requirements
SP 800-85A-4

PIV Card Data Model Test Requirements
SP 800-85B-2

Test Guidelines

Mobile Device: PIV Credentials Test Requirements
SP 800-166

NIST Validation Program

FIPS 201-3
Overview of Revisions

Andrew Regenscheid, NIST PIV Technical Lead

FIPS 201-3 Revisions

Issued: January 2022

Identity Proofing

- Align with SP 800-63
- Supervised remote proofing

Authenticators

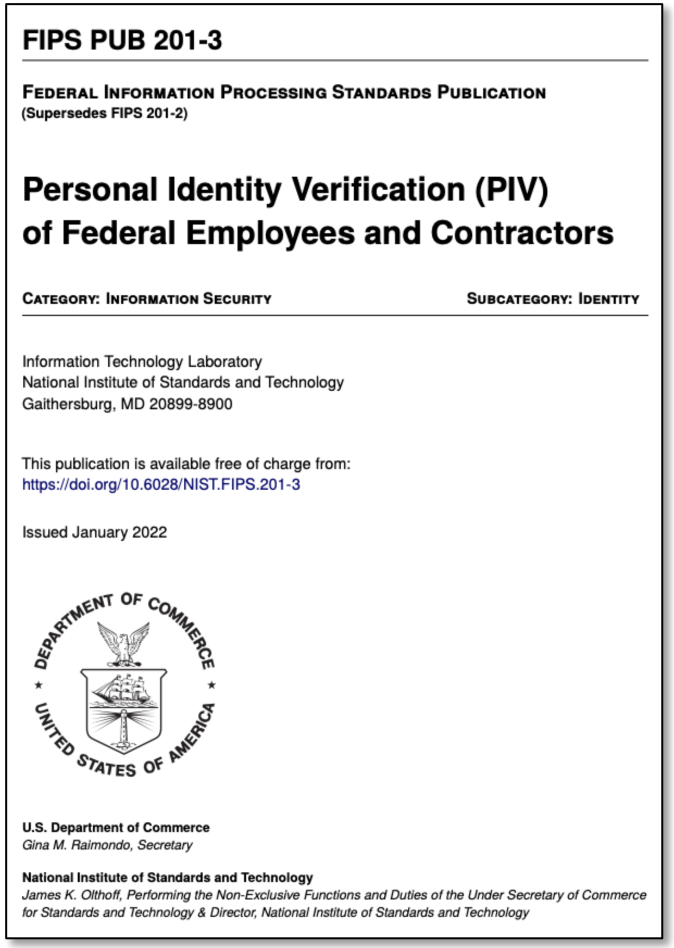
- Support new authenticators as derived PIV credentials
- Allow derived PIV credentials on additional platforms

Federation

- Facilitate interagency interoperability and trust
- Simplifies support on relying parties

Physical Access Control

- Removal of CHUID authentication mechanism
- Investigate alternative PACS tokens and authentication protocols



FIPS PUB 201-3

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION
(Supersedes FIPS 201-2)

Personal Identity Verification (PIV) of Federal Employees and Contractors

CATEGORY: INFORMATION SECURITY **SUBCATEGORY: IDENTITY**

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

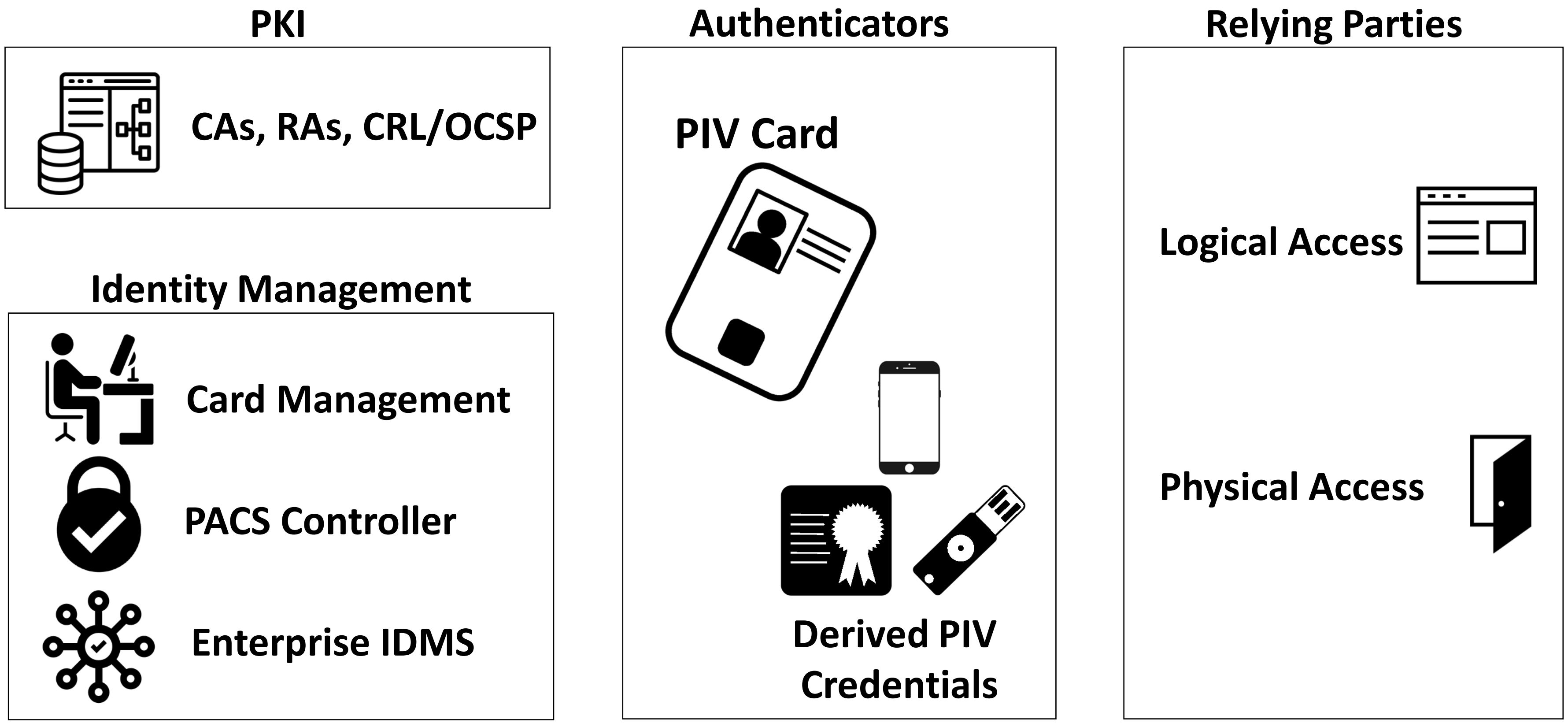
This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.201-3

