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

Digital Identity – *What's Next For NIST?*

NIST Information Technology Lab

July 2023

Welcome & Session Overview

Ryan Galluzzo, Identity Program Lead, Applied Cybersecurity Division

Why are we here today?

Purpose:

- To provide an update on the development of NIST Digital Identity Guidelines
- To provide an overview of the public comment feedback, key issues, and major themes
- To discuss potential changes to each volume to meet with the feedback we have received

Outcomes:

- ✓ You will have insight into current state of the update and the general roadmap for each volume
- ✓ You will have insight into the major areas where we received feedback
- ✓ You will have an understanding of directional changes based on the public comment period
- ✓ NIST will receive initial feedback on these planned changes

What will we be discussing?

Time	Event	Speaker/Facilitator
8:30 – 9:00am	Registration	N/A
9:00 – 9:10am	Welcome & Overview	Ryan Galluzzo
9:10 – 9:20am	Opening Remarks	Kevin Stine
9:20 – 9:50am	Comment Period Overview	David Temoshok
Break 9:50-10:00		
10:00 – 10:35	Base Volume	Connie LaSalle
10:35 – 11:30	NIST SP 800-63 A	Ryan Galluzzo
Break 11:30– 11:45		
11:45 – 12:30	NIST SP 800-64B	Andy Regenscheid
12:30 – 1:00	NIST SP 800-63C	David Temoshok
1:00 – 1:30	Closing Remarks	Ryan Galluzzo
2:00 – 2:30	Optional In-Person Discussion – Roadmap	Ryan Galluzzo

Some Notes on Engagement

We greatly encourage questions and discussion!

- Each session will have time reserved for Q&A
- We will take questions from in the room and online
- We will do our best to get to as many as possible but probably won't get to all of them
- Those in the room can raise your hand, please help in passing the mics around!

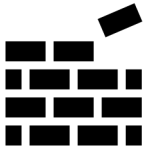
For virtual attendees, on Slack we will host an open discussion where:

- Everyone can engage in discussion, debate, and constructive feedback…
- Everyone can submit questions for NIST team members
- We may not get to all of the questions, but we will do our best
- Looking for the invite to the slack? We have posted in the Webex chat over here*

* Accuracy of arrow not guaranteed…

Rules of the Road

Be polite and be respectful!



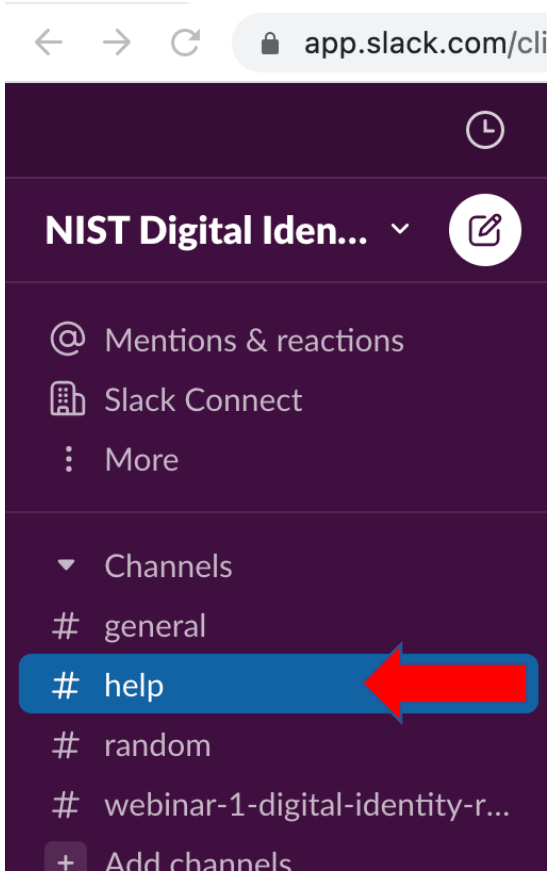
Be constructive!

No spam, no marketing!

Debate, discussion, and questions are encouraged!

