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

Digital Identity Guidelines Rev 4 – Overview of the Final Version

Digital Identity Program

Information Technology Lab

August 2025

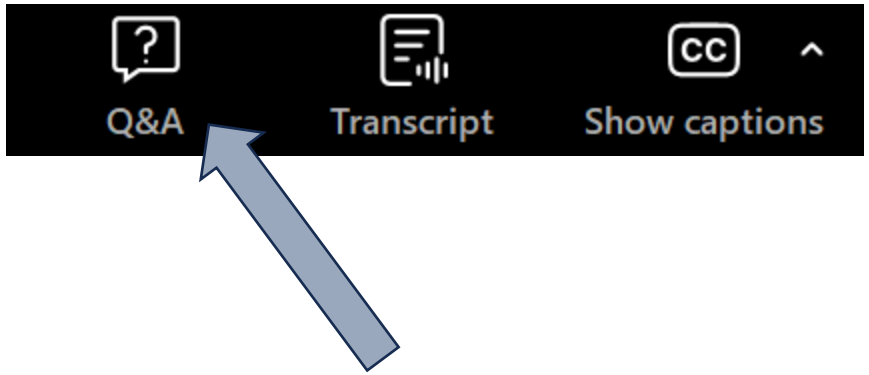
Today's Agenda

Item	Speaker
Welcome & Background	David Temoshok & Ryan Galluzzo
Base Volume	Connie LaSalle
63A: Proofing & Enrollment	Ryan Galluzzo
63B: Authenticators & Authentication	Andy Regenscheid
63C: Federation & Assertions	Ryan Galluzzo
Q&A	Team
Next Steps & Closing	Ryan Galluzzo

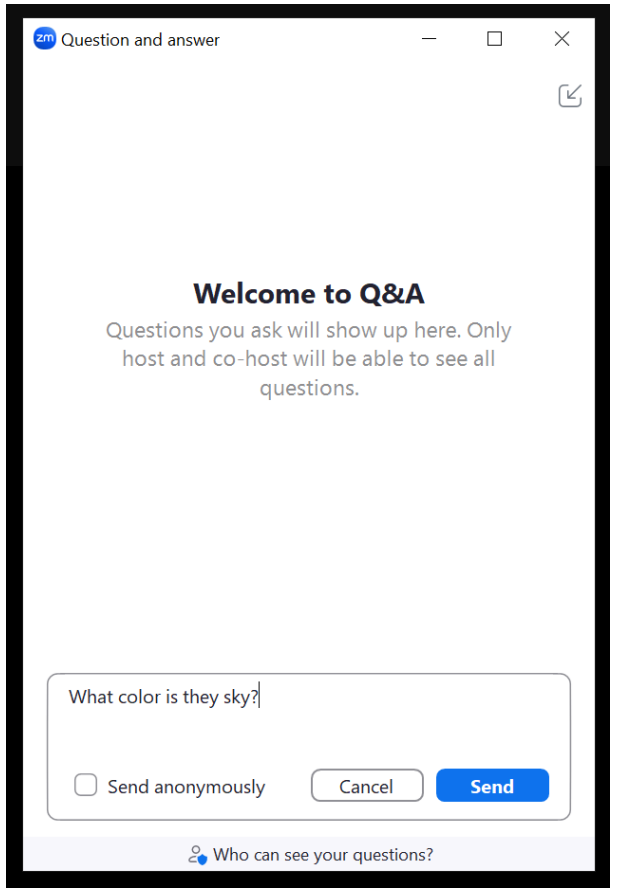
SUBMITTING QUESTIONS

Please use the Q&A function to enter your questions.

We will do our best to answer all questions during the Q&A portion of this event.



1. To open the Q&A function, click on the “Q&A” icon at the bottom of your screen

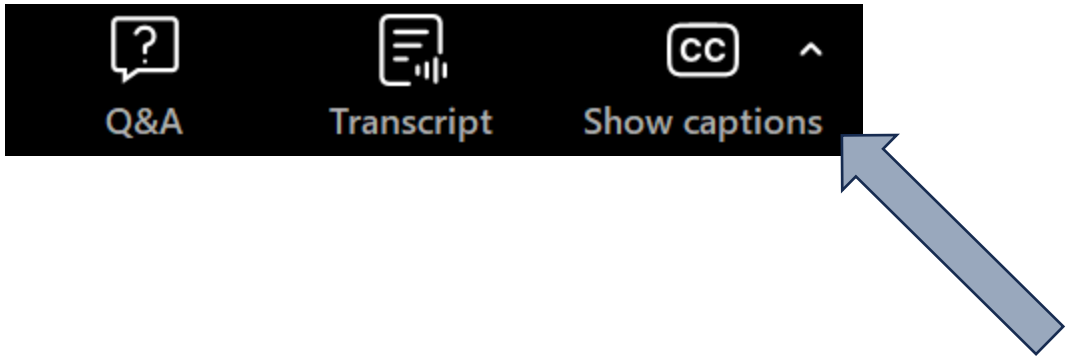


2. Type your question in the text box and click Send

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

CAPTIONS

To enable captioning during the event, click on the “Show captions” icon at the bottom of your screen.



Why are we here today?

