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

Personal Identity Verification (PIV) Webinar:

PIV Interface Specifications (SP800-73-5 Draft)
PIV Cryptographic Specifications (SP800-78-5 Draft)

NIST Information Technology Lab

For closed captioning go to:
https://www.streamtext.net/player?event=BIS-NIST-6022730

November 8, 2023

Welcome & Session Overview

Hildegard Ferraiolo, NIST PIV Program Lead

Why are we here today?

Purpose:

- Raise awareness of the comment period for updated PIV guidelines:
  - PIV Card Data Model and Interface Specifications (Draft SP 800-73-5) and
  - Cryptographic Specifications for PIV Card and associated PIV system (Draft SP 800-78-5)
- To describe the new guidelines
- To enumerate the public comment process and timeline

Outcomes:

- ✓ You gain an understanding of the updated guidelines and how they fit into the broader PIV program
- ✓ Better understanding == > insightful, targeted comments to further improve guidelines
- ✓ You will have details on the comment period and how to submit comments to the PIV team

What will we be discussing?

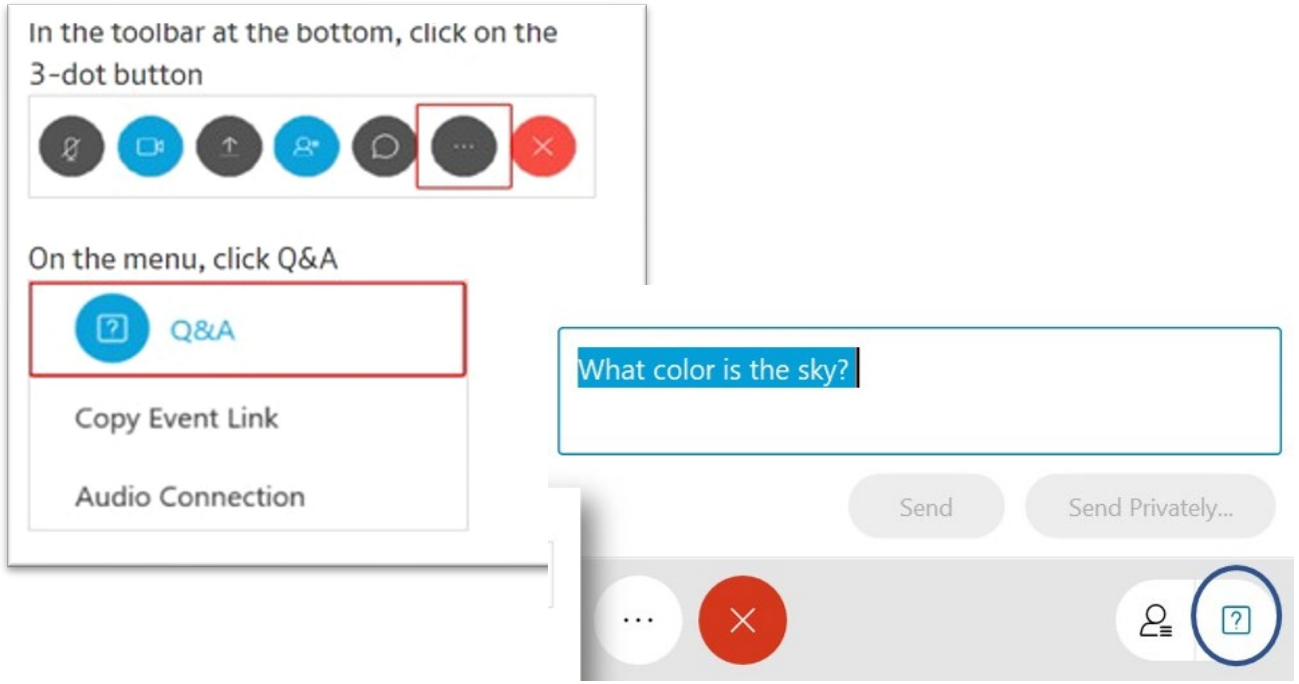
Item	Speaker	Time
Welcome	Hildegard Ferraiolo	5 minutes
Introduction to the PIV Standard	Hildegard Ferraiolo	10 minutes
Changes to SP 800-73 R5	Hildegard Ferraiolo Sarbari Gupta	30 minutes
Changes to Draft SP 800-78 R5	Hildegard Ferraiolo Andy Regenscheid	30minutes
Key Dates & Next Steps	Hildegard Ferraiolo	5 minutes

Have Questions? Please use the Q&A feature on Webex to submit questions. We will address select questions after each session.

Audience Engagement

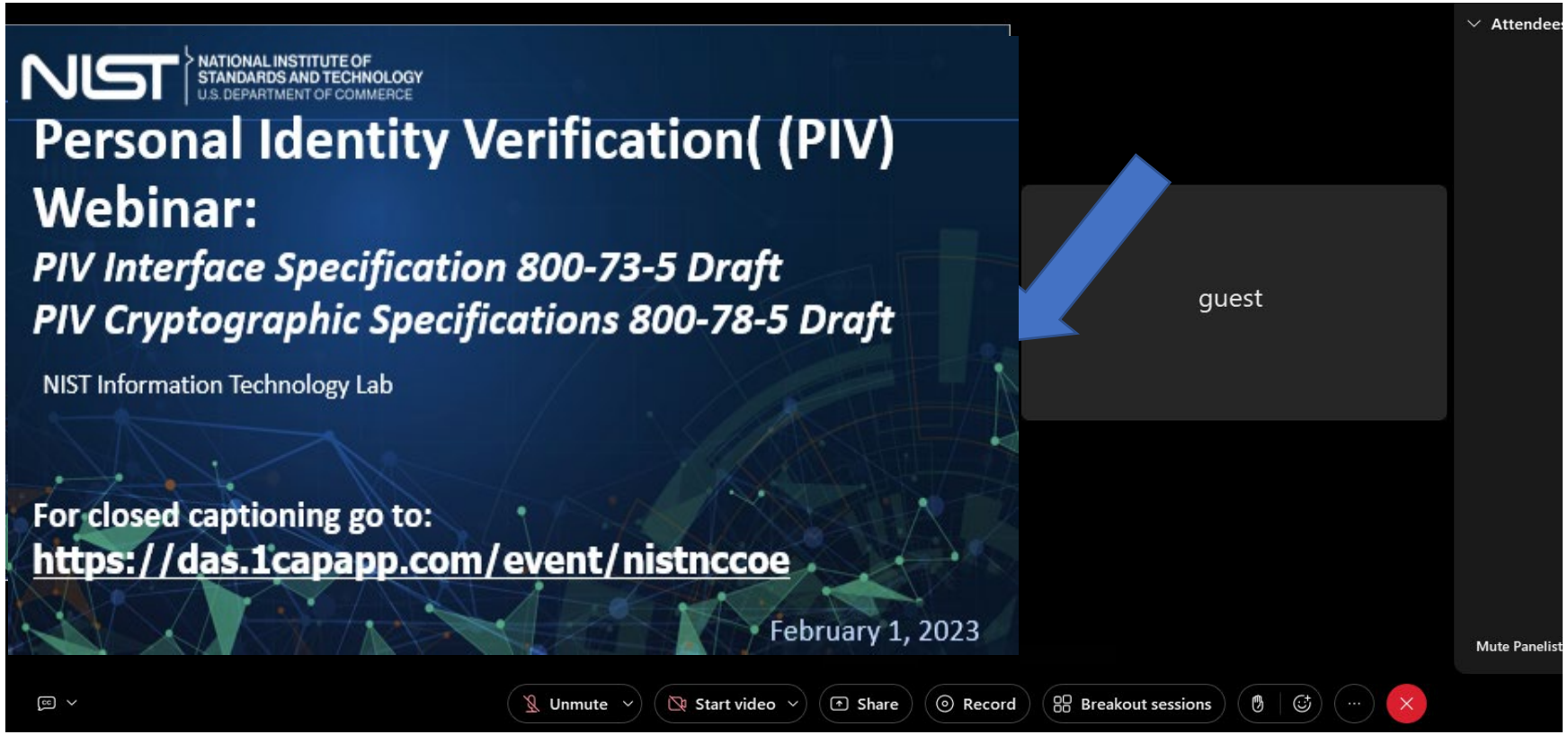
Please use the Q&A window to enter your questions for today's event.