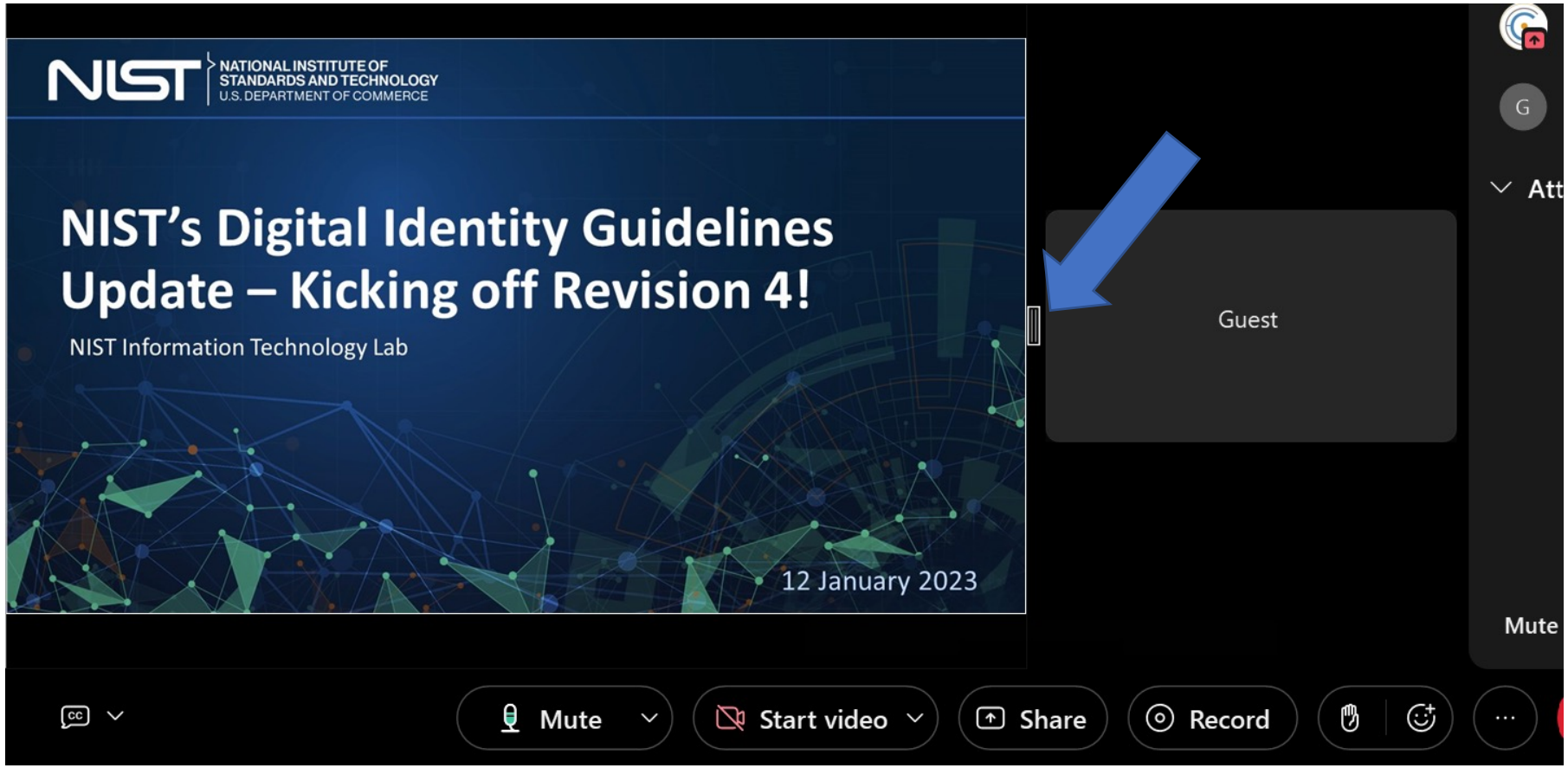
Webex Captioning

Our panel will be simulcast with live captioning. The link to access this is posted in the Webex Chat and in the "help" section of Slack



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.



Opening Remarks

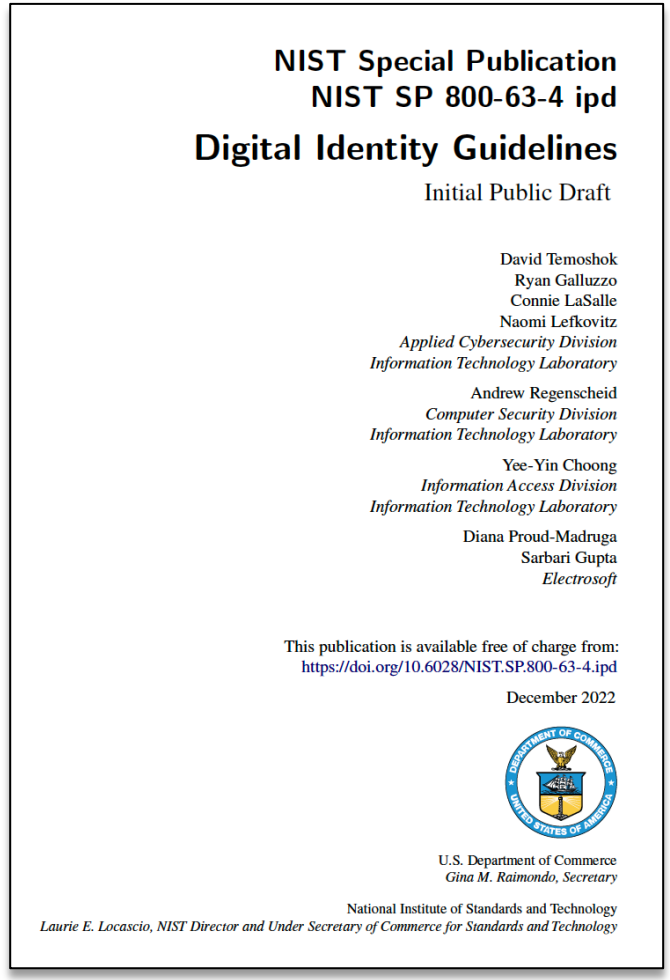
Kevin Stine, Chief of the Applied Cybersecurity Division