Purpose:

- To promote the final version NIST SP 800-63 Revision 4
- To provide you with insight into changes in the Final Version
- To provide an opportunity for questions

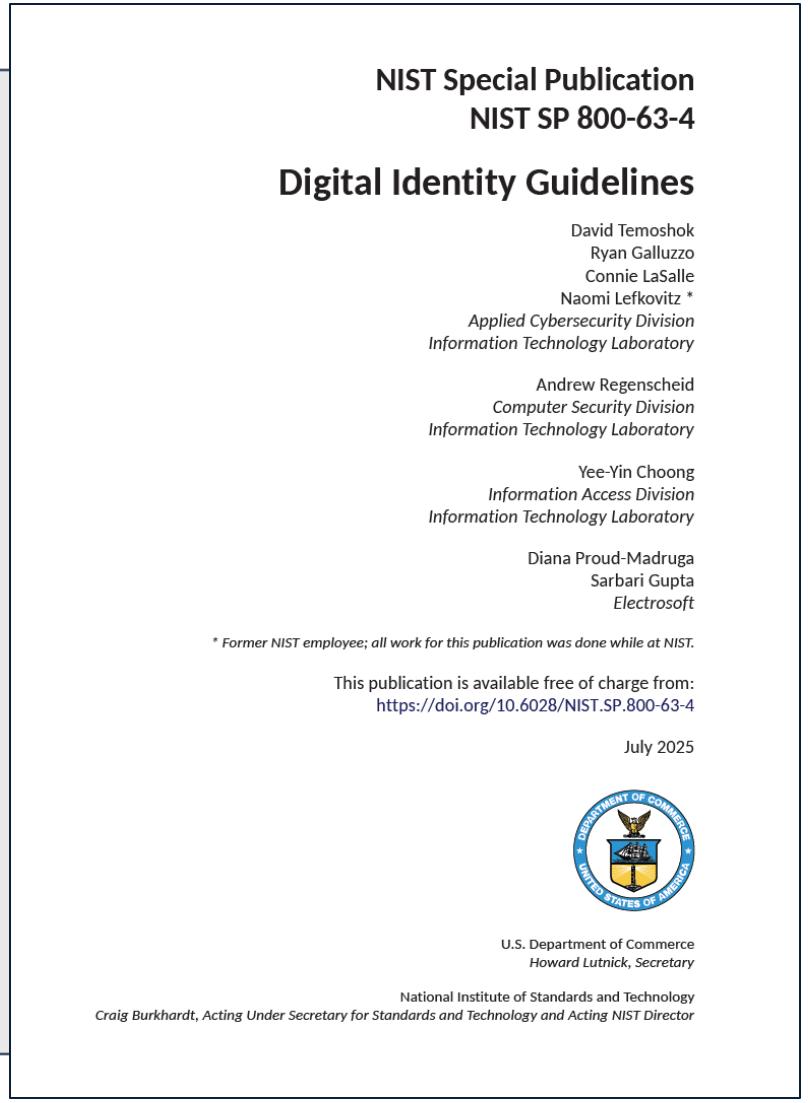
Outcomes:

- You will understand the key changes to revision 4 as well as the drivers that resulted in the final changes
- You will have insights on next steps, implementation resources, and how to provide input on these next steps

Digital Identity Guidelines (SP 800-63)

What are the Digital Identity Guidelines?

- Provide the **foundational requirements** for federal agencies to conduct digital identity management
- Provide assurance levels for **the three functions of digital identity**: identity assurance, authentication assurance, federation assurance
- Provide considerations for **enhancing privacy, usability, and customer experience** of digital identity services and technology.



NIST Special Publication
NIST SP 800-63-4

Digital Identity Guidelines

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

** Former NIST employee; all work for this publication was done while at NIST.*

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

July 2025

U.S. Department of Commerce
Howard Lutnick, Secretary

National Institute of Standards and Technology
Craig Burkhardt, Acting Under Secretary for Standards and Technology and Acting NIST Director

Motivators for Change

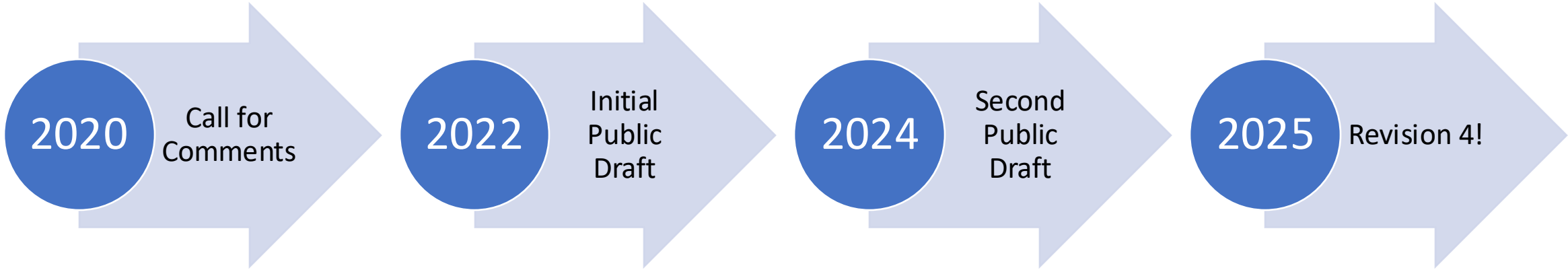
Address Emerging Threats & Technology

Improve Customer Experience

Establish Cross-Functional Approach

Address Real-world Lessons Learned

The Journey



June 2020: Initial feedback about needed updates to revision 3

December 2022: 180 day comment period nearly 4,000 comments received.

August 2024: 45 day comment period and approximately 2,000 comments received.

Final version was published in August of this year.

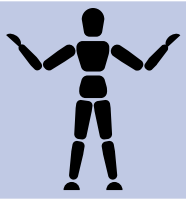
Thank you for your engagement to this point but the journey continues with conformance criteria & implementation resources!