Issued January 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

PIV Architecture



PKI

CAs, RAs, CRL/OCSP

Identity Management

Card Management

PACS Controller

Enterprise IDMS

Authenticators

PIV Card

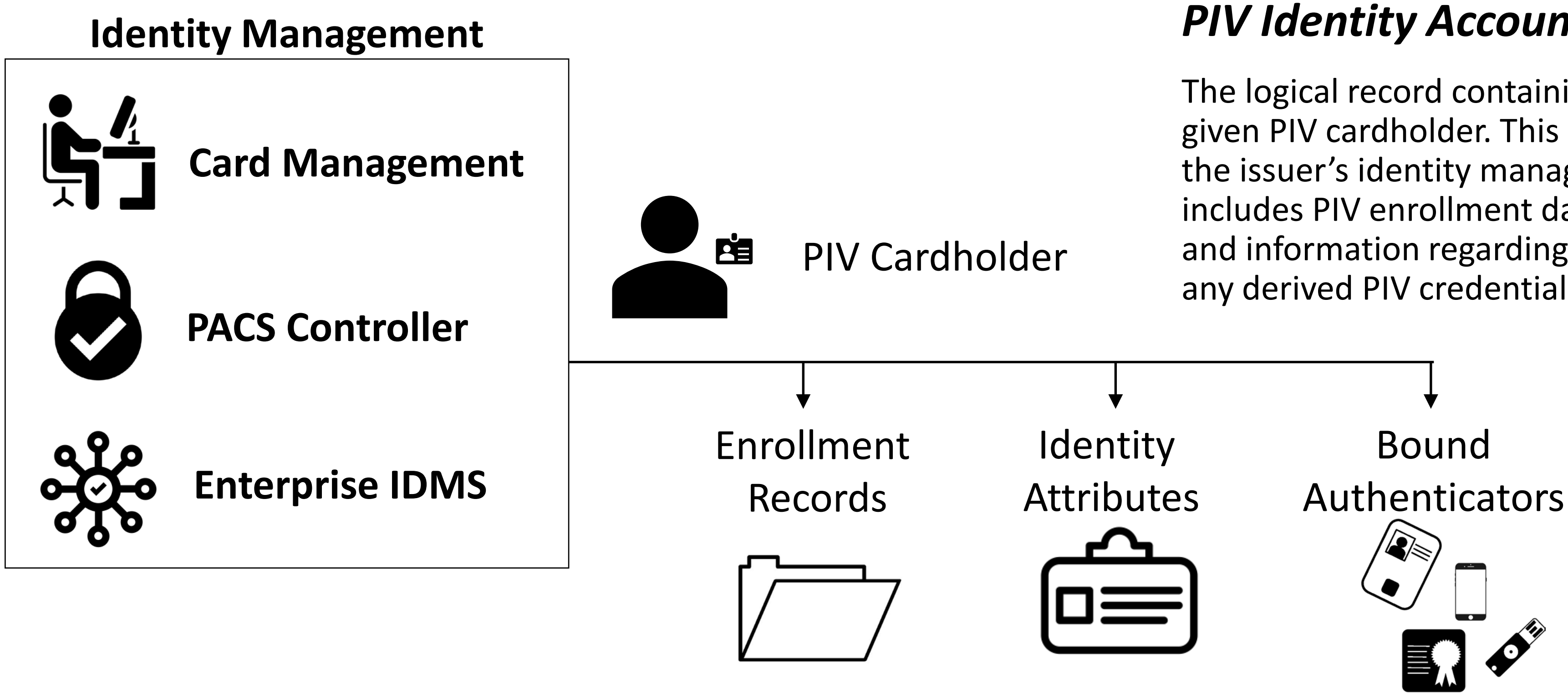
Derived PIV Credentials

Relying Parties

Logical Access

Physical Access

PIV Identity Management

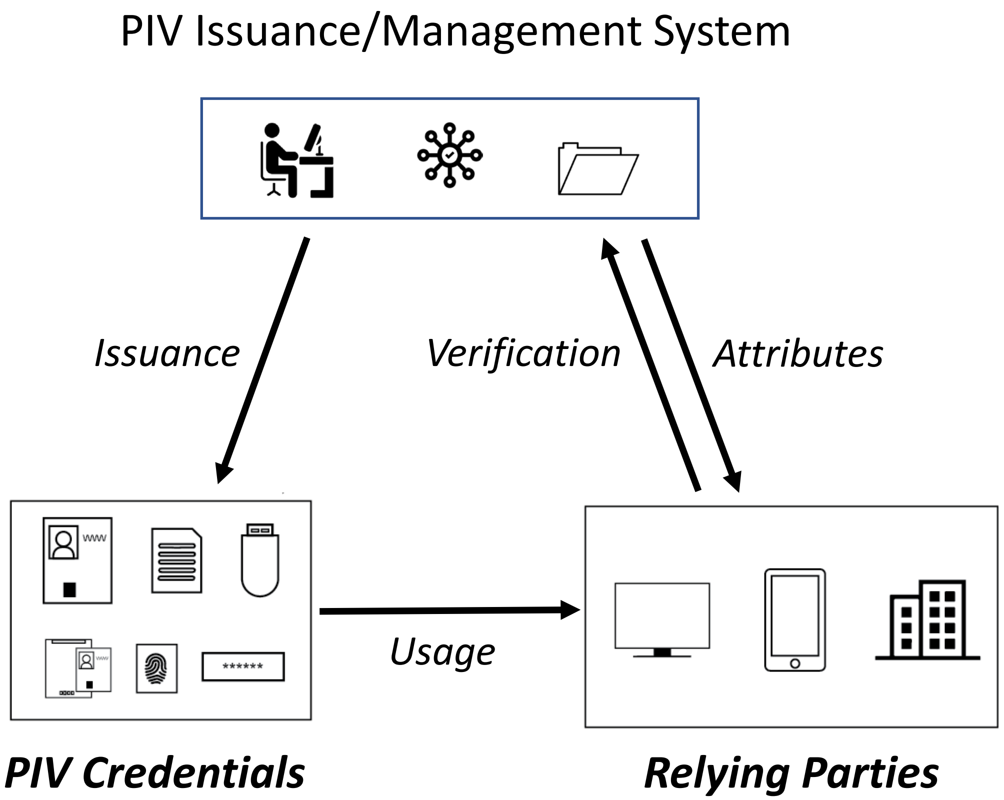


PIV Identity Account:

The logical record containing credentialing information for a given PIV cardholder. This is stored within the issuer's identity management system (or linked to it) and includes PIV enrollment data, cardholder identity attributes, and information regarding the cardholder's PIV Card and any derived PIV credentials bound to the account.

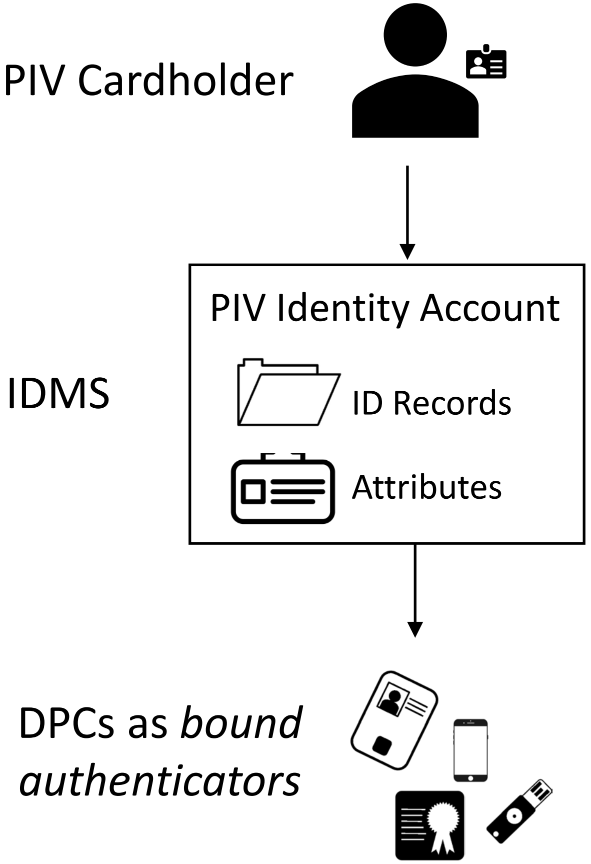
PIV/DPC Lifecycle

- **PIV Registration/Issuance**
  - Create the PIV identity account in IDMS
  - Create a PIV card
  - Bind the PIV card to the account
- **Registration of Derived PIV Credentials**
  - Bind to PIV identity account after authentication with PIV credential
  - Managed by cardholder's home agency
- **PIV Credential Usage**
  - Direct or federation between systems/agencies
  - Federation required to use non-PKI authenticators as DPCs
- **Termination of Credentials**
  - Revoking PKI certificates, as appropriate
  - Unbind/Invalidate [derived] PIV credentials in PIV identity account



Derived PIV Credentials in FIPS 201-3

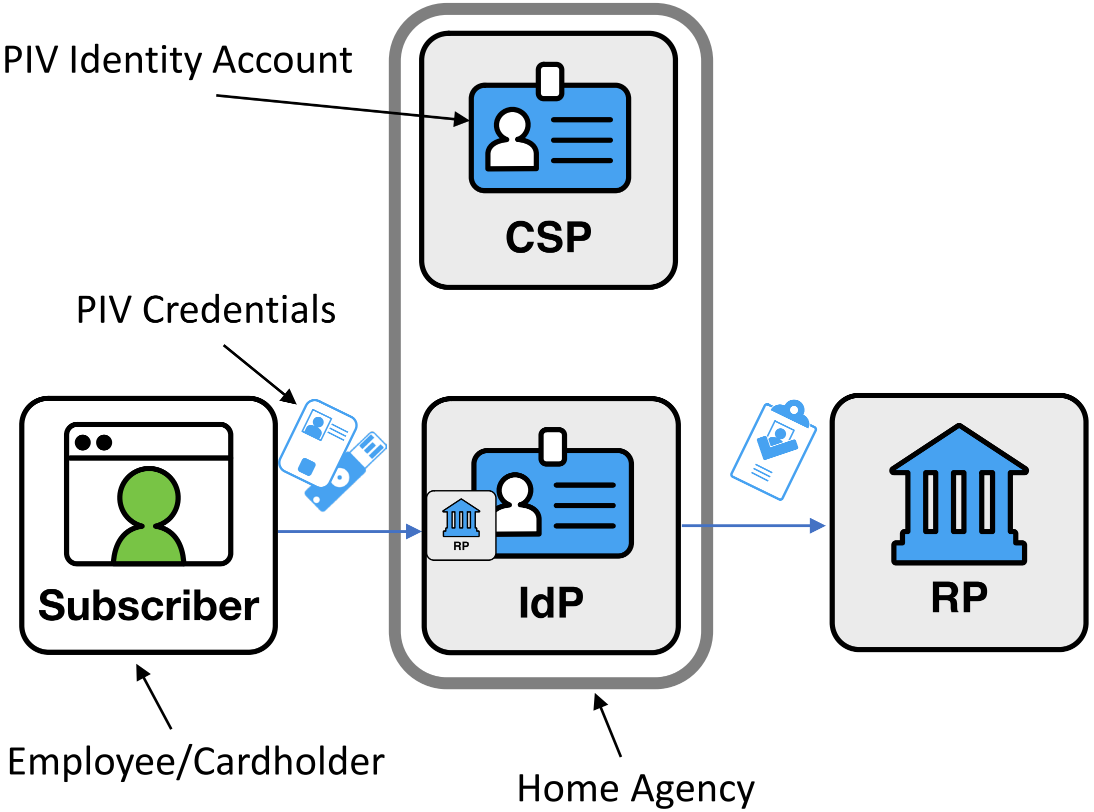
- Derived PIV Credentials as Bound Authenticators
  - An authenticator bound to subject's ***PIV identity account*** after successful authentication with PIV credential
  - Remote registration/binding allowed, with notification to the cardholder
  - ***Phishing-resistant authenticators*** based on **AAL2/AAL3** in SP 800-63B
- DPCs managed by agency responsible for the PIV identity account
  - Authoritative source for cardholder attributes and status
  - Cardholder's home agency has strongest relationship to employee
  - Non-PKI credentials can only be verified by ***PIV Issuer's IdP***
  - Interagency use cases supported through federation
- **Revised technical guidelines:**
  NIST SP 800-157r1, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*



Federation

- Recommended way to accept and process PIV credentials from other agencies
- Provides real-time sharing and identity assertions and attributes from the PIV account at cardholder’s home agency
- Facilitates interoperability between applications and a variety of authenticators

- **New technical guidelines: NIST SP 800-217, *Guidelines for the Use of Personal Identity Verification (PIV) Credentials with Federation***



Summary

- **FIPS 201-3: PIV as federal enterprise identity management**
  - Facilitate stronger, ***centralized identity management***
  - Maintain high-assurance ***identity proofing***
  - ***Increased flexibility*** to accommodate emerging use cases
- **Authenticators**
  - ***PIV authentication certificate*** as the root of trust
  - Agencies can select and deploy phishing-resistant ***derived PIV credentials*** that meet their needs
- **Federation**
  - ***Federation protocols*** are the basis for ***interoperability*** with relying parties
  - Agencies will need to federate using ***interoperable standards/profiles*** to facilitate interagency use

Introduction – NIST and the Digital Identity Guidelines

Ryan Galluzzo, Digital Identity Program Lead, Applied Cybersecurity Division

What Are the Digital Identity Guidelines?