Comment Period Overview

David Temoshok, NIST SP 800-63 Lead, Applied Cybersecurity Division

What Are the Digital Identity Guidelines?

- Details the process and technical requirements for Digital Identity
- 4 volumes:
  - Base – Digital Identity Model and Risk Management
  - A – Identity Proofing & Enrollment
  - B – Authentication & Lifecycle Management
  - C – Federation & Assertions
- Last major revision in June of 2017
- Call for Comments in September 2020
- Draft & Public Comment Period in December 2022
- Closed Comments in April 2023



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

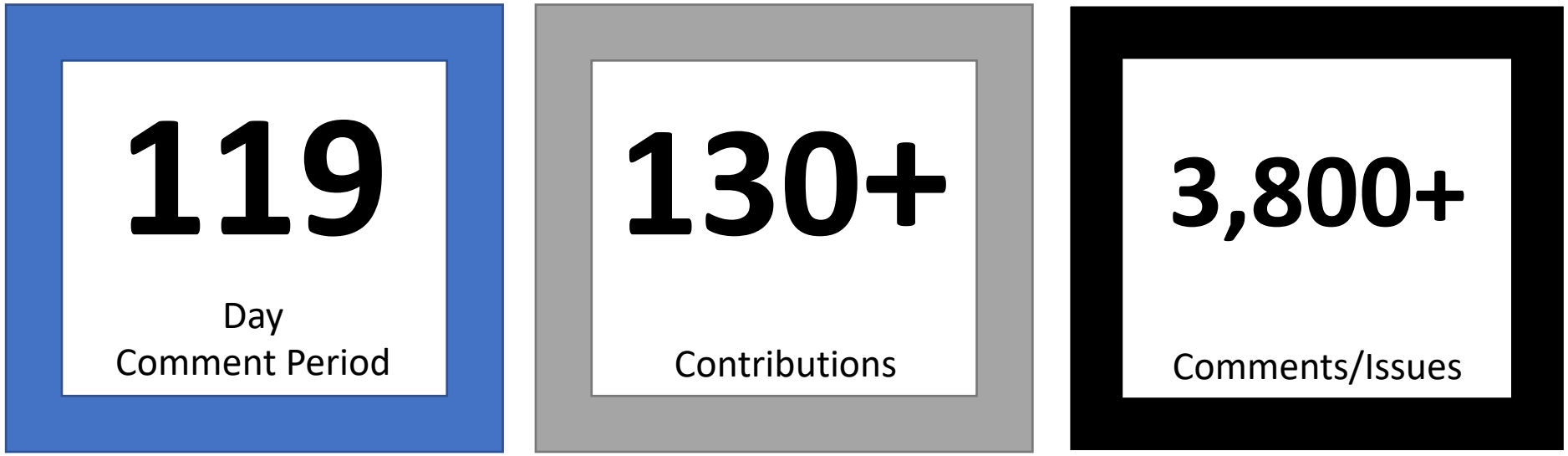
National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Why Did We Make Changes?

- 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.