NIST SP 800-63-4

Digital Identity Guidelines: Digital Identity Model and Risk Management

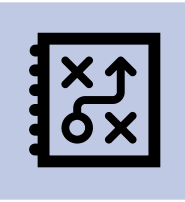
Base Volume – At a Glance

From Revision 3 to Revision 4



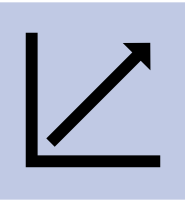
Refines Digital Identity Models

- Adds subscriber-controlled wallets to the models
- Streamlines content and moves more details to volumes



Defines an updated risk management model

- Introduces CX-focused evaluations
- Introduces “tailoring” of assurance levels
- Eliminates flow diagrams
- Promotes cross-functional risk assessment teams



Establishes Continuous Improvement Metrics

- Introduces a requirement for continuous improvement program
- Offers recommended metrics for programs

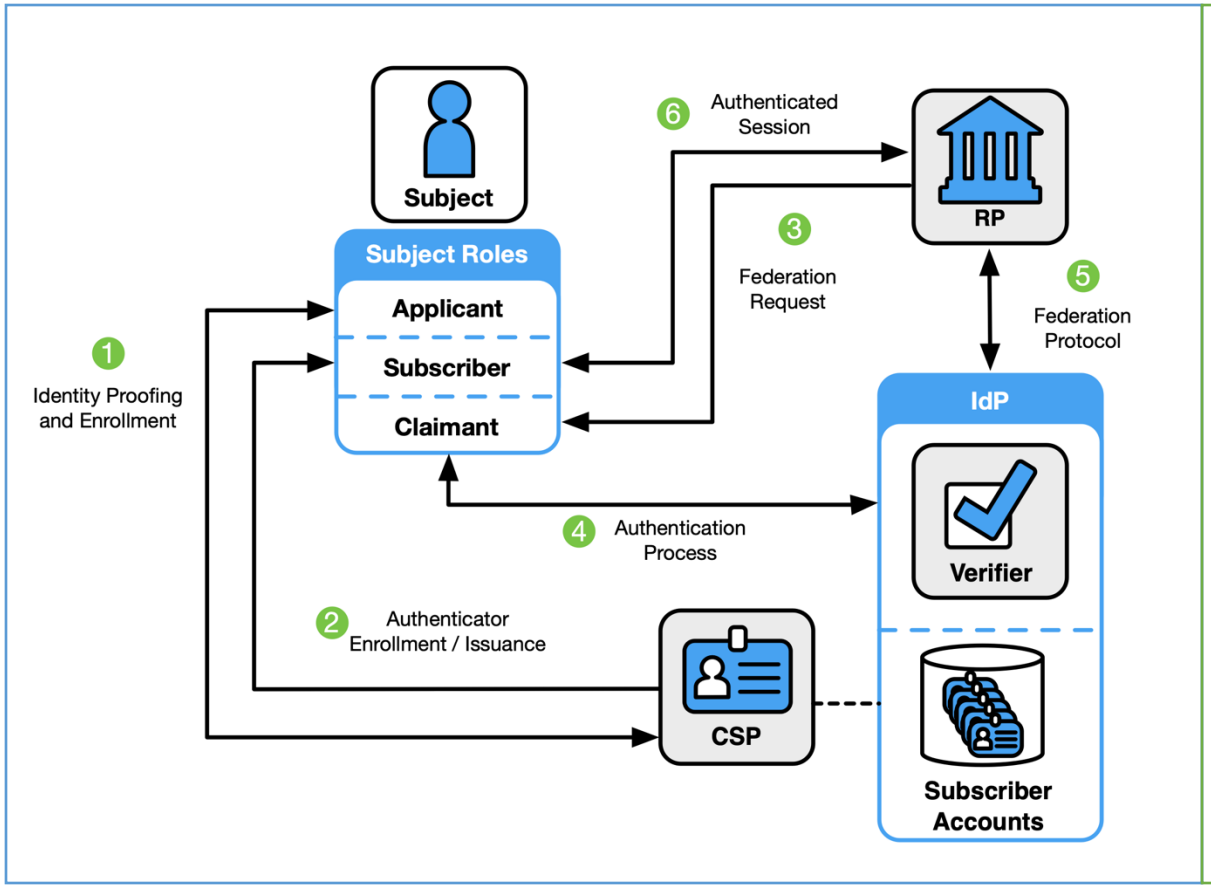
From 2PD to Final

- Refines language on Digital Identity Model
- Moves more from base volume details to specific volumes
- Refines application of the DIRM to CSPs and documentary expectations
- Incorporates more considerations for selecting FAL3 – including the risk of a compromised IdP and the availability of FAL3 options
- Provides examples of “user profiles” for each assurance level to aid in assurance level discussion
- Reflects changes to policy environment