- Details the process and technical requirements for meeting the digital identity management.
- Describes identity risk management process and assurance level selections (identity, authentication, federation assurance).
- Provides considerations for enhancing privacy and usability of digital identity solutions and technology.
- Inclusive of 4 volumes:
  - Base – Digital Identity Model and Risk Management
  - A – Identity Proofing & Enrollment
  - B – Authentication & Lifecycle Management
  - C – Federation & Assertions
- Last major revision was in June of 2017.

NIST Special Publication
NIST SP 800-63-4 ipd

Digital Identity Guidelines

Initial Public Draft

David Temoshok
Ryan Galluzzo
Connie LaSalle
Naomi Lefkovitz
Applied Cybersecurity Division
Information Technology Laboratory

Andrew Regenscheid
Computer Security Division
Information Technology Laboratory

Yee-Yin Choong
Information Access Division
Information Technology Laboratory

Diana Proud-Madruga
Sarbari Gupta
Electrosoft

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-4.ipd

December 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Why Are We Making Changes?

NIST

- **Advance equity.**
- **Emphasize optionality and choice for individuals.**
- **Deter phishing, fraud, and advanced threats.**
- **Address lessons learned through real-world implementations.**
- **Emphasize multi-disciplinary risk management processes.**
- **Clarify and consolidate requirements where needed.**

The technical, threat, and political landscapes have shifted since 2017 – our guidance needed to evolve to accommodate these changes

What Aren’t We Changing?

Publication Structure

- There will remain 4 volumes each focused on their respective aspects of digital identity.

Decoupled Assurance Levels (IAL/AAL/FAL)

- There will still be three different types of assurance levels (identity, authentication, and federation) with three levels of assurance each.

Privacy, Usability, and Security

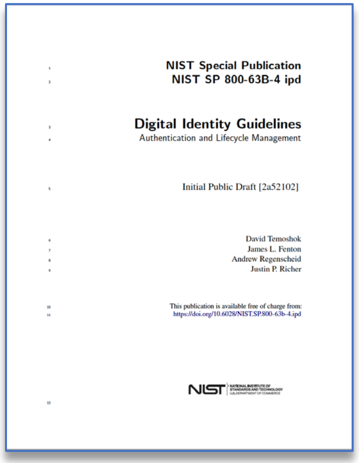
- There will still be emphasis on balancing risks to each of these critical components of identity and solution delivery and volumes continue to include specific requirements and considerations…we’ve just taken things one step further to consider equitable access!

What Are We Changing?

All four volumes feature substantial updates, some of the most impactful include:

- Revamps Risk Management and Assurance Selection Process
- Introduces digital evidence concept (e.g., mDL and Verifiable Credentials)
- Mandates Trusted Referees as an option and introduces Applicant References
- Updated biometric performance requirements for proofing and authentication
- Defines phishing resistance and updates password requirements (e.g., composition & rotation)
- Establishes a new Identity Assurance Level 1 where biometrics are optional
- Provides normative language for the providers and agencies to assess the impact of technology on equity

What Does 800-63 have to do with anything?



NIST Special Publication
NIST SP 800-63B-4 ipd

Digital Identity Guidelines
Authentication and Lifecycle Management

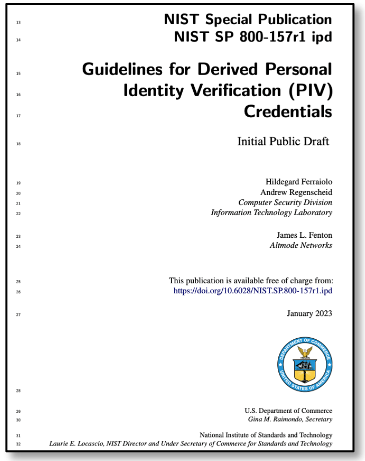
Initial Public Draft [2a52102]

David Temoshok
James L. Fenton
Andrew Regenscheid
Justin P. Richer

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63b-4.ipd

800-63B & 800-157

- Establishes common authentication assurance levels
- Provides technical authenticator requirements for derived authenticators
- Establishes technical requirements for phishing resistance
- 800-157r1 leverages 800-63B as a base of requirements with additional considerations for identity & lifecycle management



NIST Special Publication
NIST SP 800-157r1 ipd

Guidelines for Derived Personal Identity Verification (PIV) Credentials

Initial Public Draft

Hildegard Ferraiolo
Andrew Regenscheid
Computer Security Division
Information Technology Laboratory

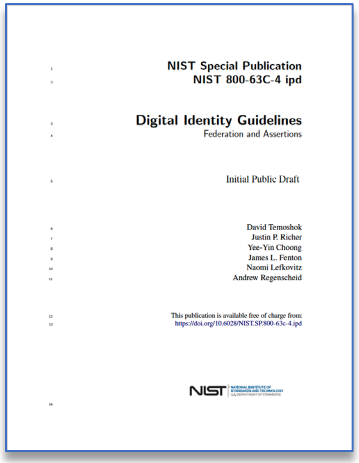
James L. Fenton
Altmode Networks

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-157r1.ipd

January 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology



NIST Special Publication
NIST 800-63C-4 ipd

Digital Identity Guidelines
Federation and Assertions

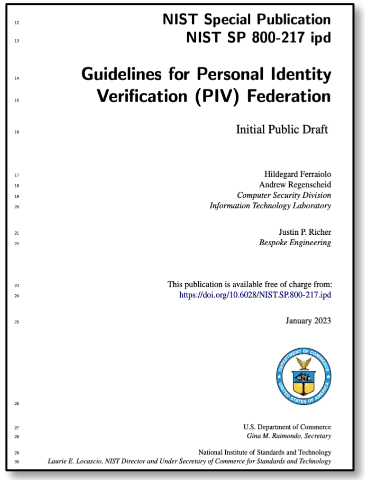
Initial Public Draft

David Temoshok
Justin P. Richer
Yee-Yin Choong
James L. Fenton
Naomi Lefkovitz
Andrew Regenscheid

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63c-4.ipd

800-63C & 800-217

- Establishes common federation assurance levels
- Provides technical requirements for federation and assertions
- Provides guidance for federation trust agreements, registration, and presentation models
- 800-217 serves as a "profile" of 800-63C for PIV applications



NIST Special Publication
NIST SP 800-217 ipd

Guidelines for Personal Identity Verification (PIV) Federation

Initial Public Draft

Hildegard Ferraiolo
Andrew Regenscheid
Computer Security Division
Information Technology Laboratory

Justin P. Richer
Bespoke Engineering

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-217.ipd

January 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

The Digital Identity Guidelines – particularly volumes B & C – provide the framework for the updates to SP 800-217 and SP 800-157-1

Comment Submission

- Where can I find the documents?
  - 800-63-4: Base Volume
  - 800-63A-4: Identity Proofing and Enrollment
  - 800-63B-4: Authentication and Lifecycle Management
  - 800-63C-4: Federation and Assertions
- How do I submit comments?
  - Email them to: dig-comments@nist.gov
- What format should my comments be in?
  - The preferred format is the comment sheet available here: Comment template (xls)
- What kind of comments are most helpful?
  - All of them!
  - Reference our Note to Reviewers for specific questions
  - Please do not send marketing material
- What if I have questions before I submit comments?
  - Email any questions or requests for clarifications you may have to: dig-comments@nist.gov
  - We will do our best to respond to as many questions as possible
- Will my comments be made public?
  - Yes! Our process is open and transparent and we will post all comments as issues on our GitHub repository
- How can I keep up to speed on any changes?
  - There will not be changes to the text between now and the close of the comment period
  - But, if we get frequent comments or areas where clarification is regularly requested, we will post them to our “Ongoing Updates” page
  - Follow along at: https://pages.nist.gov/800-63-4/

COMMENTS ARE DUE MARCH 24th!!!!