Contributions

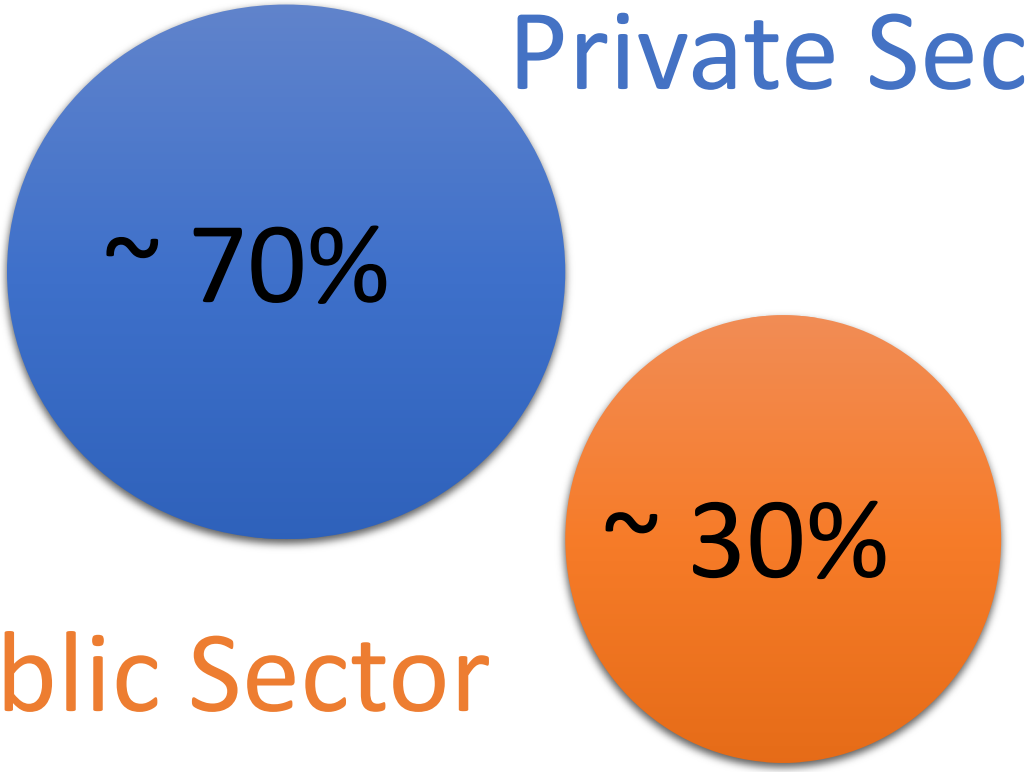
The comment period closed on April 14th and we received a tremendous amount of feedback from a diverse array of interested parties.



Comments will be triaged, analyzed, adjudicated and updated timeline developed.

End of the Comment Period is NOT the end of dialogue!

Who Did We Hear From?



- Government
- Advocacy
- Gaming & Gambling
- Identity Services
- Higher Education
- Manufacturing
- Security

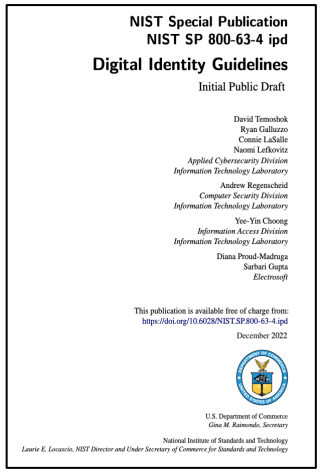
Comment Adjudication Process

- Open all comments as GitHub issues
- Links to common, related issues

- Status: Accept, Accept in Principle, Noted, Not Accepted
- Adjudication rationale
- All issues: Open or Closed

- Text changes
- Implementation Resources
- Other NIST pubs
- Research

Comment Adjudication & Volume Status


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

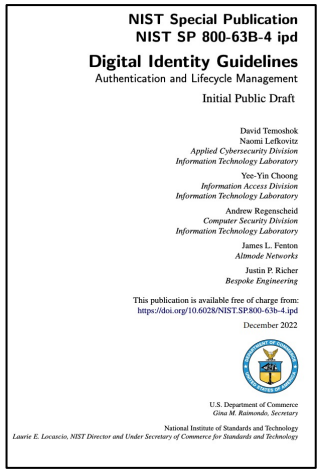
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-4.ipd
December 2022

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

Base Volume

Total Comments: 983

Likely Next Step: Second Public Comment


NIST Special Publication
NIST SP 800-63B-4 ipd
Digital Identity Guidelines
Authentication and Lifecycle Management
Initial Public Draft

David Temoshok
Naomi Lefkovitz
Applied Cybersecurity Division
Information Technology Laboratory
Yee-Yin Choong
Information Access Division
Information Technology Laboratory
Andrew Regenscheid
Computer Security Division
Information Technology Laboratory
James L. Fenton
Altmode Networks
Justin P. Richer
Bespoke Engineering

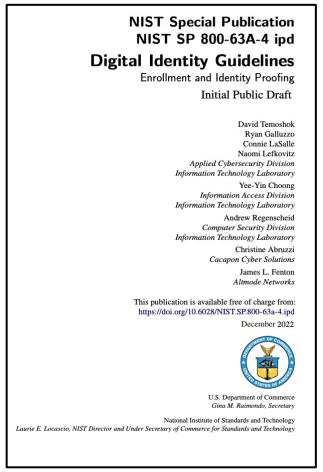
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63b-4.ipd
December 2022

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

800-63B

Total Comments: 795

Likely Next Step: Final


NIST Special Publication
NIST SP 800-63A-4 ipd
Digital Identity Guidelines
Enrollment and Identity Proofing
Initial Public Draft