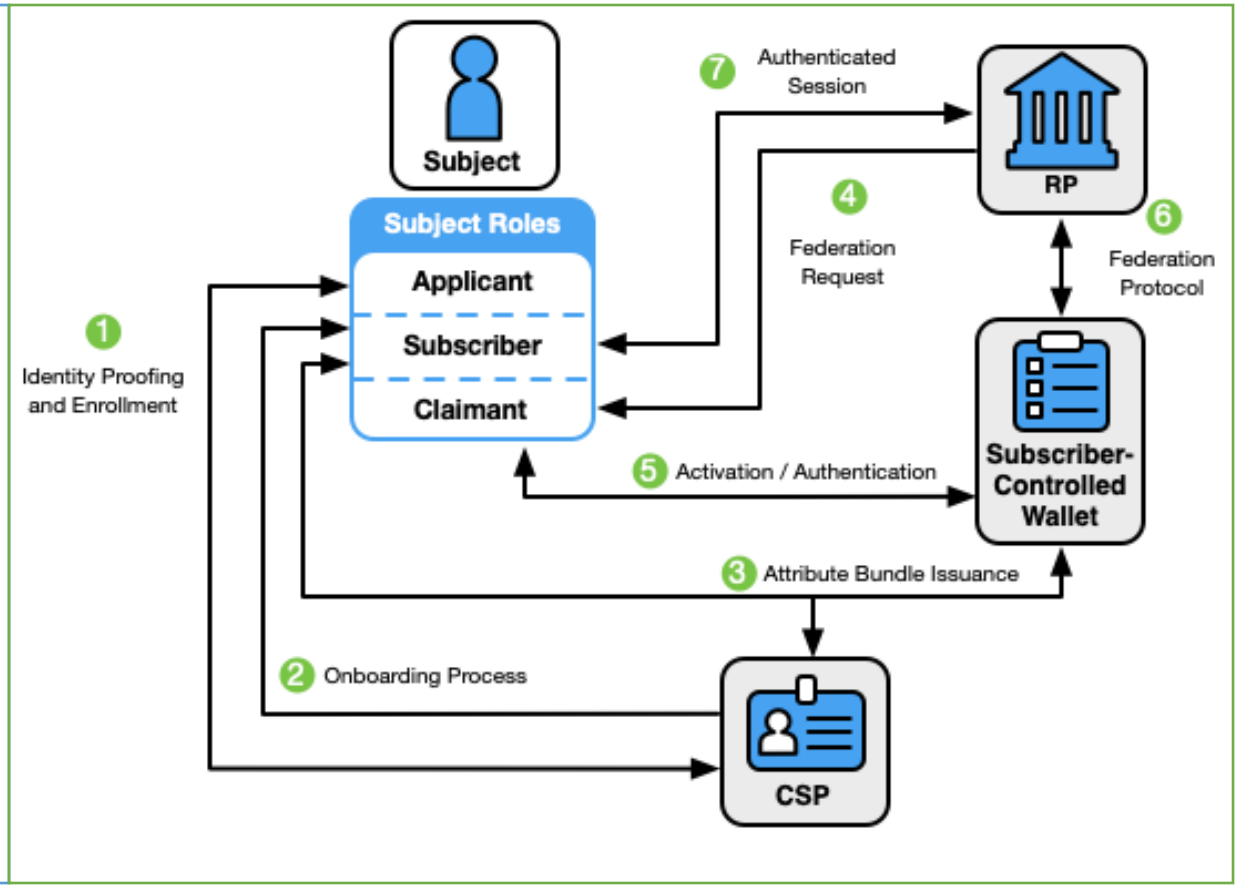
The Details: Introduction of CX

- **Driving Principle**: End-users are at the center of system design, risk assessments, and decision-making
- **Call to Action**: End-user capabilities, limitations, and perspectives must be better understood and reflected throughout the account lifecycle
- **Rev 4 Actions:** Revamped DIRM approach, addition of continuous evaluation & improvement metrics, and Redress requirements highlight the criticality of understanding customers and offering usable solutions

The Details: Subscriber-Controlled Wallet



Federated Identity Model (Added in IPD)



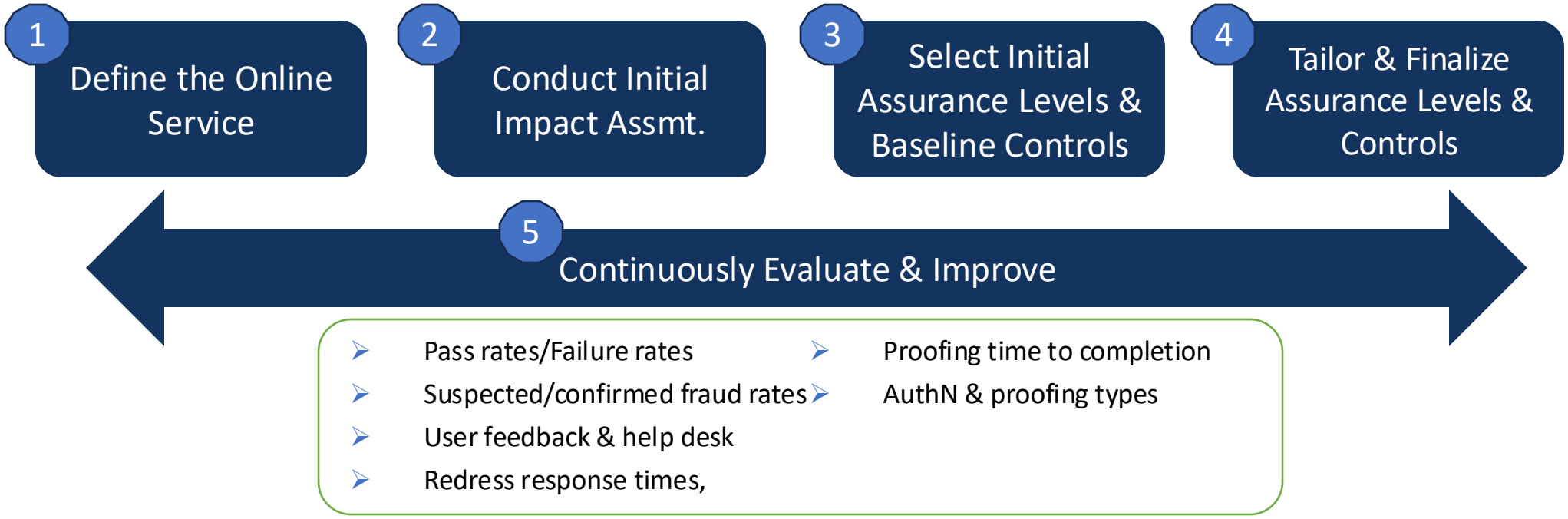
Subscriber Controlled (Added in 2PD)

The Final represents a more complete view of Digital Identity Models by incorporating both a federated identity model and subscriber-controlled wallet model

The Details: Updated Risk Management

Identification and management of risks are presented along two dimensions:

Dimension 1: Risks to the online service	Dimension 2: Risks from the identity system
Informs **Initial Assurance Levels & Controls Selections**	Informs **Tailoring & Final Assurance Levels and Controls Selections**
What are the identity-related risks associated with a compromise of the online service?	What are the risks posed by an identity system if implemented at the initial assurance levels?