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**.



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.



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
  - New authenticators -> Derived PIV Credentials
- Align with New Policy
  - (i.e., OMB, OPM)

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

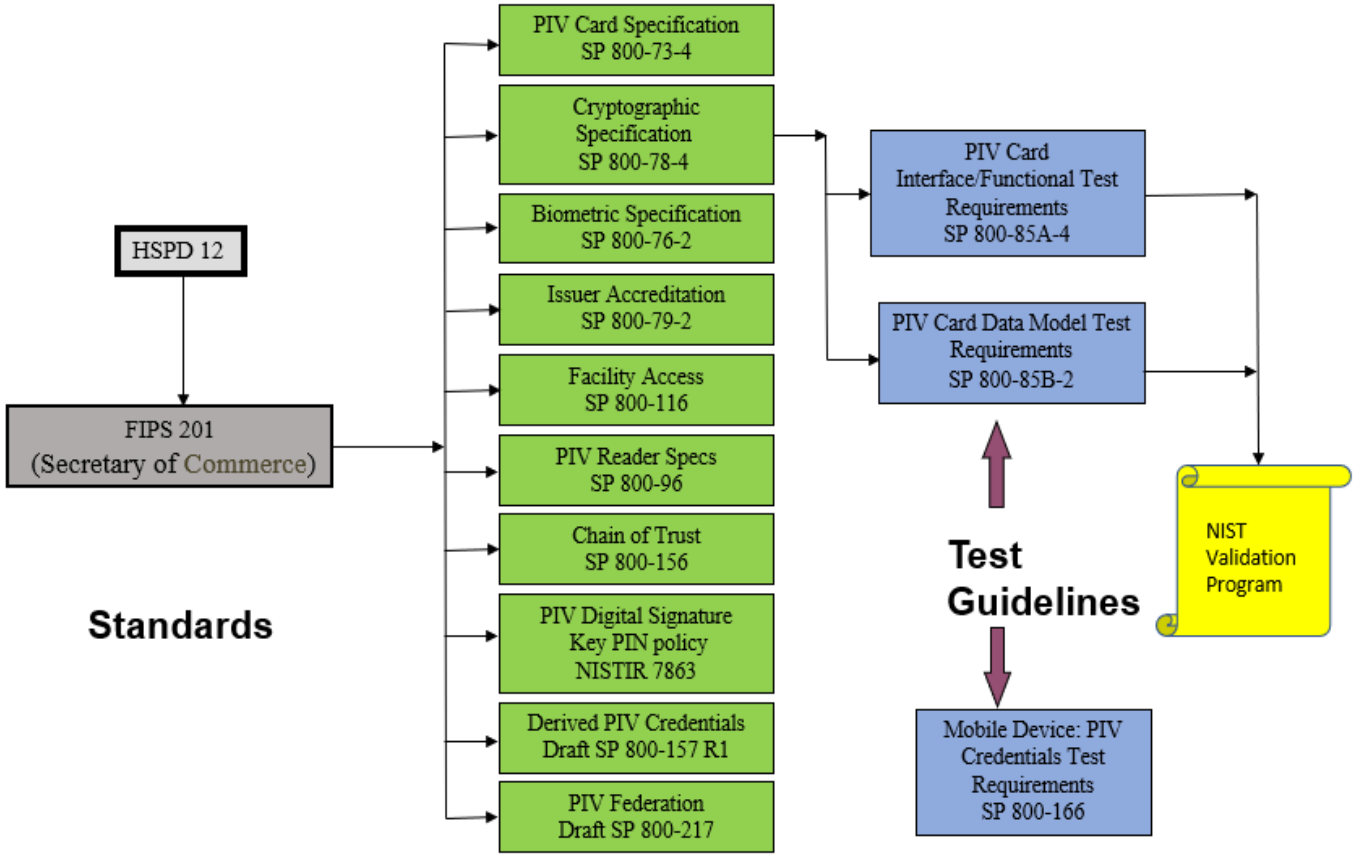
→ Card/application interface specifications
→ PIV Reader specifications
→ *Federation (new with FIPS 201-3)*