David Temoshok
Ryan Galluzzo
Connie LaSalle
Naomi Lefkovitz
Applied Cybersecurity Division
Information Technology Laboratory
Yee-Yin Choong
Information Access Division
Information Technology Laboratory
Andrew Regenscheid
Computer Security Division
Information Technology Laboratory
Christine Abruzzi
Cacapon Cyber Solutions
James L. Fenton
Altmode Networks

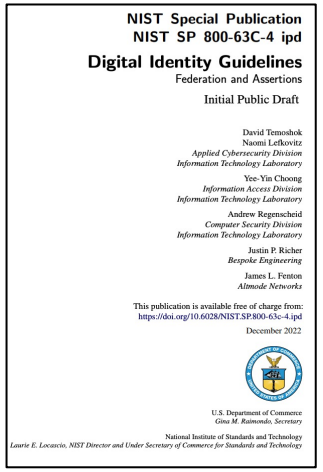
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63a-4.ipd
December 2022

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

800-63A

Total Comments: 1504

Likely Next Step: Second Public Comment


NIST Special Publication
NIST SP 800-63C-4 ipd
Digital Identity Guidelines
Federation and Assertions
Initial Public Draft

David Temoshok
Naomi Lefkovitz
Applied Cybersecurity Division
Information Technology Laboratory
Yee-Yin Choong
Information Access Division
Information Technology Laboratory
Andrew Regenscheid
Computer Security Division
Information Technology Laboratory
Justin P. Richer
Bespoke Engineering
James L. Fenton
Altmode Networks

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63c-4.ipd
December 2022

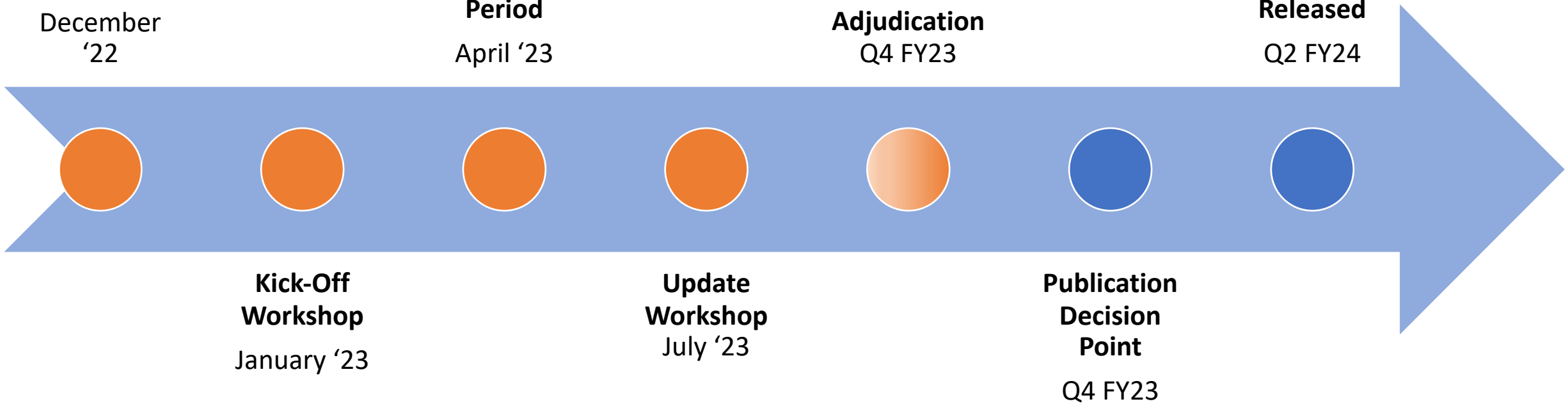
U.S. Department of Commerce
Gina M. Raimondo, Secretary
National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

800-63C

Total Comments: 610

Likely Next Step: TBD

What's Next?