The webinar will resume shortly

NIST SP 800-157, Revision 1:
Guidelines for Derived PIV Credentials

Andrew Regenscheid
Jim Fenton

Derived PIV Guidelines Overview

Purpose:

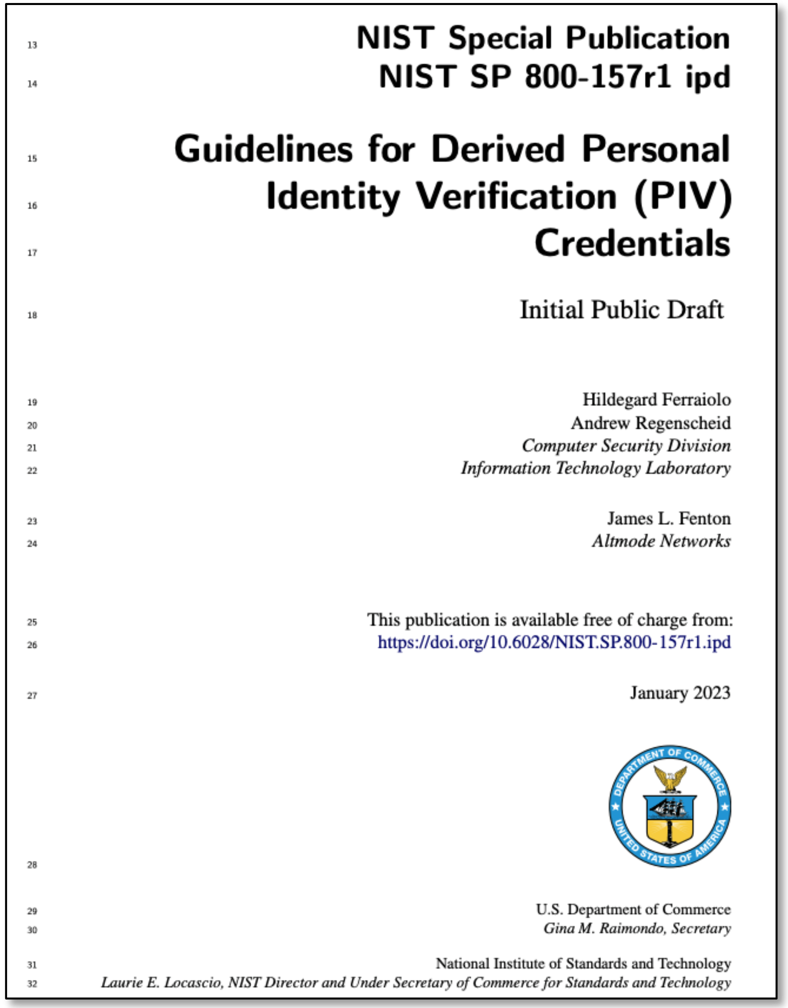
- Support additional authenticators as derived PIV credentials
- Allow derived PIV credentials on additional platforms

Scope:

- Issuance/binding and management activities by PIV issuer
- Phishing-resistant multifactor authenticators based on Draft SP 800-63B-4
  - PKI-based Derived PIV credentials
  - Non-PKI-based authenticators

Authentication Assurance Levels

AAL1	~~• Single-factor authentication~~ ***-63B level not supported in -157r1***
AAL2	• Multifactor authentication, ***-157r1 specifies phishing resistance***
AAL3	• Hardware-based, cryptographic multifactor authentication



NIST Special Publication
NIST SP 800-157r1 ipd

Guidelines for Derived Personal Identity Verification (PIV) Credentials

Initial Public Draft

Hildegard Ferraiolo
Andrew Regenscheid
Computer Security Division
Information Technology Laboratory

James L. Fenton
Altmode Networks

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-157r1.ipd

January 2023

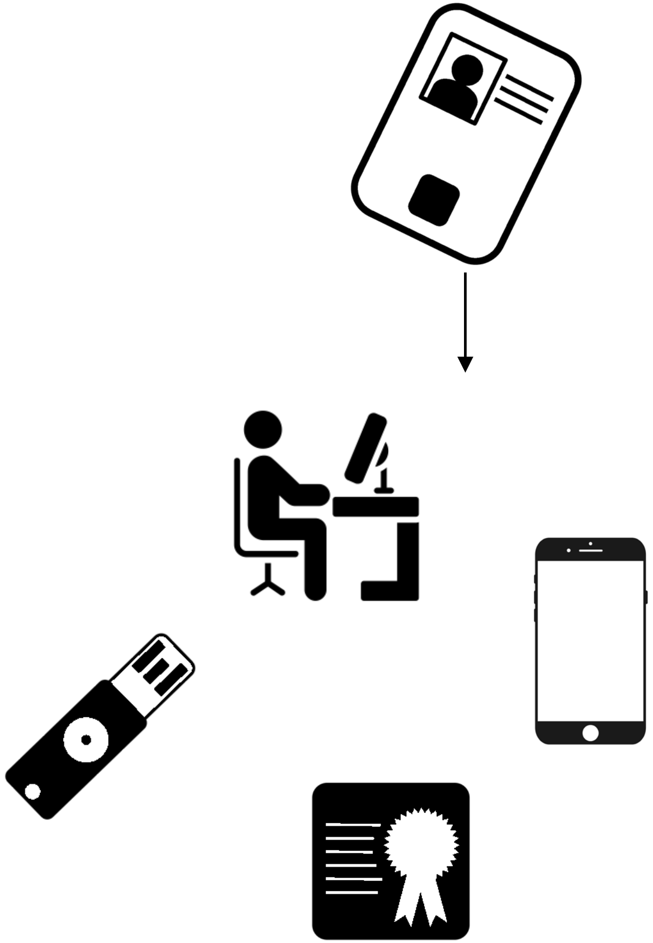
U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

New aspects of SP 800-157r1

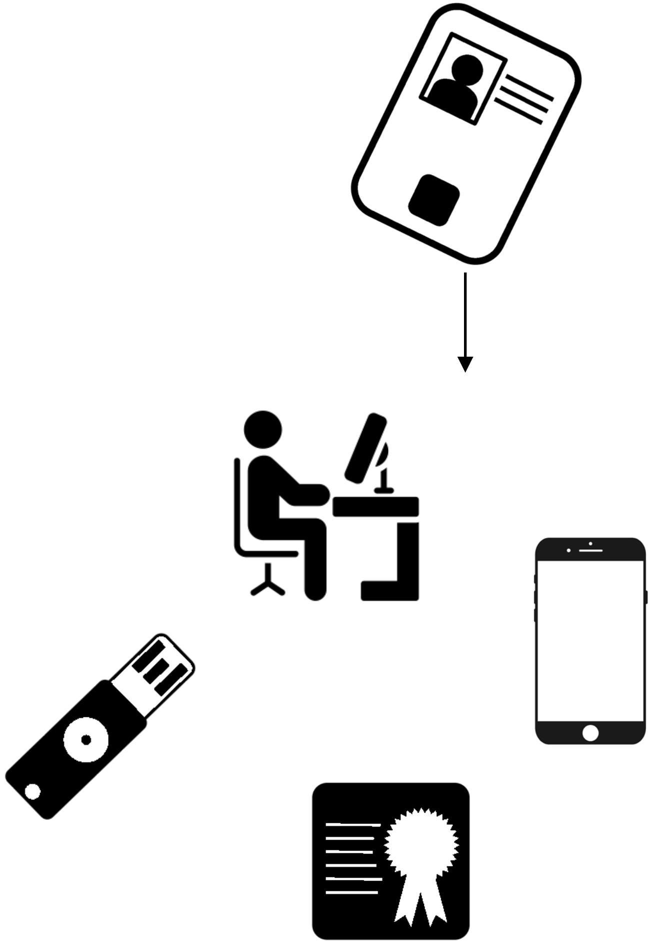
Revision of NIST SP 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials* (December 2014)

- Broaden use of Derived PIV Credentials beyond mobile devices
- Guidelines for the use of other authenticators as derived PIV credentials
- Support for both embedded and separate authenticators
- New guidelines for use of wireless authenticators for derived PIV authentication
- Align authenticator requirements with SP 800-63B-4



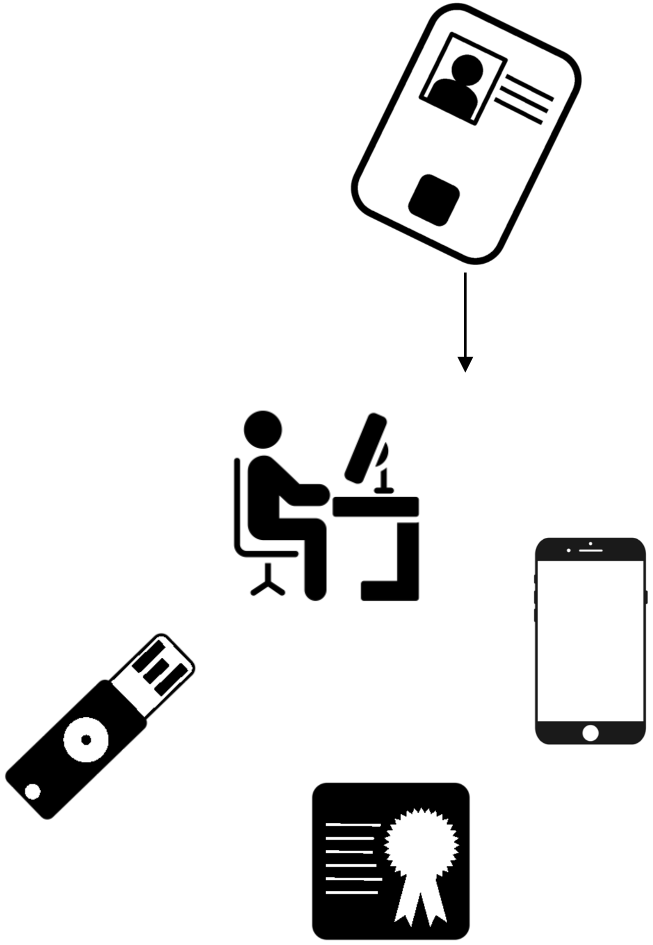
Classes of Authenticators

- **SP 800-157r1 recognizes two classes of authenticators as derived PIV credentials**
  - PKI-based credentials (supported since initial SP 800-157)
  - Non-PKI-based credentials (addition in SP 800-157 Revision 1)
- **Different lifecycle characteristics**
- **Phishing resistance required**
  - Requires a connection between authenticator and user’s device
- **Non-PKI-based derived PIV credentials require federation for interoperability and interagency use**
- **Either class can be connected or embedded in user device**
- **Issuance of derived PIV credentials (and types and numbers of them) remains *optional* by issuing agencies**