Trust enablement

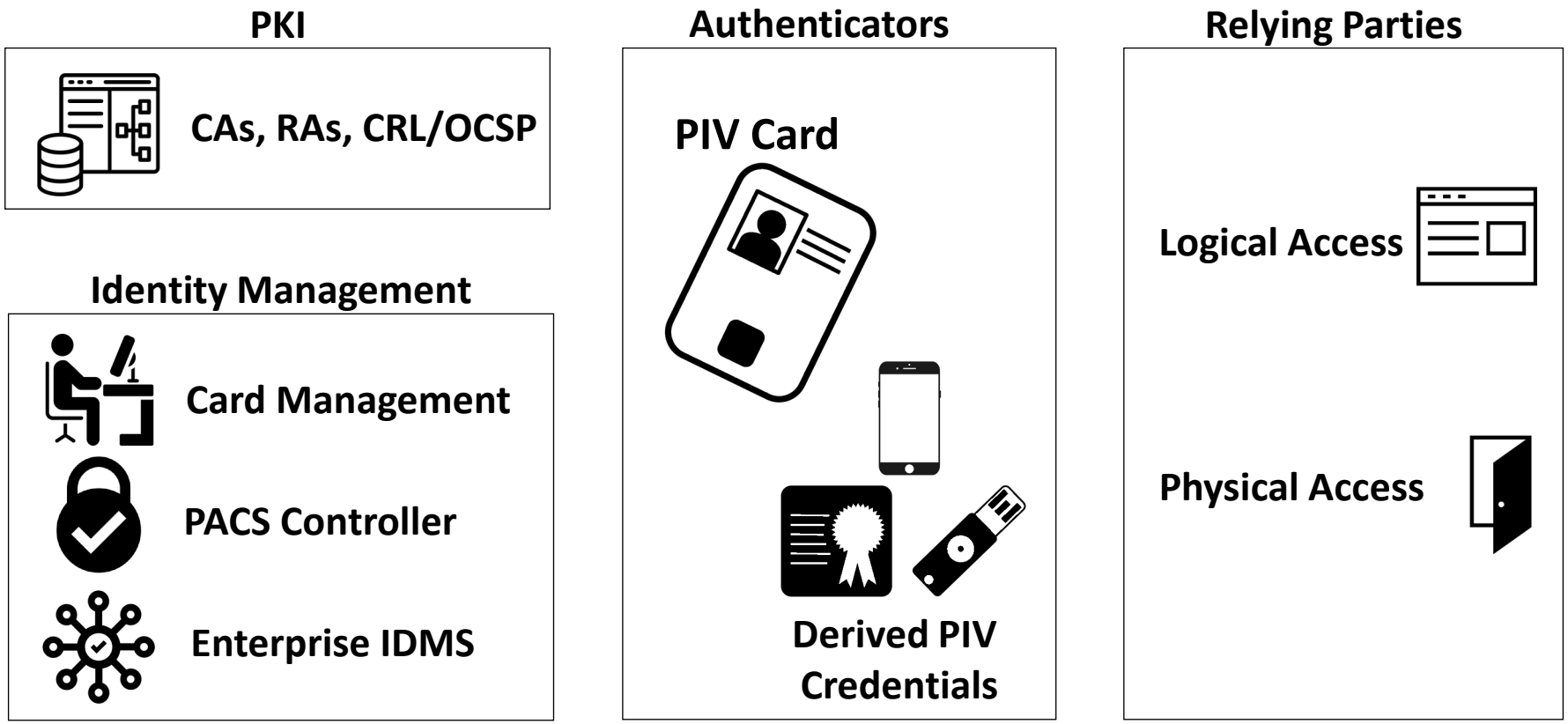
→ PIV Issuer accreditation guidelines

Privacy

→ Requirements for PIV issuers and implementers



PIV Architecture



PIV Architecture

Focus today

PKI

CAs, RAs, CRL/OCSP

Identity Management

Card Management

PACS Controller

Enterprise IDMS

Authenticators

PIV Card

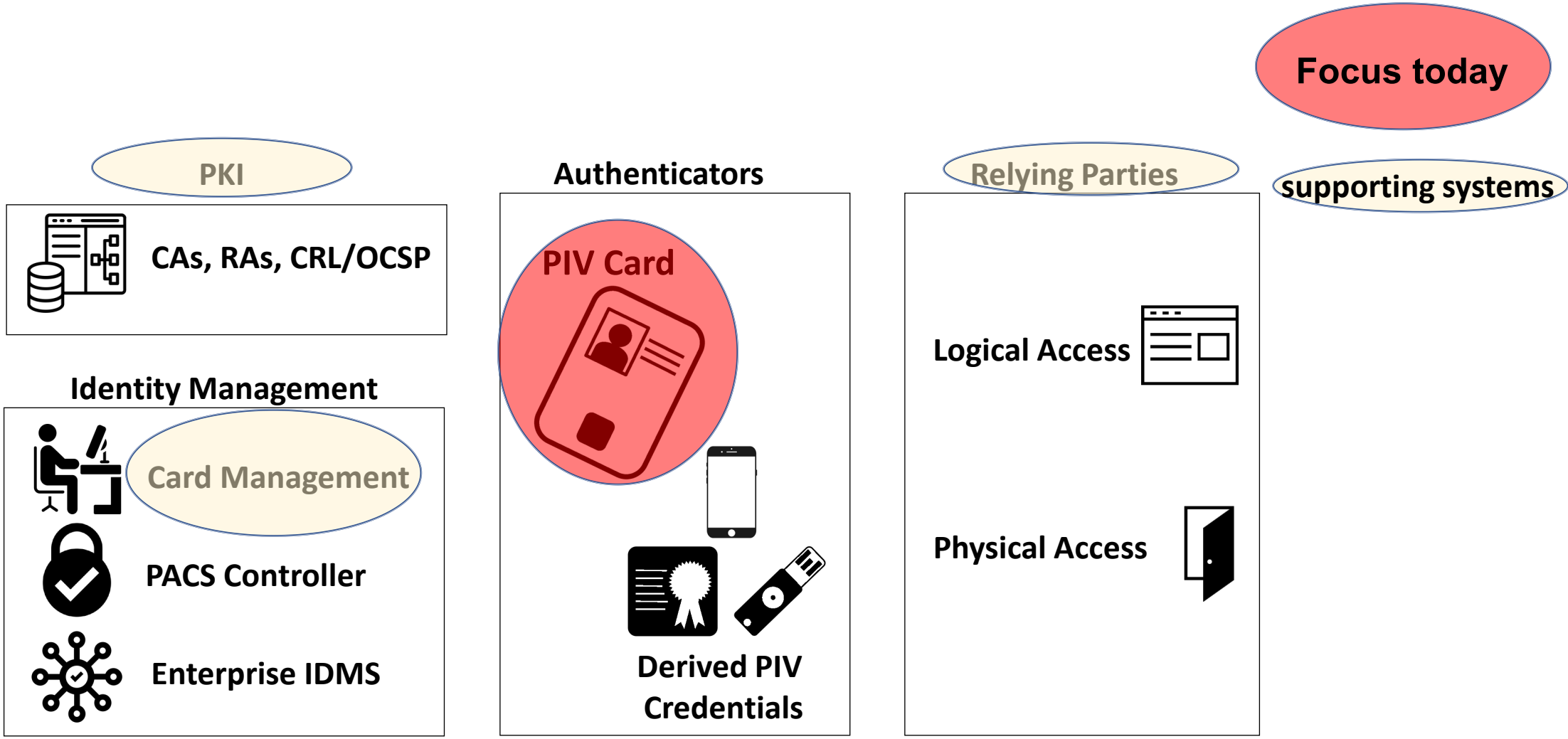
Derived PIV Credentials

Relying Parties

Logical Access

Physical Access

PIV Architecture



Draft NIST SP 800-73, Revision 5:

Data Model and *Interfaces for the PIV Card* ***in 3 Parts***

Hildegard Ferraiolo
Sarbari Gupta

SP 800-73 Revision 5 (3-Parts)

Scope:

- A companion document of FIPS 201 that contains the technical specification/details of the FIPS 201-3 defined PIV card

- Includes specifications for:
  - The Card's on-board credentials and
  - Its services (authentication, encryption and signing)

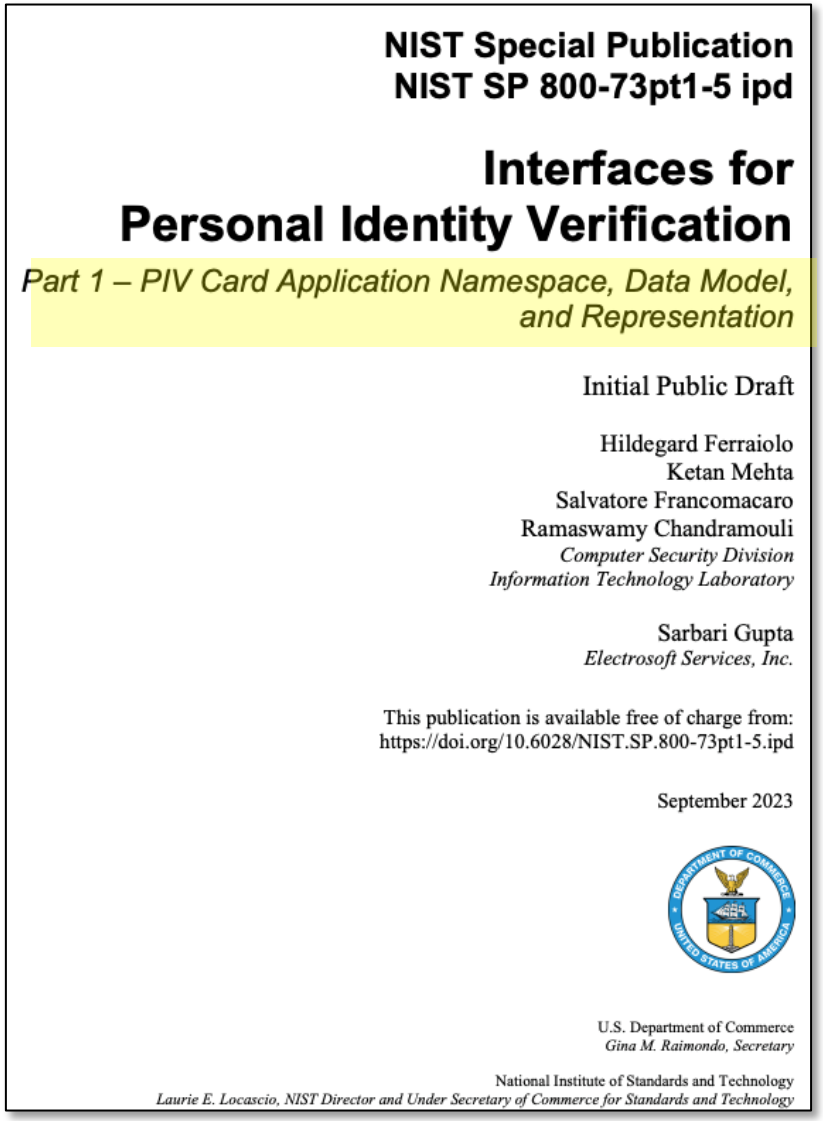
Purpose:

- Enable inter-agency interoperable use of PIV Cards to retrieve and use on-board identity credentials
- For authentication, signing and encryption in federal application s (e.g., to access to federally controlled facilities and information systems)

Part 1 of SP 800-73 Revision 5

PIV Data Model:

- Defines the PIV card application, the data model and how credentials are represented - including
  - PKI Credential (PKI-AUTH, PKI-CAK)
  - Biometric (fingerprint, facial, iris)
  - Encryption and Signing key



NIST Special Publication
NIST SP 800-73pt1-5 ipd

Interfaces for Personal Identity Verification

Part 1 – PIV Card Application Namespace, Data Model, and Representation

Initial Public Draft

Hildegard Ferraiolo
Ketan Mehta
Salvatore Francomacaro
Ramaswamy Chandramouli
Computer Security Division
Information Technology Laboratory

Sarbari Gupta
Electrosoft Services, Inc.