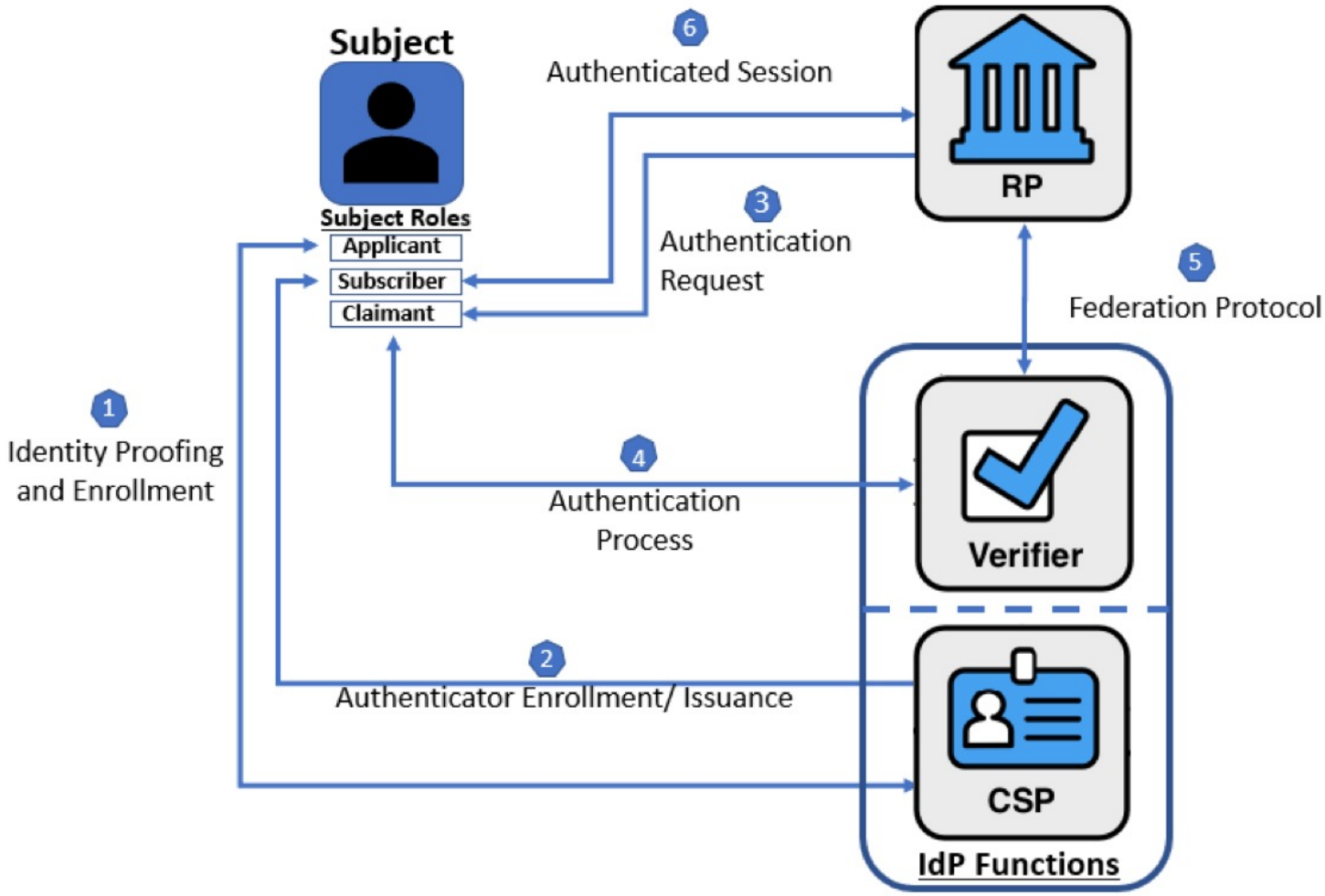
Some volumes will require a second public draft; to avoid implementation challenges all volumes will be issued as Final at the same time.

NIST SP 800-63-4: Digital Identity Guidelines (Base Volume)

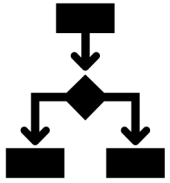
Connie LaSalle, Senior Technology Policy Advisor, Information Technology Lab

Volume Overview – 800-63 Base Volume

- Introduces and describes foundational concepts, roles, and responsibilities referenced throughout all volumes, framed within the context of a digital identity model.
- Provides a risk assessment methodology and a risk-based process of selecting assurance levels for identity proofing, authentication, and federation.
- Enumerates the definitions and abbreviations relevant to the special publication.