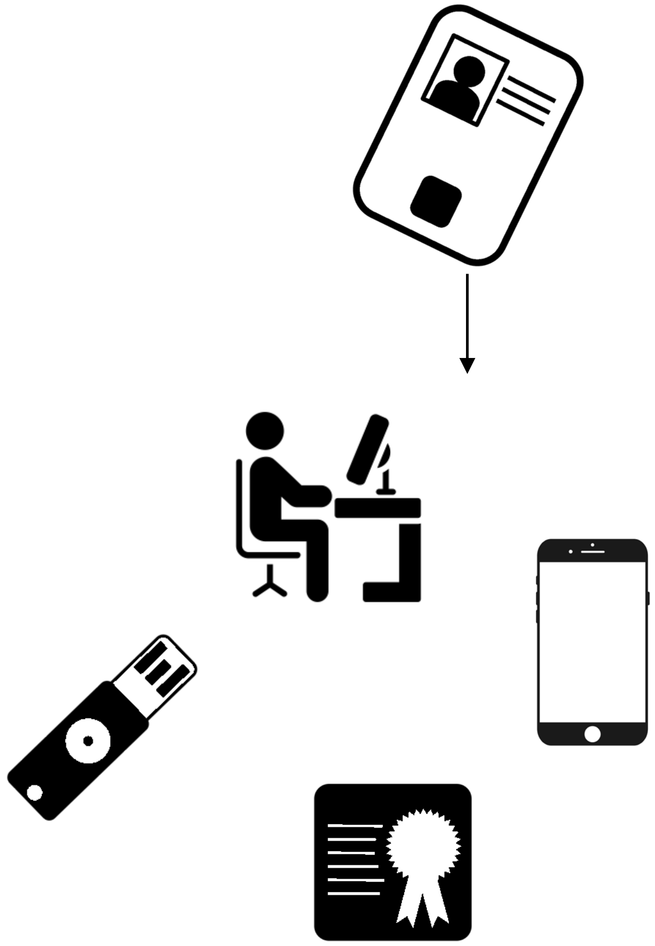
PKI-based and non-PKI-based

- **PKI-based derived PIV credentials**
  - Certificate-based
  - Carry identifying information (attributes) about PIV cardholder
  - Defined expiration
  - Invalidation by collection or inclusion in certificate revocation list (CRL)
- **Non-PKI-based derived PIV credentials**
  - They are also cryptographic authenticators with public keys
  - It’s the lack of “infrastructure” that differentiates them
    - No explicit expiration
    - No revocation (since no CRL)
    - No cardholder attributes
  - Invalidation depends on the issuing agency no longer accepting it for authentication, e.g., if PIV identity account is terminated
  - Issuing agency is required to do all authentication
  - Other agencies accepting non-PKI derived PIV credentials must use federation
    - This also makes attributes available



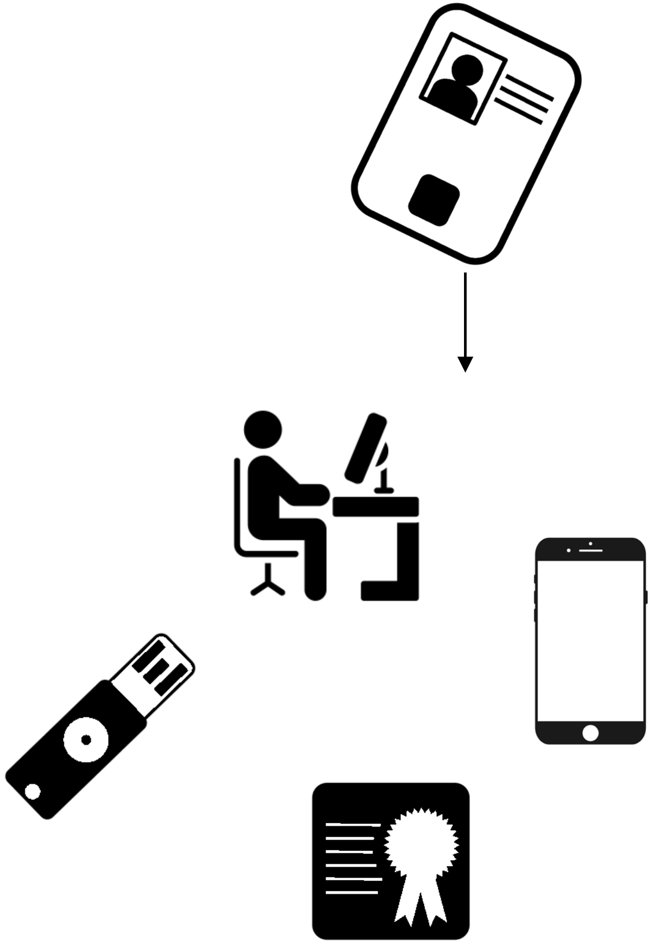
Lifecycle Considerations

- **Derived PIV credentials are tied to the PIV identity account, not the PIV Card**
  - Remain valid if PIV Card is lost/damaged
  - Useful as backup credentials until PIV Card can be replaced
- **PKI-based derived PIV credential lifecycle similar to that of PIV Cards**
  - Issuance based on PKI-AUTH authentication with PIV Card rather than identity proofing and registration
  - Rekey and modification as required, e.g., expiration or name change
- **Non-PKI-based derived PIV credential is a little different**
  - Issuance similar to PKI-based
  - Rekey and modification not expected
  - Usage requires direct communication with PIV identity account
- **Issuer must ensure invalidation of all derived PIV credentials when PIV identity account is terminated**



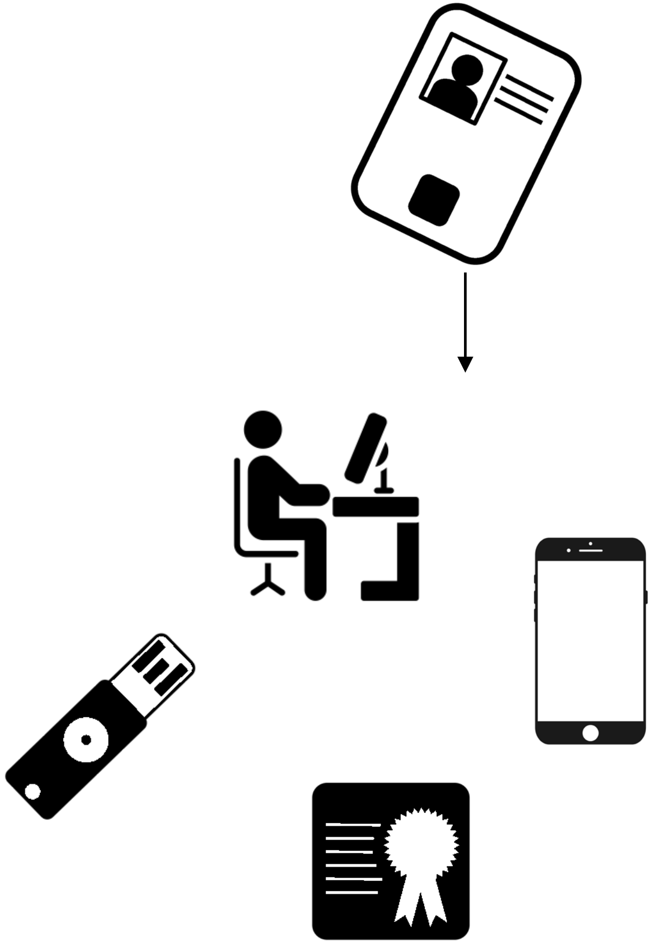
Connected Authenticators

- **Derived PIV credentials are no longer limited to mobile devices**
  - May be embedded in other types of user devices (e.g., desktop and laptop computers)
  - May also be separate authenticators
    - USB devices containing and validating certificates
    - Other non-PKI devices, such as FIDO2
- **Phishing resistance requires the authenticator to be connected to the user's device**
  - Connection can be wired or wireless
  - Wireless connection requirements similar to that of PIV Card (e.g., virtual contact interface)
  - See also SP 800-63B-4 Sec. 5.2.12 for general requirements



Derived PIV and AAL

- **Derived PIV credentials can be issued at authentication assurance level (AAL) 2 or 3**
- **Authentication Assurance Level 2 (AAL2)**
  - Hardware or software-based multifactor cryptographic authenticator
  - Must be phishing resistant
  - Similar to LOA3 derived PIV credentials
- **Authentication Assurance Level 3 (AAL3)**
  - Hardware-based multifactor cryptographic authenticator
  - Must be phishing resistant (AAL3 requirement)
  - Private key is generated on-device and never leaves the device
  - Suitably secure security processors (e.g., TPM, TEE) are considered “hardware” if the private key cannot be exported
  - Similar to LOA4 derived PIV credentials



Targeted Issues for Comment/Feedback

- Are the new controls for issuance, use, maintenance, and termination of non-PKI-based derived PIV credentials clear and practical to implement?

- Are phishing-resistant authenticators available to meet agency use cases as well as the requirements for derived PIV authentication?

- Are the new controls sufficient to provide comparable assurance to PIV Cards and other derived PIV credentials?