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-73pt1-5.ipd

September 2023

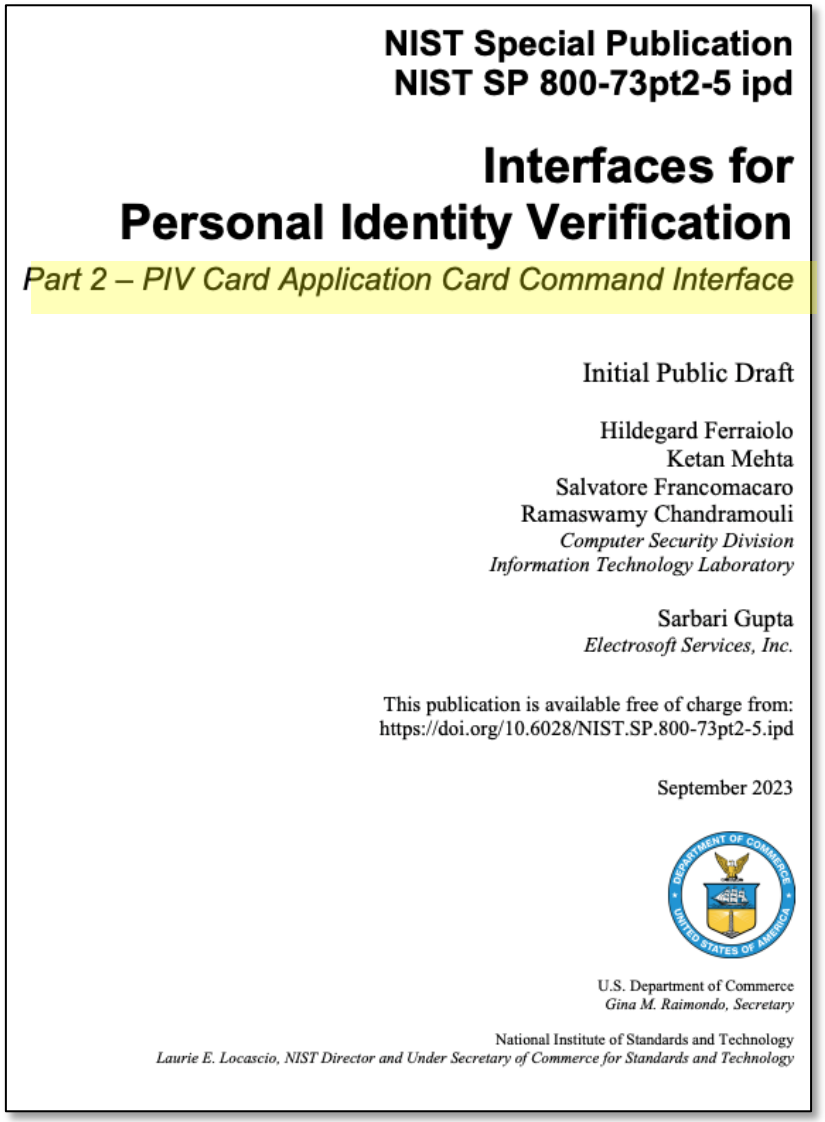
U.S. Department of Commerce
Gina M. Raimondo, Secretary

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

Part 2 of SP 800-73 Revision 5

PIV Card Interface:

- Defines low-level commands/responses
  - *Goal: for a reader to interact with PIV Card*
  - Sequence of commands for authentication, signing and encryption services
  - To achieve up to 3 factors for authentication



NIST Special Publication
NIST SP 800-73pt2-5 ipd

Interfaces for Personal Identity Verification

Part 2 – PIV Card Application Card Command Interface

Initial Public Draft

Hildegard Ferraiolo
Ketan Mehta
Salvatore Francomacaro
Ramaswamy Chandramouli
Computer Security Division
Information Technology Laboratory

Sarbari Gupta
Electrosoft Services, Inc.

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-73pt2-5.ipd

September 2023

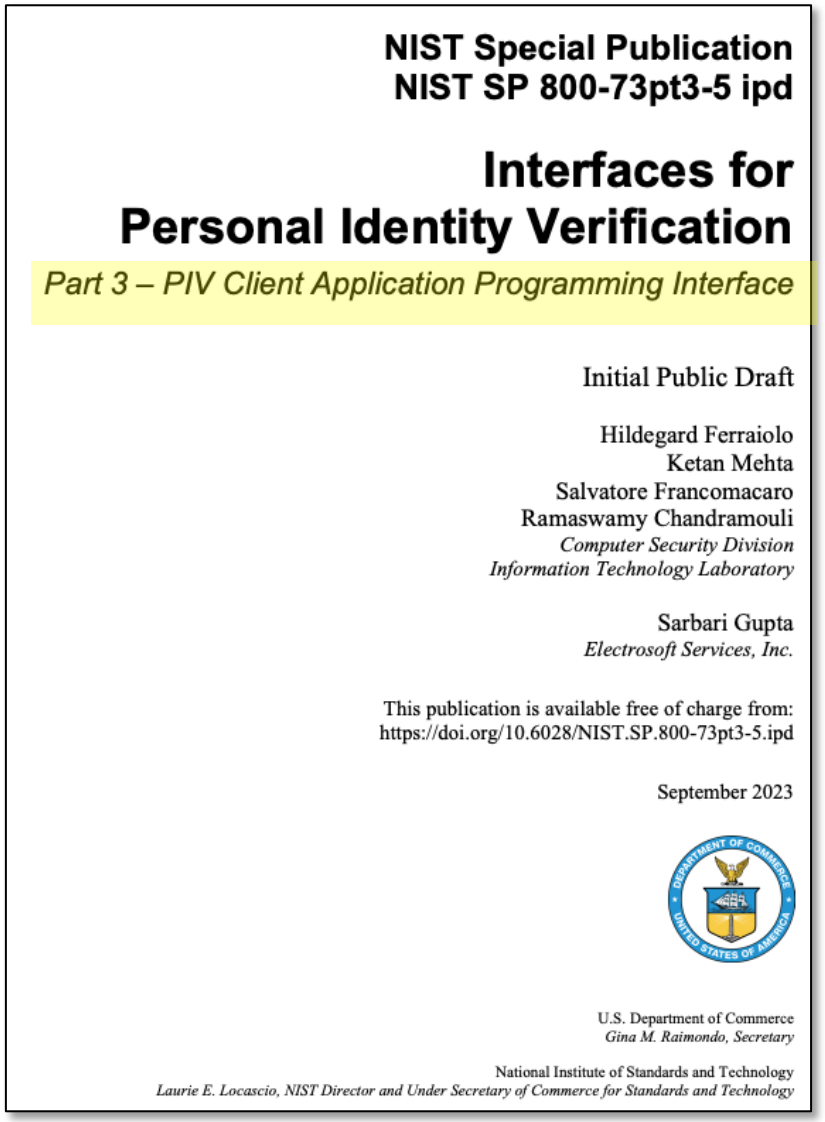
U.S. Department of Commerce
Gina M. Raimondo, Secretary

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

Part 3 of SP 800-73 Revision 5

PIV Middleware Interface:

- Defines application-level API calls
  - *Goal: for OS native applications to interact with PIV card*
  - Sequence of function calls to achieve authentication, signing and encryption services from card
  - To achieve up to 3 factors for authentication



NIST Special Publication
NIST SP 800-73pt3-5 ipd

Interfaces for Personal Identity Verification

Part 3 – PIV Client Application Programming Interface

Initial Public Draft

Hildegard Ferraiolo
Ketan Mehta
Salvatore Francomacaro
Ramaswamy Chandramouli
Computer Security Division
Information Technology Laboratory

Sarbari Gupta
Electrosoft Services, Inc.