63 Base- Key Changes from Revision 3

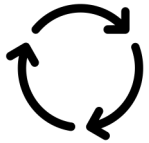


Revamps the risk management approach to be more process-oriented

Amends the assurance level selection process and introduces tailoring

Updates the digital identity model to support more deployment options

Introduces new terms and concepts that flow throughout



Focuses on continuous evaluation and improvement of identity systems

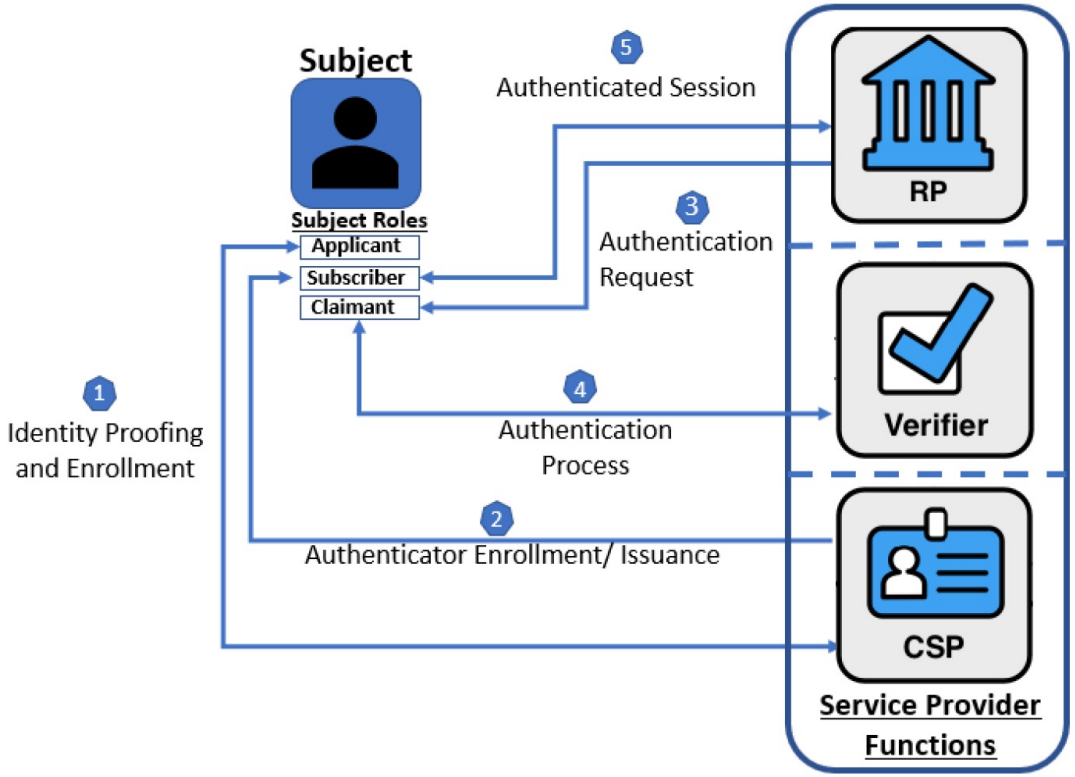
Emphasizes a multi-disciplinary approach to assessing and managing risk

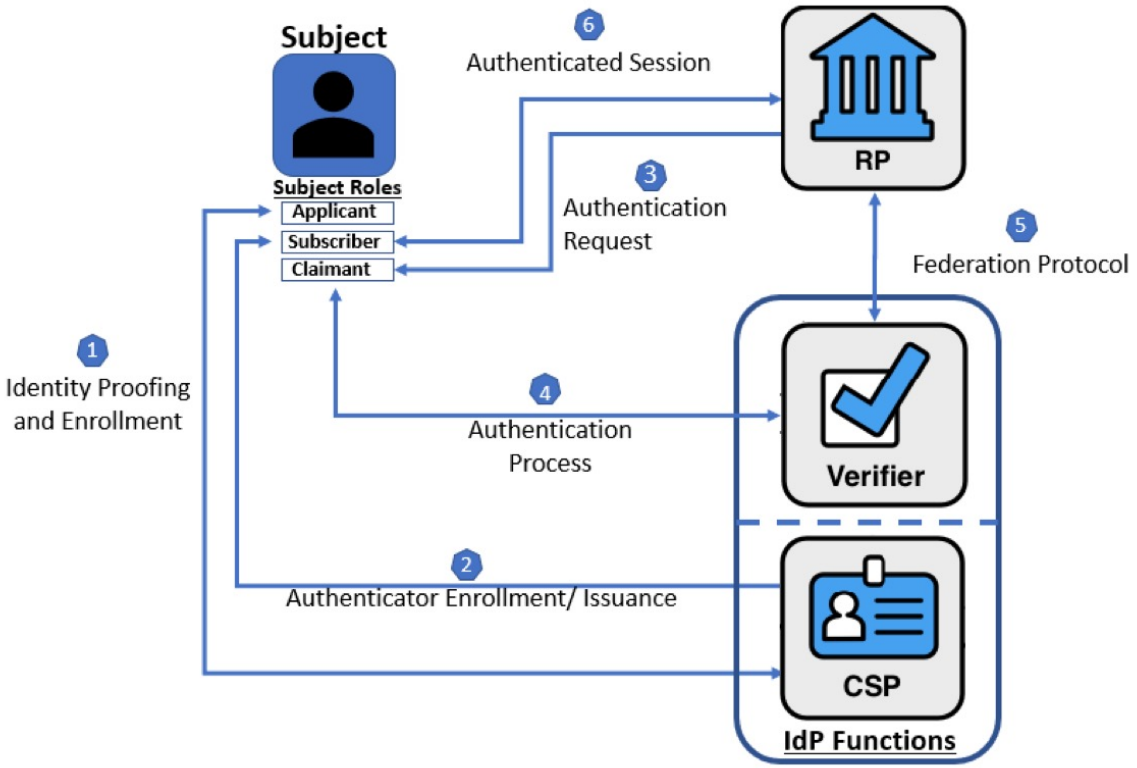
Details equity considerations and elevates evaluation of risks to individuals and communities within impact assessment and risk management processes

Key Changes from Rev. 3 – 800-63 Base Volume

Updated Digital identity Model

- Updated Digital Identity Model to better illustrate participant roles and functions and provide a separate model for federation.