NIST SP 800-217:
Guidelines for PIV Federation

Andrew Regenscheid
Justin Richer

PIV Federation Guidelines Overview

Scope: Federation and Assertions from PIV Identity Accounts

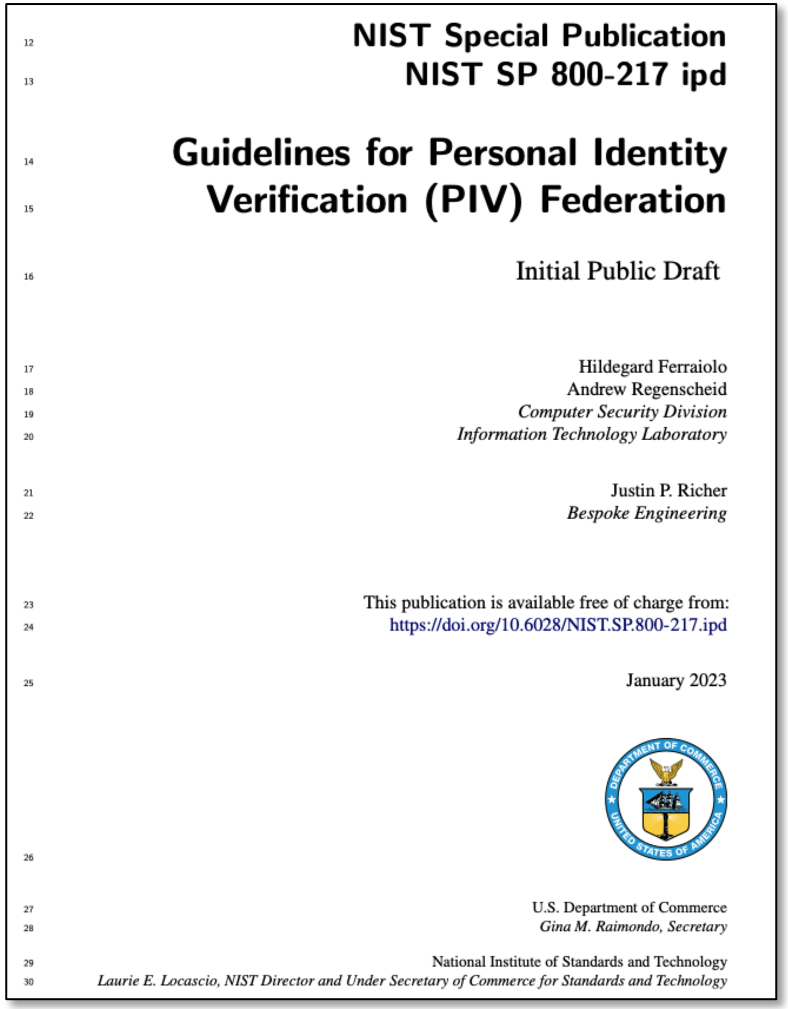
- Architectures and use cases – interagency trust and enterprise SSO
- PIV Identity Providers
- Trust agreements
- Attributes and assertion contents
- Relying Party responsibilities

Purpose:

- Foundation for providing technical interoperability and interagency trust
- Applies and extends guidelines from Draft SP 800-63C-4
- Objective-driven – deployments will need protocol-specific profiles

Federation Assurance Levels

FAL1	• Basic protections supported by a broad range of technologies
FAL2	• Assertion injection protection using modern federation protocols
FAL3	• Protection against assertion theft/forgery using RP-side authentication



NIST Special Publication
NIST SP 800-217 ipd

Guidelines for Personal Identity Verification (PIV) Federation

Initial Public Draft

Hildegard Ferraiolo
Andrew Regenscheid
Computer Security Division
Information Technology Laboratory

Justin P. Richer
Bespoke Engineering

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-217.ipd

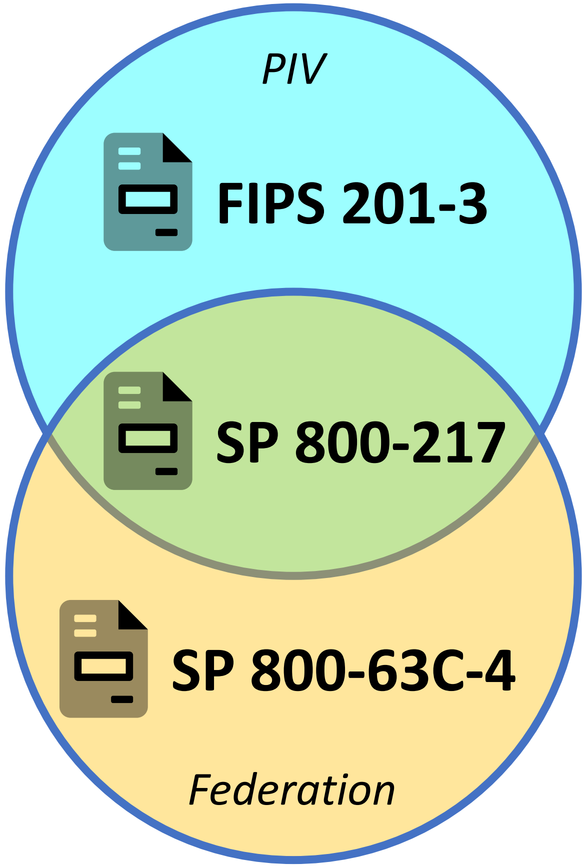
January 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

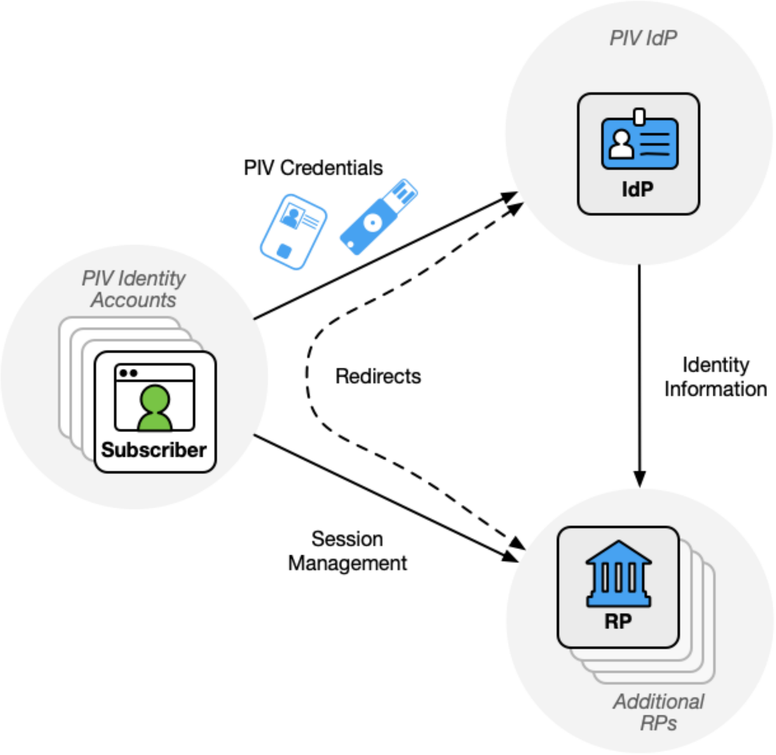
Relationship to Other Documents

- **FIPS201-3**: defines PIV identity accounts, PIV Cards, account management and lifecycle
- **SP 800-63C-4**: defines requirements and best practices for federation and assertions
  - Part of the SP 800-63-4 *Digital Identity Guidelines* suite
- **SP 800-217**: defines *PIV federation*
  - Guidelines for using federation protocols in the PIV ecosystem



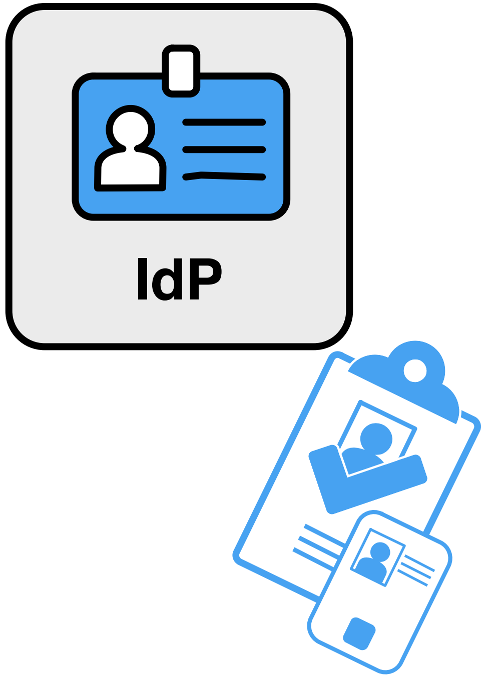
PIV Federation

- Federated authentication of **PIV identity accounts**
  - Other accounts are out of scope
- Uses PIV credentials for primary authentication at the IdP
  - Either PIV Card or derived PIV credential
- Allows use of non-PKI-based derived PIV credentials across domain boundaries
  - IdP has to be associated with the issuing agency in this case
  - Subscriber logs in at the IdP with their derived PIV credential
  - Federation protocol allows subscriber to log in to the RP
- Limits reliance on PKI credentials and systems at RPs



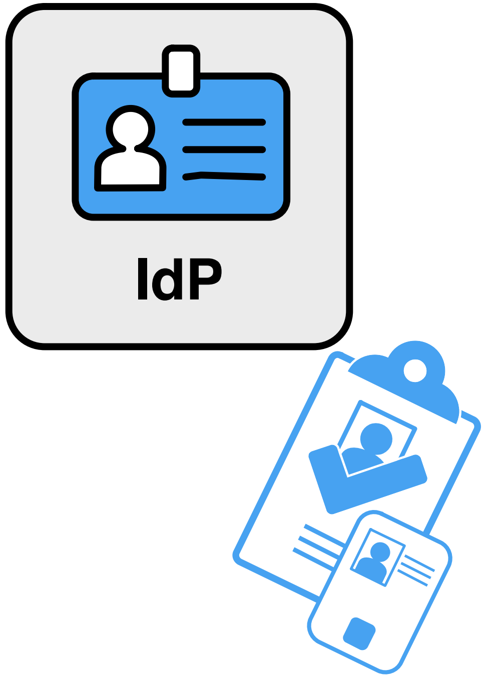
PIV IdP

- The IdP trusted by the RP for a PIV federation transaction
  - Defined in the trust agreement between the RP and IdP
- RP maps the PIV identity account to a PIV IdP
  - Deterministic mapping defined in the trust agreement
  - Determined by organization, agency, individual account, etc.
- Uses PIV credentials for authentication
  - Could be run by or on behalf of issuing agency
  - Could be a proxy or a PKI-enabled gateway (at FAL1)
- See Section 5.1 in SP 800-63C-4 for guidance on trust agreements