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-73pt3-5.ipd

September 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

PIV Data Model Elements (No Change)

7 Mandatory Data Objects:

1. Card Capability Container
2. Card Holder Unique Identifier
3. X.509 Certificate for PIV Authentication
4. X.509 Certificate for Card Authentication
5. Cardholder Fingerprints
6. Cardholder Facial Image
7. Security Object

2 Conditional Data Objects (mandatory if cardholder has a government-issued email account):

1. X.509 Certificate for Digital Signature
2. X.509 Certificate for Key Management

27 Optional Data Objects:

- Printed Information
- Discovery Object
- Key History Object
- 20 retired X.509 Certificates for Key Management
- Cardholder Iris Images
- Biometric Information Templates Group Template
- Secure Messaging Certificate Signer
- Pairing Code Reference Data Container

Updates to Authentication Mechanisms (driven by FIPS 201-3)

Removed Features

- CHUID Authentication Mechanism
  - (CHUID Data Object itself remains on card to support other functions)

New Optional Feature Added

- Secure Messaging as an authentication mechanism** (SM-AUTH)

  **To support single-factor wireless authentication mechanisms for PACS

Deprecated Features

- VIS Authentication Mechanism
- Symmetric Card Authentication Key and associated SYM-CAK authentication mechanism

Updated Feature

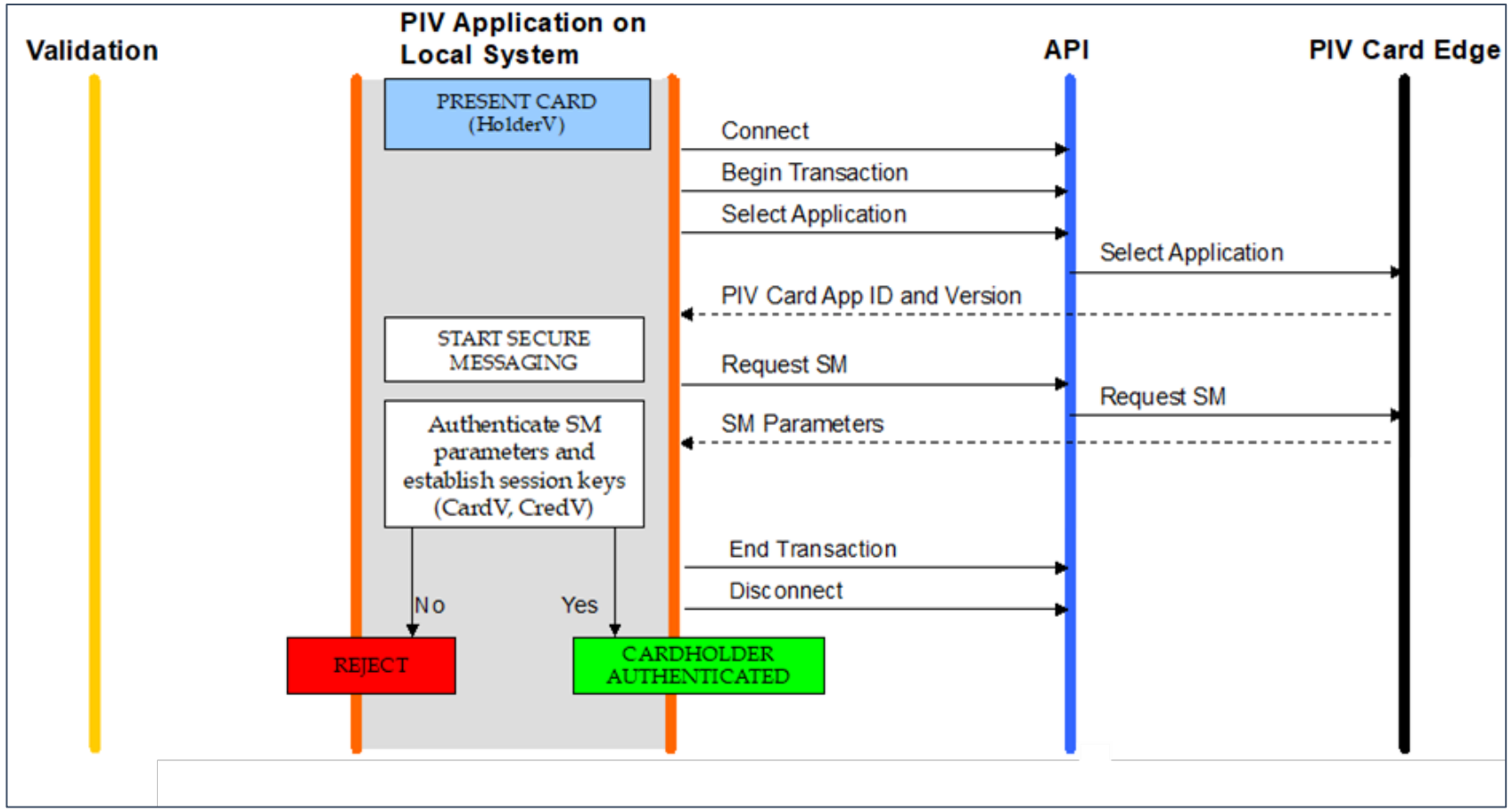
- Electronic Facial Image can be used in BIO and BIO-A as a general authentication mechanism

Updated List of PIV Authentication Mechanisms

Name	Description	Status
PKI-AUTH	Authentication Using PIV Authentication Key	AVAILABLE
PKI-CAK	Authentication Using Asymmetric Card Authentication Key	AVAILABLE
BIO	Unattended Authentication Using PIV Biometrics (Off-Card Comparison)	AVAILABLE
BIO-A	Attended Authentication Using Biometrics (Off-Card Comparison)	AVAILABLE
SYM-CAK	Authentication Using Symmetric Card Authentication Key	**DEPRECATED**
OCC-AUTH	Authentication Using On-Card Biometric One-to-One Comparison	AVAILABLE
VIS	Authentication Using PIV Visual Credentials	**DEPRECATED**
SM-AUTH	Authentication Using Secure Messaging Key	**NEW**, AVAILABLE
CHUID	Authentication Using PIV CHUID	**REMOVED**

Authentication Using Secure Messaging Key

- PIV cardholder can be authenticated via SM-AUTH if PIV Card supports the secure messaging protocol



Updates that impact NPIVP

- The NIST Personal Identity Verification Program (NPIVP) was established to:
  - Validate Conformance of PIV Middleware and PIV Card Applications with SP 800-73
  - Provide assurance of interoperability of PIV Middleware and PIV Card Applications
- With release of SP 800-73-5:
  - Conformance with SP 800-73-5 Part 3 is OPTIONAL for PIV Middleware
  - NPIVP PIV Middleware conformance testing will be discontinued
    - Since smart card support is natively supported in most Operating Systems

Updates to PIV Card Activation Methods

- PIN
  - Restricted number of consecutive retries for PIN activation to 10 or less
    - To mitigate risk of retry attacks based on a 6-to-8-digit PIN
- On-Card Comparison (OCC)
  - Fingerprints used for OCC SHOULD be imaged from fingers not imaged for off-card one-to-one comparison (BIO, BIO-A)
  - Restricted number of consecutive retries for OCC activation to 10 or less
    - To trigger enrollment of new OCC biometrics
  - Updated CHANGE REFERENCE DATA command to allow reset of OCC reference data for Card activation

Other Updates

- Updated allowed cryptographic algorithms to match updates in SP 800-78-5 Draft
- Deprecated use of separate content signing keys for Biometric Data and CHUID
- Removed:
  - Extended Application CardURL and Security Object Buffer elements from Card Capability Container Object
  - Buffer Length, DUNS, and Organizational Identifier elements from CHUID Data Object
  - MSCUID element from all X.509v3 Certificate data objects except retired key management certificates
- Clarified that Card UUID, Expiration Date and Cardholder UUID data CHUID fields cannot be modified post issuance