NIST SP 800-63A-4

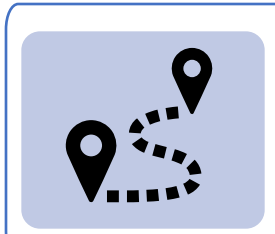
Identity Proofing and Enrollment

Volume A: At a Glance

From Revision 3 to Revision 4

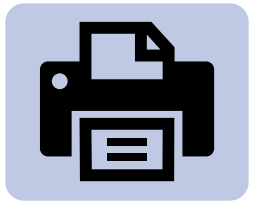
Introduces New Roles & Types of Proofing

- Provides new roles for identity proofing
- Provides new taxonomy for proofing types



Updates Assurance Levels and Pathways

- Provides IAL1 as lower assurance proofing option
- Defines three different pathways to IAL2
- Addition of subscriber account



Emphasizes Need for Exception Handling

- Updates Trusted Referees and introduces Applicant References
- Mandates CSPs provide exception handling, though provides flexibility in how this is achieved

Provides Fraud & Biometric Requirements

- Directs CSPs to establish fraud prevention programs and recommends RPs do the same
- Introduces fraud and deepfake/injection controls
- Provides biometric protections & performance metrics

From 2PD to Final

- Provides additional training requirements for Proofing Agents
- Adds “deepfake” and injection protections to the documents
- Updates evidence requirements for IAL2 (e.g., allows for one superior)
- Includes address and email risk checks as recommended fraud checks
- Updates requirements for subscriber accounts to address topics such as multi-account scenarios
- Directs CSPs to provide information to RPs on the type of proofing used

The Details: Roles

- Removes the mandate for CSPs to support trusted referees but recommends they are supported as part of exception handling.
- Provides additional requirements and updates language around training for proofing agents and trusted referees.
- Applicant references remain recommended to support exception handling.
- Allows for exception handling processes to be deployed with other risk management steps (e.g., limiting access or authorizations, time-based access, or additional analysis).

Proofing Agent

An agent of the CSP who is trained to attend on-site and remote identity proofing and make limited, risk-based decisions

Trusted Referee

An agent of the CSP or RP who is vetted and trained to support exception handling scenarios

Process Assistant

Provides basic support services to an applicant, such as translation or accessibility support

Applicant Reference

Participates in the identity proofing process on behalf of the applicant to vouch for aspects of the applicant's identity

The Details: Multiple Pathways to IAL2

Non-Biometric	Digital Evidence	Biometric
➢ Does not use **automated** comparison of biometric samples obtained from the applicant	➢ Uses digital identity evidence (e.g., mDLs) or authentication to digital accounts	➢ Uses **automated** comparison of biometric samples obtained from the applicant
➢ Verification is accomplished by using confirmation codes and/or **visual comparison** of a portrait on evidence to the applicant presenting it	➢ Verification is accomplished by using authentication to a device or account and at lower levels through confirmation codes	➢ Verification is accomplished by automated comparison of live facial image or other biometric sample obtained from an applicant to the biometric in the associated identity evidence

➢ **Directs CSPs to provide an indication to RPs of the verification pathway used at IAL2 – either in assertions, via an API, or through trust agreements**