Home IdP

- The officially-declared IdP of a given issuing agency
  - Applies to all PIV identity accounts issued and managed by that agency
  - Only one home IdP for any agency at a time
  - Operated by or on behalf of the issuing agency
  - Provides a stable federated identifier for each PIV identity account
- Additional requirements beyond "generic" PIV IdP
  - Assumes close relationship with PIV identity account management
  - Aware of current status of PIV identity account
  - Can verify any PIV credentials bound to the account
- Issuing agency publishes a record of the home IdP's properties
- PIV IdP is required to be the home IdP at FAL2 and FAL3

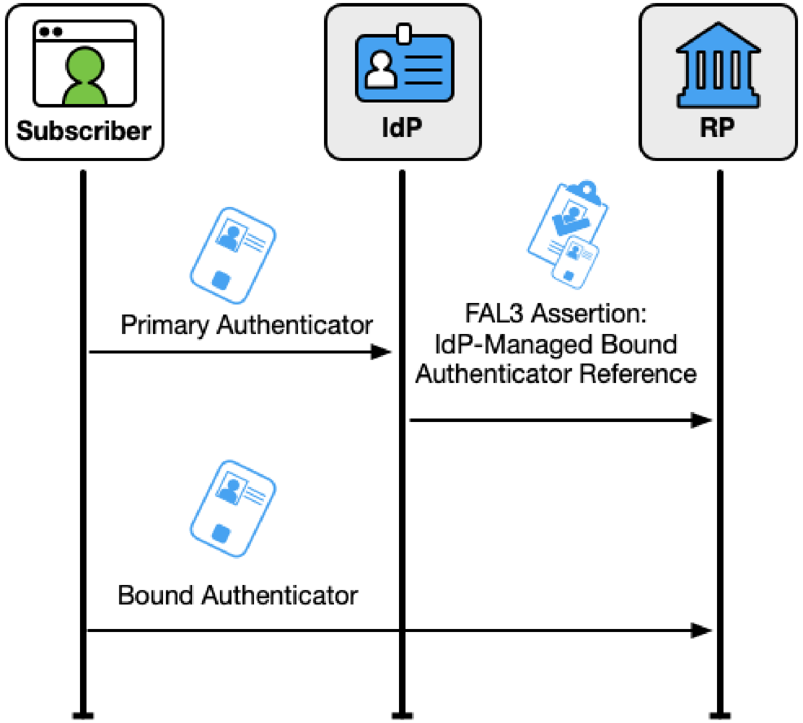


Federation Assurance Level

- Additional requirements on top of SP 800-63C-4
- **FAL1:** Base Level
  - Best practices of current federation protocols.
  - Allow for non-home IdPs, such as a PKI-to-federation bridge.
  - Allow for dynamic connection to unknown RPs.
  - Allow for low-risk connections.
- **FAL2:** Strong connection to home IdP
  - *Recommended target for most PIV federation scenarios.*
  - Required use of back-channel assertion presentation.
  - Required use of ***home IdP*** for a given PIV identity account.
- **FAL3:** Proof of Possession of a Bound Authenticator
  - Requires use of a ***bound authenticator*** – an authenticator verified by the RP in addition to an assertion.
  - Strongly mitigates assertion theft and forgery attacks.

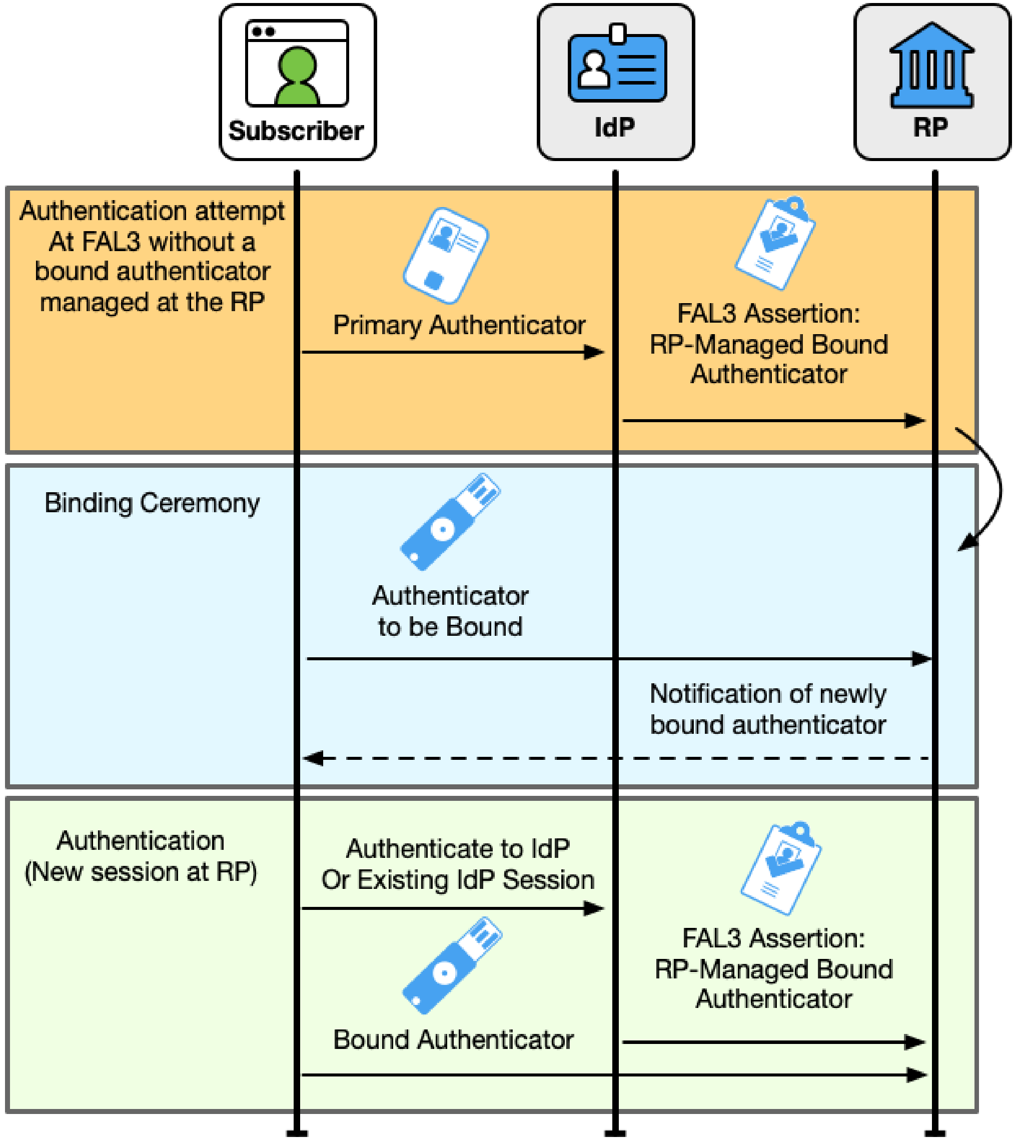
Bound Authenticators – IdP Managed

- IdP binds an authenticator to the PIV identity account that can also be presented to the RP.
- ***Authentication Process:***
  - Subscriber authentication to IdP using primary authenticator.
    - Could be a PIV Card or derived PIV credential.
  - IdP assertion references identifier of bound authenticator.
  - RP verifies:
    - The contents of the assertion from the IdP.
    - Subscriber possession of the identified bound authenticator.
- ***Bound Authenticator Requirements:***
  - Mutually trusted by IdP and RP.
  - Independently verifiable by the RP – e.g., a PKI certificate.
    - Usually the PIV Card's authentication certificate, could be a PKI-based derived PIV credential.
  - Phishing-resistant authentication process.



Bound Authenticators – RP Managed

- RP binds an authenticator in the RP subscriber account as part of a binding ceremony.
- ***Binding Ceremony:***
  - Could use RP or subscriber-provided authenticators.
  - ***Trust on first use*** model allowed with initial assertion presentation to RP.
  - Provide out-of-band notification to subscriber.
- ***Authentication Process:***
  - Subscriber authentication to IdP using a PIV credential.
  - IdP assertion includes indicator for the RP to verify a bound authenticator.
  - RP verifies:
    - The contents of the assertion from the IdP.
    - Subscriber possession of an authenticator bound to the RP subscriber account using a phishing resistant process.


Subscriber
IdP
RP
Authentication attempt At FAL3 without a bound authenticator managed at the RP
Primary Authenticator
FAL3 Assertion: RP-Managed Bound Authenticator
Binding Ceremony
Authenticator to be Bound
Notification of newly bound authenticator
Authentication (New session at RP)
Authenticate to IdP Or Existing IdP Session
Bound Authenticator
FAL3 Assertion: RP-Managed Bound Authenticator

Targeted Issues for Comment/Feedback

Home IdP Attributes:

- Are additional attributes needed in the guidelines to achieve interagency or cross-domain interoperability?
- Are additional attributes required for RP provisioning and access?