NIST SP 800-78 Revision 5:
PIV Algorithms and Key Sizes

Andrew Regenscheid
Hildegard Ferraiolo

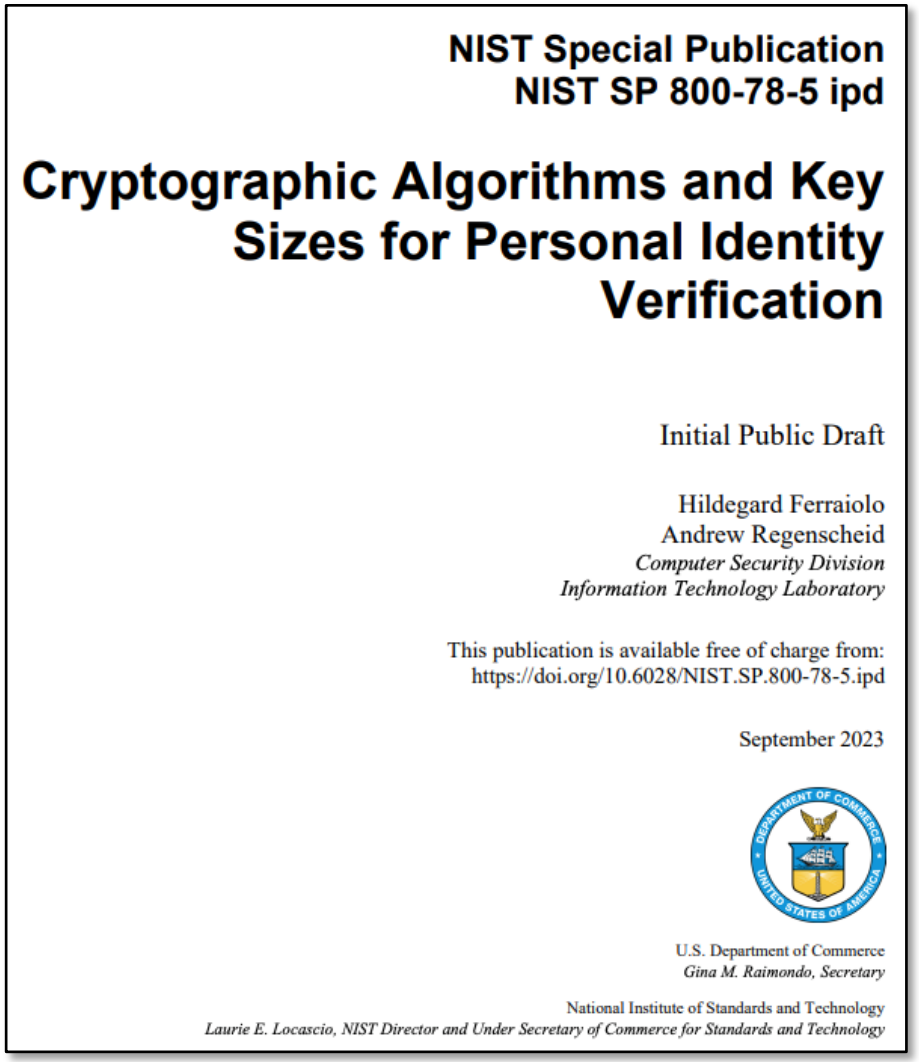
PIV Algorithm and Key Sizes

Purpose:

To define the technical specifications needed for the mandatory and optional cryptographic keys specified in FIPS 201 as well as the supporting infrastructure

Scope:

PIV Card, infrastructure components that support issuance and management of the PIV Card, and applications that rely on the credentials supported by the PIV Card to provide security services



NIST Special Publication
NIST SP 800-78-5 ipd

Cryptographic Algorithms and Key Sizes for Personal Identity Verification

Initial Public Draft

Hildegard Ferraiolo
Andrew Regenscheid
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-78-5.ipd

September 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 PIV Card's Cryptographic Keys

PIV Keys:

- The asymmetric PIV Authentication key,
- An asymmetric Card Authentication key,
- A symmetric Card Authentication key (deprecated),
- An asymmetric digital signature key for signing documents and messages,
- An asymmetric key management key that supports key establishment or key transport and
- up to 20 retired key management keys,
- A symmetric PIV Card Application Administration Key, and
- An asymmetric PIV Secure Messaging key that supports the establishment of session
- keys for use with secure messaging and supporting cardholder authentication using the
- SM-AUTH authentication mechanism.

- **These algorithms and key sizes need to be supported by relying systems too!**

PIV Content Signer Specifications

Signature specification on Authentication Information (i.e., the Content signer):

- X.509 public key certificates,
- The optional secure messaging card verifiable certificate (CVC),
- The optional intermediate CVC,
- The CHUID data object,
- Biometric information (e.g., fingerprints), and
- The NIST SP 800-73-5 Security Object.

Drivers for SP 800-78 Revision 5 Update

Alignment with FIPS 201 Revision 3:

- Accommodation of the Secure Messaging Authentication key
- Deprecation of the symmetric card authentication key

Aligning with Cryptographic Transitioning Guidelines (per SP 800-131A Revision 2)

- Deprecation of 3TDEA algorithm with identifiers
- Removal of the retired RNG from CAVP PIV component testing where applicable

Adding 128 bit Cryptographic Strength

PIV Key Type	Recommended Algorithms and Key Sizes Through 2030	Recommended Algorithm and Key Sizes for 2031 and Beyond
PIV Authentication key	RSA (2048 or 3072 bits) ECDSA (Curve P-256 or P-384)	RSA 3072 bits ECDSA (Curve P-256 or P-384)
Asymmetric Card Authentication key	RSA (2048 or 3072 bits) ECDSA (Curve P-256 or P-384)	RSA 3072 bits ECDSA (Curve P-256 or P-384)
Symmetric Card Authentication key	3TDEA (deprecated), AES-128, AES-192, or AES-256	AES-128, AES-192, or AES-256
Digital signature key	RSA (2048 or 3072 bits) ECDSA (Curve P-256 or P-384)	RSA 3072 bits ECDSA (Curve P-256 or P-384)
Key management key	RSA key transport (2048 or 3072 bits) ECDH (Curve P-256 or P-384)	RSA key transport 3072 ECDH (Curve P-256 or P-384)
PIV Secure Messaging key	ECDH (Curve P-256 or P-384)	ECDH (Curve P-256 or P-384)

Cryptography Transitions

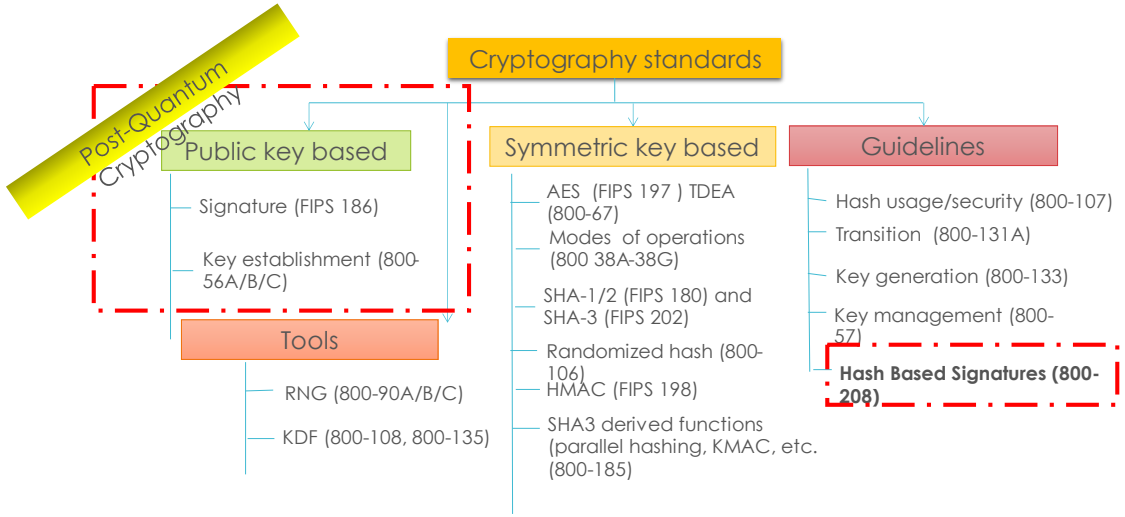
- **Cryptography employed after 2031 *SHOULD* provide 128 bits of security strength, e.g.,**
  - *Encryption*: AES (128, 192, & 256 key sizes)
  - *Signatures*: RSA-3072, ECDSA with P-256 or P-384
- ***However*, this decision should be made in the context of longer-term cryptographic transition and modernization plans.**
  - Namely, the need to plan and invest for a future migration to post-quantum algorithms.
  - Capital investments for PIV systems should be selected with an emphasis on ensuring a timely migration to post-quantum algorithms once standards, technologies, and services are available.
  - If the migration to 128-bit cryptography would require infrastructure upgrades, agencies may defer these improvements until the post-quantum migration.
- **Post-quantum algorithms will be specified in a future revision of this document once foundational standards supporting their use have been adopted.**