The Details: Injection Attacks

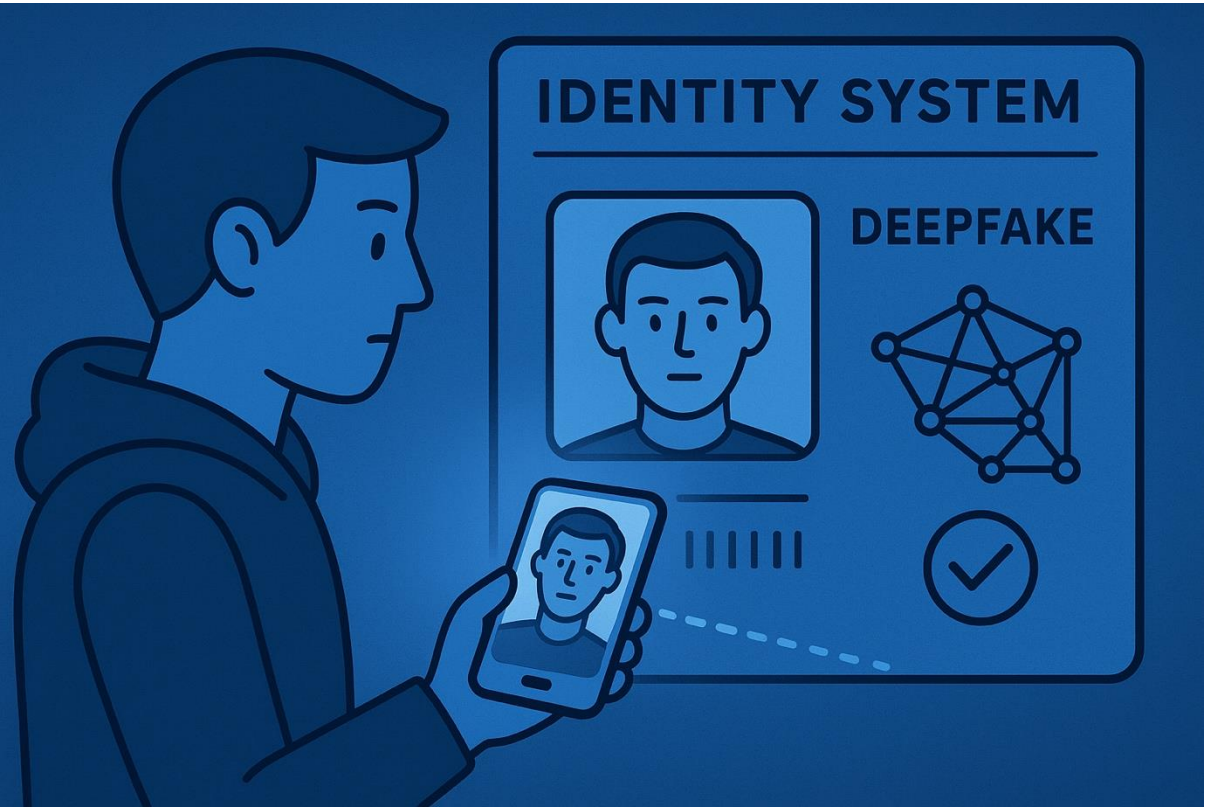
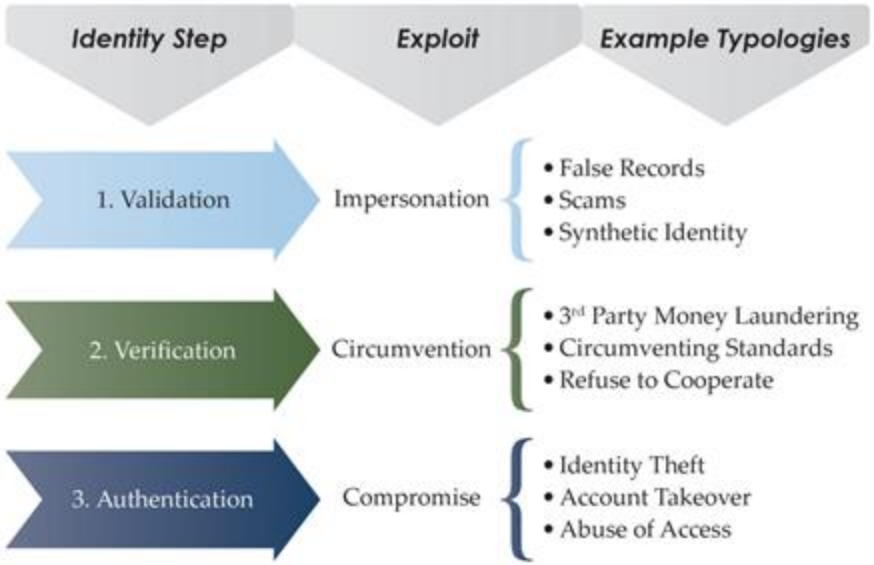


*Image created with ChatGPT. ☺

- Emphasizes the need to address both injection attacks AND detection of forged media.
- Provides requirements for defending against injection of forged digital media.
- Mandates that services analyze media for indications of forgery or modification.
- Mandates analysis of signals to detect threats such as virtual cameras and camera emulators.
- Mandates analysis of communication streams to identify indications of injection.
- Mandates PAD for biometric verification.
- Mandates use in both remote attended (e.g., video chat) and remote unattended sessions.

In the Weeds: Fraud Management



Identity-Related Exploitations and Typologies Attackers use to Undermine Identity Processes

Identity Exploitation	Number of BSA Reports	Total Suspicious Amounts
Impersonation	1.7 million	$200 billion
Compromise	~446,000	$112 billion
Circumvention	~323,000	$39 billion
Total	**2.4 million**	**$351 billion**

Exploitations Reported in Identity-Related BSA Reports

- Requires the creation of fraud management programs at CSPs and recommends this for RPs

- Requires:
  - Date of Death Checks
  - Evaluation and blocking of suspicious communications channels
  - Automated attack detection tools
  - **Privacy assessment of all fraud tools**

- Recommends:
  - SIM Swap Detection
  - Transaction Analytics
  - Device or Account Tenure checks
  - Mailing Address checks
  - Fraud Indicator checks
  - Device finger printing

NIST SP 800-63B-4

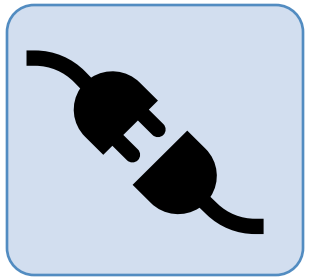
Authentication and Authenticator Management

Volume B: At a Glance

From Revision 3 to Revision 4

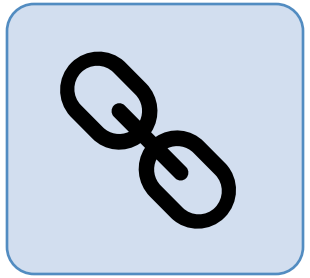
Updates Recovery Section

- Substantially re-written for options and clarity
- Provides multiple paths to recovery
- Aligns recovery requirements to AAL and IAL



Adds Phishing Resistance & New Authenticators

- Defines phishing resistant authenticators
- Allows for synced authenticators at AAL2
- Adds wallets as authenticators



Updates Session Management

- Relaxes session management time frames
- Supports implementation flexibility
- Sets considerations for new technology