PIV Federation:

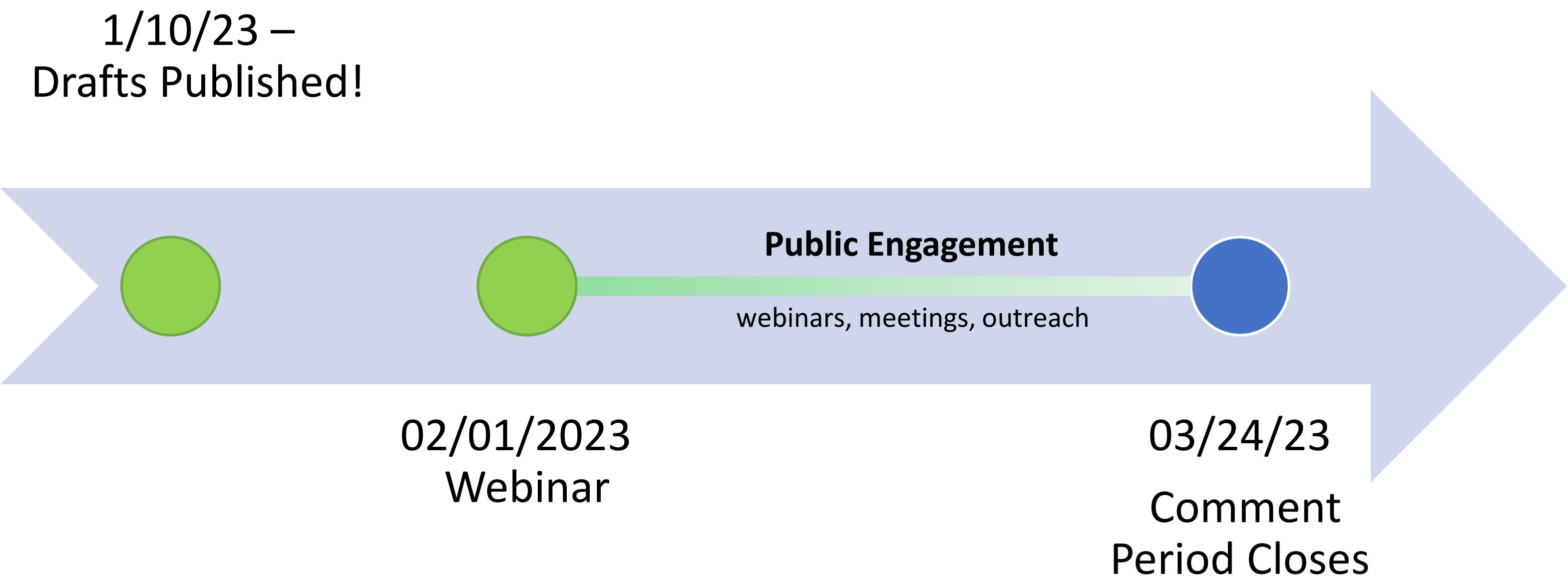
- Are additional process steps or mechanisms needed for the connection and communication between home IdP and PIV identity account?
- Do the required parameters for establishing trust agreements fit the use cases for PIV RPs?
- Are the required identity attributes sufficient for PIV use cases?
- Are the federated subject identifier requirements sufficient for PIV use cases?
- Is it clear how to apply the binding ceremony for RP-managed bound authenticators at FAL3 to PIV and non-PIV authenticators?

Key Dates and Next Steps

Hildegard Ferraiolo, NIST PIV Program Lead

Key Dates

The release of the drafts on 1/10 kicked off a comment period to collect feedback and conduct engagement with the public, government, and industry.



1/10/23 –
Drafts Published!

Public Engagement

webinars, meetings, outreach

02/01/2023
Webinar

03/24/23

Comment
Period Closes

What happens during the public comment period?

- Engagement & Outreach
- Continued Research
- Triage of Comments

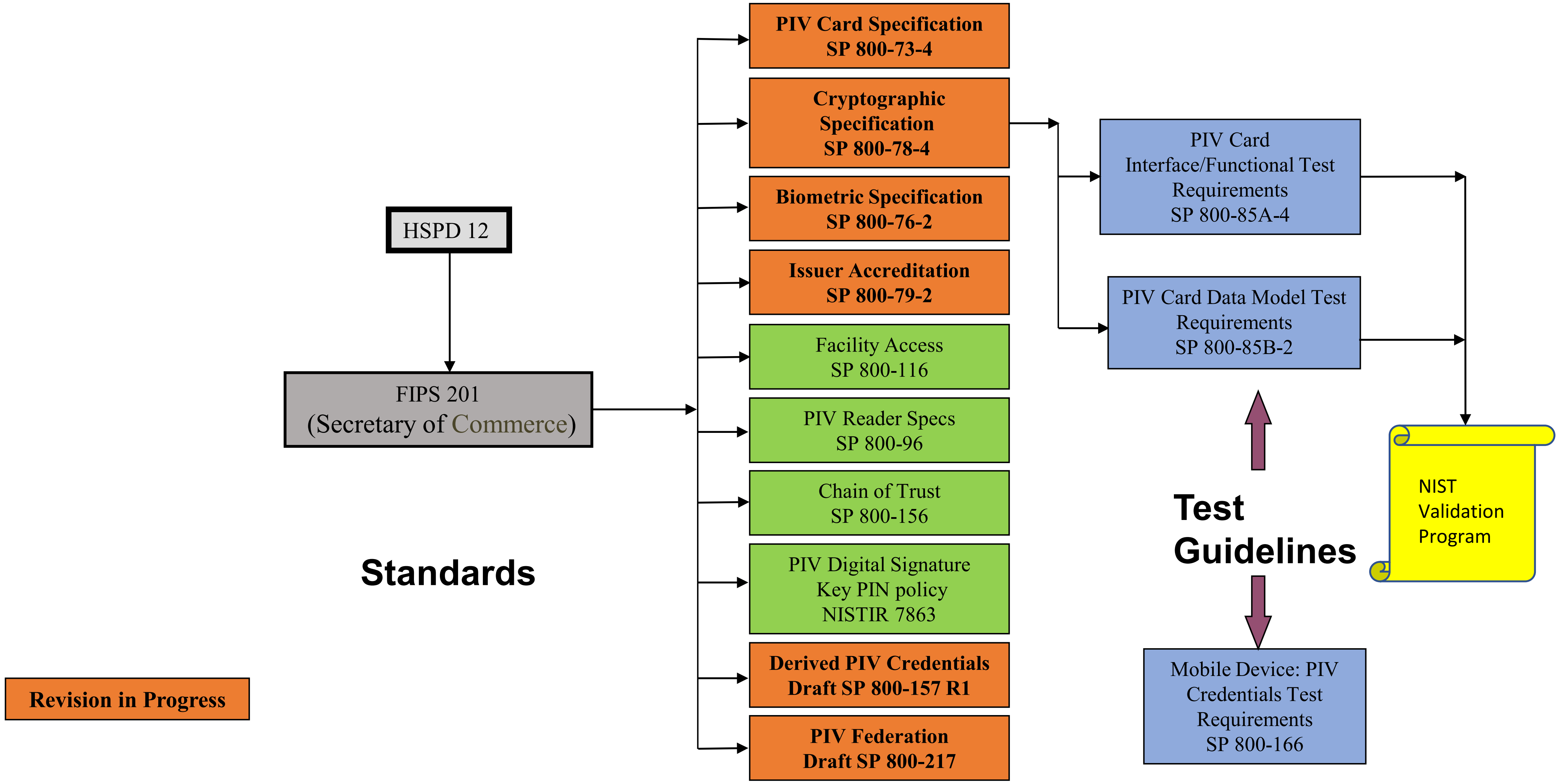
What happens after the comment period?

- Review and adjudication of comments
- Engagement to clarify or elaborate
- Additional research on input
- final publication

Comment Submission

- When are comments due?
  - March 24, 2023
- Where can I find the documents?
  - Draft SP 800-157 R1 Guidelines for Derived PIV Credentials
  - Draft SP 800-217 - Guidelines for PIV Federation
- How do I submit comments?
  - Email them to: piv_comments@nist.gov
- What format should my comments be in?
  - The preferred format is the comment sheet available here:
    - Draft SP 800-157 R1 Comment template (xls)
    - Draft SP 800-217 Comment template (xls)
- What kind of comments are most helpful?
  - All of them!
  - Please do not send marketing material
- What if I have questions before I submit comments?
  - Email any questions or requests for clarifications you may have to: piv_comments@nist.gov
  - We will do our best to respond to as many questions as possible
- Will my comments be made public?
  - Yes! Our process is open and transparent and we will post all comments as issues on our GitHub repository

There is more: Further PIV Guidelines Update



HSPD 12

FIPS 201
(Secretary of Commerce)

Standards

PIV Card Specification
SP 800-73-4

Cryptographic Specification
SP 800-78-4

Biometric Specification
SP 800-76-2

Issuer Accreditation
SP 800-79-2

Facility Access
SP 800-116

PIV Reader Specs
SP 800-96

Chain of Trust
SP 800-156

PIV Digital Signature Key PIN policy
NISTIR 7863

Derived PIV Credentials
Draft SP 800-157 R1

PIV Federation
Draft SP 800-217

PIV Card Interface/Functional Test Requirements
SP 800-85A-4

PIV Card Data Model Test Requirements
SP 800-85B-2

Test Guidelines

Mobile Device: PIV Credentials Test Requirements
SP 800-166

NIST Validation Program

Revision in Progress

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

NIST
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
UNITED STATES DEPARTMENT OF COMMERCE
100 Bureau Drive

Thank you for your participation today!