PQC Standards

- **Quantum computers threaten the security of current, widely-deployed public key cryptosystems:**
  - *Signatures*– ECDSA, RSA
  - *Key Establishment*–Diffie-Hellman, RSA
- Will need to be replaced with new algorithms and standards to prepare for quantum era
- After a six-year public solicitation and evaluation process, NIST selected four algorithms:

  Signatures
  - CRYSTALS-Dilithium → ML-DSA (Draft FIPS 203)
  - SPHINCS+ → SL-DSA (Draft FIPS 204)
  - FALCON → *Standard to be development*

  Key Establishment
  - CRYSTALS-KYBER → MWLE-KEM (Draft FIPS 205)



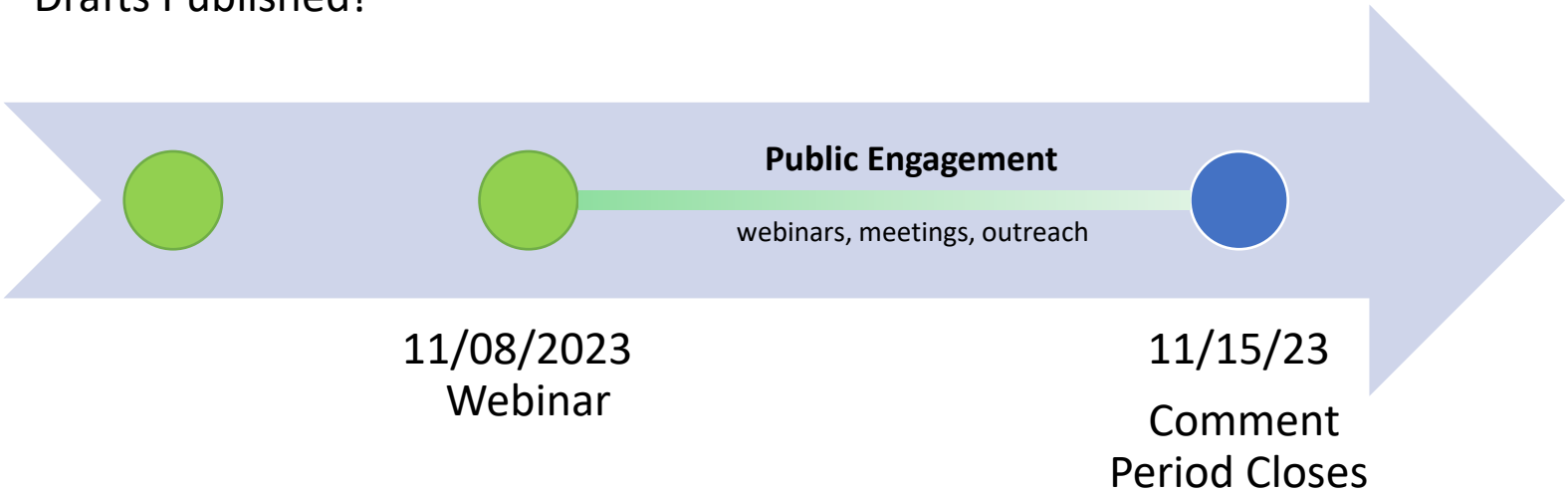
PQC– Much Work Remains

- Operations
- Infrastructure Modernization
- PQC Adoption in Software/Systems
- Hardware Acceleration/Support
- Implementation in Cryptographic Libraries
- Protocol/Application Standards
- $\mathbb{Z}_q[X]$ Algorithm Standards

Key Dates and Next Steps

Hildegard Ferraiolo, NIST PIV Program Lead

Key Dates



What happens during the public comment period?

- Engagement & Outreach
- Continued Research
- Triage of Comments

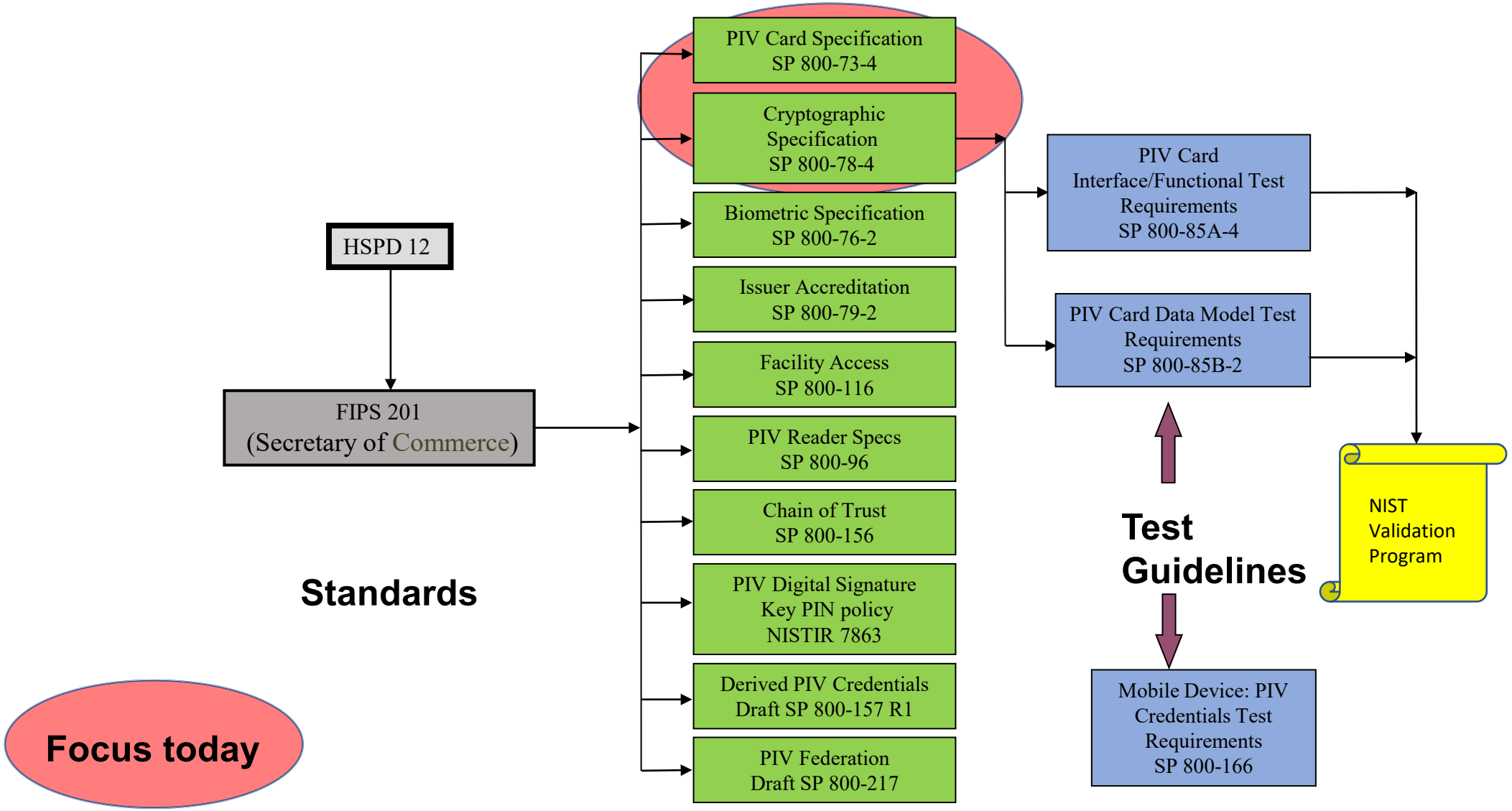
What happens after the comment period?