From 2PD to Final

- Updates language to clarify the use of “hybrid” flows and connections and aligns language to standards that have been updated since 2PD publication
- Introduces the use of session monitoring and DBSC to support extended session timeframes
- Further refines and clarifies the language around account recovery
- Provides minor updates to synced authenticator text (e.g., allowing for additional risk signals or factors in the absence of attestation)
- Updates password length requirements and divides the length requirements based on MFA usage

The Details: Account Recovery

Account Recovery Methods

Saved Recovery Codes

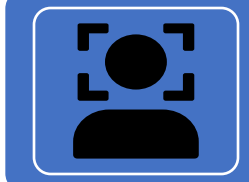
- e.g., printed/written alphanumeric codes

Issued Recovery Codes

- e.g., code sent to previously registered address

Recovery Contacts

- Recovery codes sent to previously registered addresses of trusted associates



Repeated Identity Proofing

- Repeat a portion of the identity proofing process
- MAY verify the user with a biometric from initial proofing

Recovery Processes by AAL

AAL1

- Any one available recovery method
- Repeated proofing not possible because AAL2 is required to access personal information

AAL2

- Two recovery codes sent using different methods,
- One recovery code + SF authentication, or
- Repeated identity proofing

AAL3

- If **IAL1/IAL2** account, same as **AAL2**
- If **IAL3** account, perform biometric comparison in an onsite attended session

Account recovery **requires notification** to the subscriber to mitigate additional authentication risks

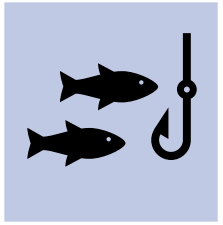
Details: Syncable Authenticators

Syncable Authenticators:

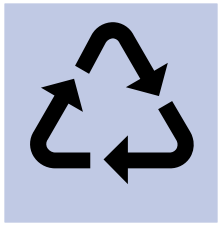
- Cryptographic authenticators where authentication keys can be cloned and exported to other storage
- Authentication keys usually resident on a user endpoint
- Supports the syncing of those keys to other endpoints (i.e., devices).

The guidance:

- Provides requirements and considerations for use
- Confirms allowability at AAL2 (with user verification)
- Reflects the content from SP 800-63B Supplement 1



Phishing Resistant



Replay Resistant

Multi-factor (w/UV)

Since AAL3 prohibits export of keys, the **maximum achievable** AAL for syncable authenticators is **AAL2**

The Details: Session Lifetimes/Timeouts

Two types of timeouts:

- Inactivity (time since last observed activity)
- Overall (time since last [re-]authentication)

Choice of timeout limits:

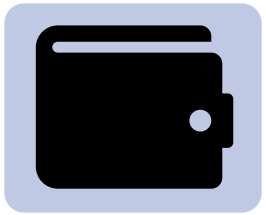
- Establishment of timeout limits is required
- Overall limit of <12 hours at AAL3 is required
- Most timeout limits are recommendations because of dependence on application and endpoint environment
- Updated to account for techniques to enable extended sessions including DBSC and session analysis

NIST SP 800-63C-4

Federation and Assertions

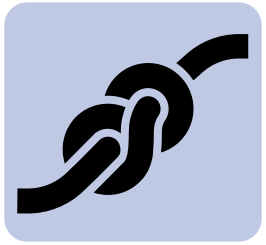
Volume C: At a Glance

From Revision 3 to Revision 4



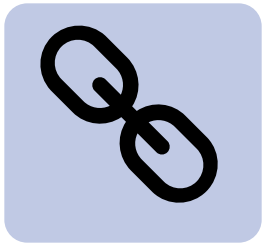
Updates Structure, adds subscriber-controlled wallet

- New structure to account for two forms of federation: general & subscriber-controlled wallets
- Provides requirements for user attribute bundles(credentials) stored in digital wallets



Updates FALs

- Defines Holder of Key (HOK) assertions and RP bound authenticators for use at FAL3
- Separates out encryption requirements at FAL2 based on presence of PII
- Defines trust agreement requirements for all FALs



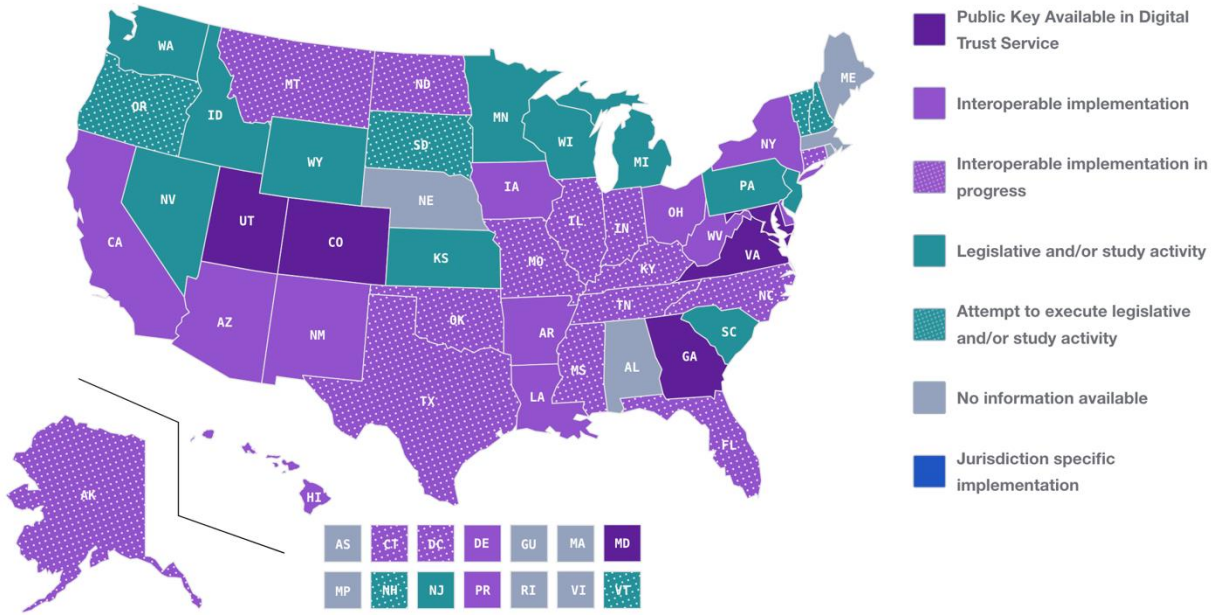
Adds protocol-based examples

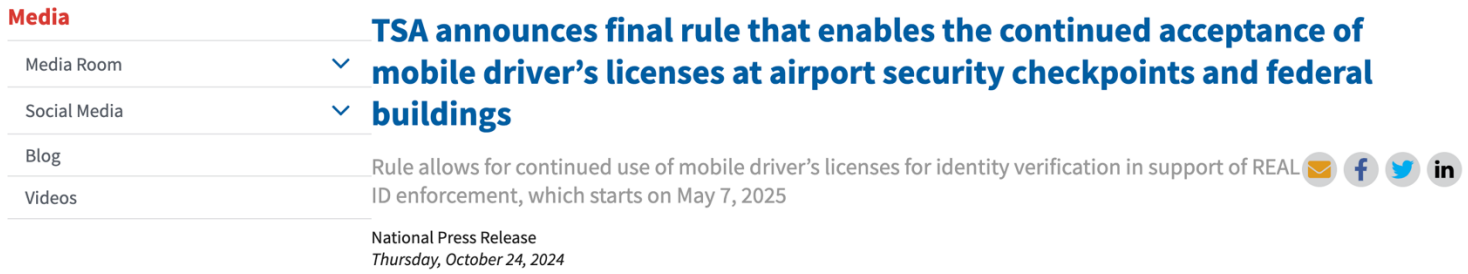
- Provides examples of how protocols could meet requirements
- Covers three examples: OIDC, SAML, Wallets (OID4VP and VCI)

From 2PD to Final

- Clarifies language around key usage, management, and verification
- Allows for hosted wallets in addition to device-based wallets
- Updates trust agreement requirements to better align with ecosystem
- Updates wallet assertion content to better align with where presentation standards have evolved
- Clarifies RP bound authenticators and traditional methods of independent verification of IdP credentials (e.g., HoK)
- Adds examples of wallet protocols to section 9

In the Weeds: Subscriber Controlled Wallets





- Enables use of subscriber-controlled wallets and attribute bundles (i.e., verifiable digital credentials)
- Provides requirements for presenting attribute bundles online
- Provides requirements for the attribute bundles and functions of wallets
- Allows for both subscriber-controlled wallets and cloud-hosted wallets
- Mandates cryptographic holder binding of attribute bundles when presented from wallets
- Brings text into better alignment with emerging standards

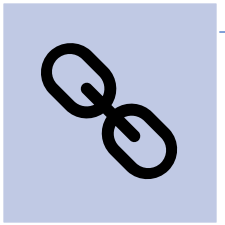
FAL3 and Bound Authenticators

More clearly describes two primary techniques for achieving FAL3:

Holder of Key

A holder-of-key assertion includes a unique identifier for an authenticator that can be verified independently by the RP, such as the public key of a certificate controlled by the subscriber.

- **Examples:** Smart Card Authenticated Mutual TLS



Bound Authenticator

A bound authenticator is an authenticator bound to the RP subscriber account and managed by the RP. Can be given to the subscriber by the RP or provided by the subscriber.

- **Examples**: Cryptographic authenticator

FAL3 provides techniques for high-risk federation transactions and is **not expected** to be deployed for public facing applications.

Protocol-Based Examples

Mapping FALs to Common Federation Protocols

	OIDC	SAML	Wallet
FAL1	Basic and Implicit OIDC profiles. Allows for dynamic registration and IdP discovery.	SAML Web-SSO profile. Allows for front-channel presentation. Allows for IdP-initiated login.	OIDC4VCI to issue credentials, OIDC4VP to present credentials. Subscriber can use their chosen CSP. Allows for cloud wallets.
FAL2	Authorization Code and Hybrid flows of OIDC. Requires RP to trust IdP ahead of time.	SAML Artifact Binding profile.	Use on-device presentation without going through a browser. RP can have a trusted CSP list without knowing specific wallets. Allows for cloud wallets.
FAL3	Include the claims for Holder-of-Key and Bound Authenticator assertion presentations in the ID Token.	SAML Holder-of-Key profile.	CSP has strict onboarding procedures that are known to the RP. On-device wallet uses proof of possession presentation.

NEW!

- Section 9 provides a mapping and substantial set of examples for implementing aspects of federation consistent with 800-63C
- These examples are not comprehensive but illustrative.
- No simple “do this protocol” to “achieve this FAL”
- Focus is on aspects and options within the protocols that are needed
- Greater detail possible in profiles or implementation resources

Q&A

Next Steps & Closing

What is Next?

Conformance Criteria

- For all 4 volumes – controls, control objectives, and assessment methods
- Exploring machine readable OSCAL versions

Implementation Resources

- Still open to feedback! Send dig-comments@nist.gov any recommendations
- DIRM Workbook and user guide
- User journeys for identity proofing flows

Ongoing Research

- Deepfake detection and injection protections
- NCCoE mDL Project
- NCCoE Project – Digital Identity: Applying Digital Identity Standards to Software Agents

Thank You!