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

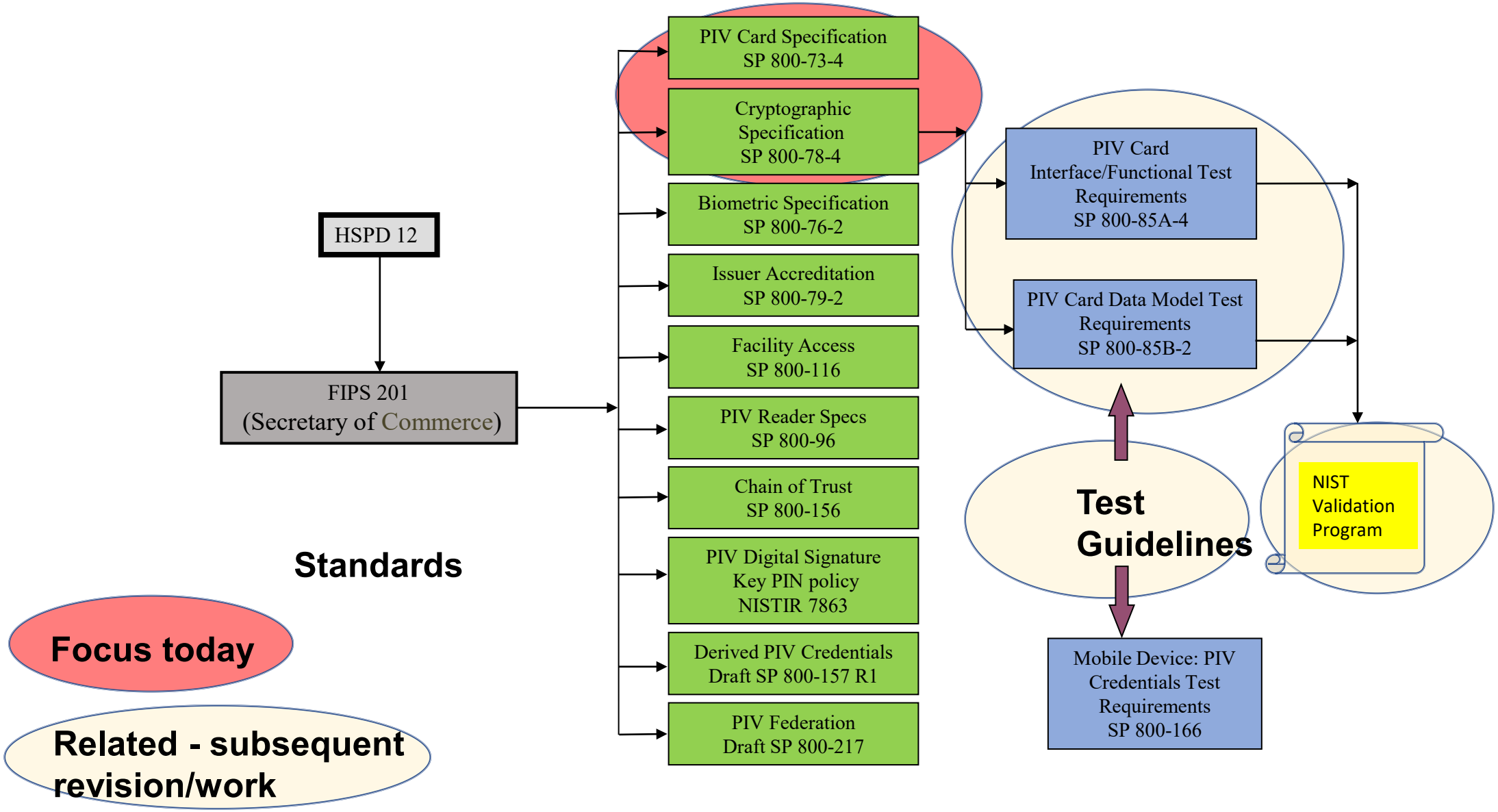
Comment Submission

- When are comments due?
  - December 8, 2023
- Where can I find the documents?
  - Draft SP 800-73-5 Part 1 PIV Card Data Model
  - Draft SP 800-73-5 Part 2 - PIV Card Edge Interface
  - Draft SP 800-73-5 Part 3 - PIV API
  - Draft SP 800-78-5 Cryptographic Algorithms and Key Sizes
- 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 800-73-5 Comment template (xls)
    - Draft SP 800-78-5 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

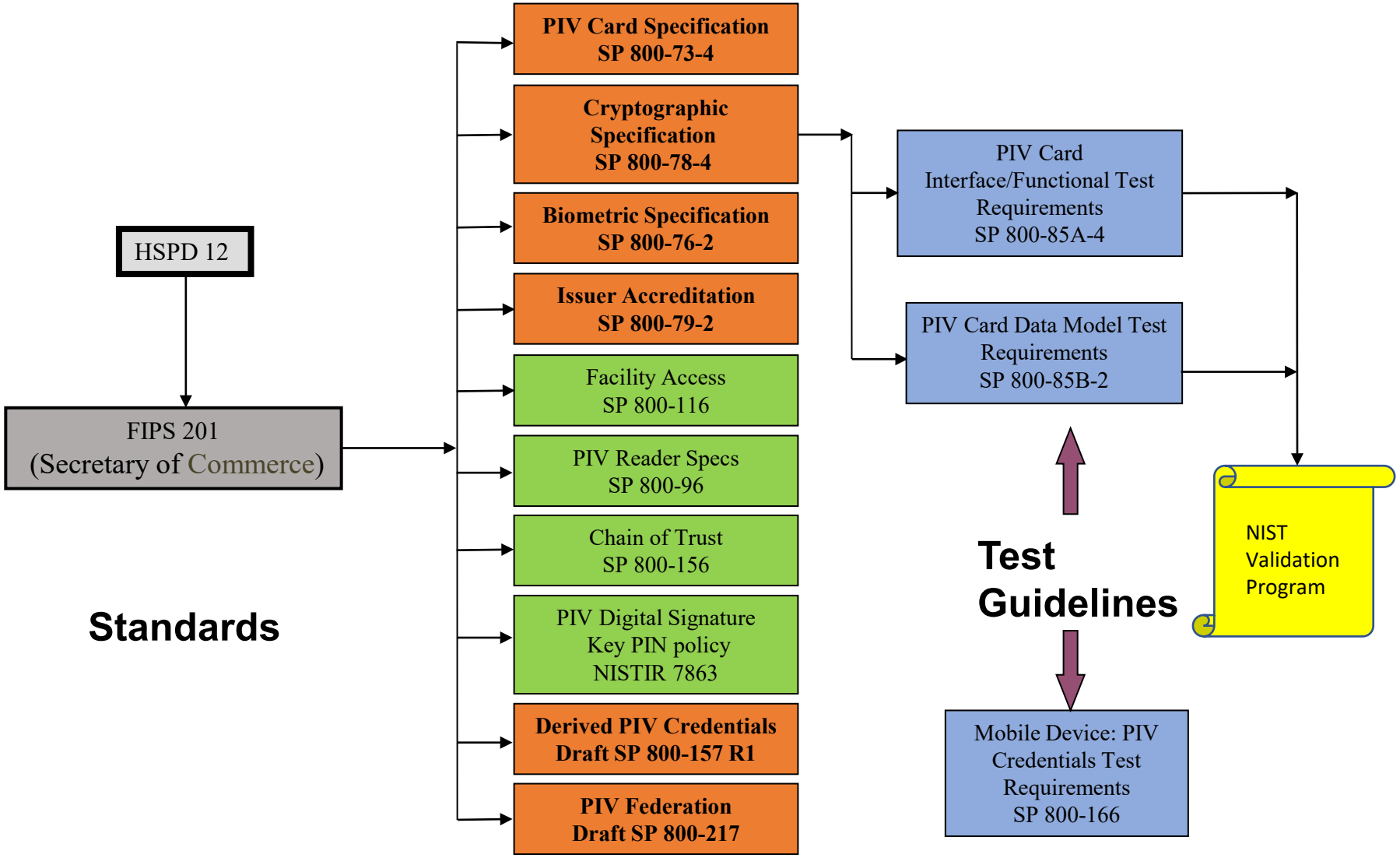
FIPS 201 and Supporting Special Publications



FIPS 201 and Supporting Special Publications



Currently Updating:



Revision in Progress

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

Thank you for your participation today!