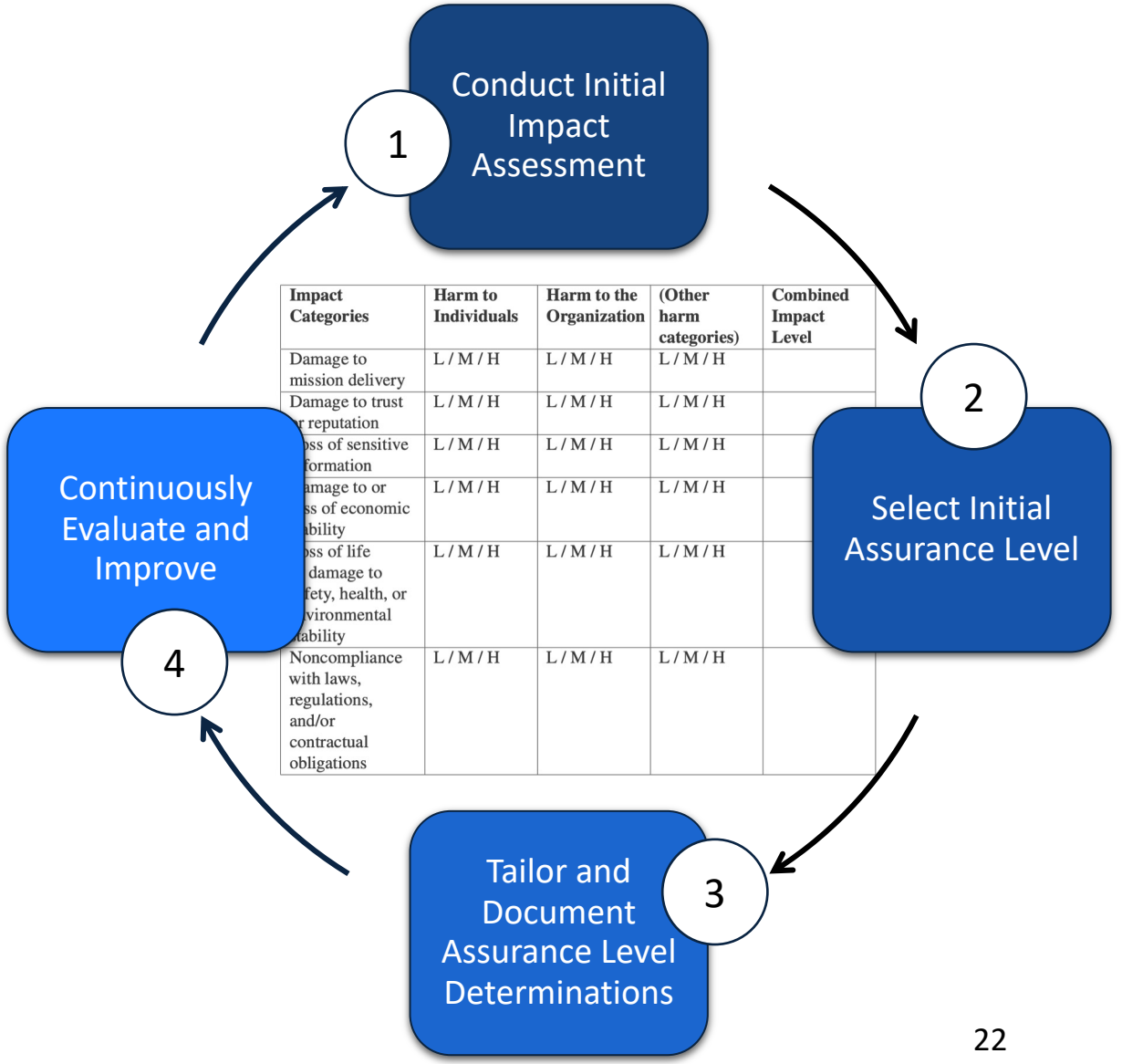
Key Changes from Rev. 3 – 800-63 Base Volume

Updated Digital Identity Risk Management

- Updated Risk Management Model to incorporate lessons learned and emerging attacks - social engineering, automated attacks, synthetic identity.
- Revised risk assessment and impact analysis processes to address risks and impacts for equity, privacy and usability and impacts to organization, agency mission, individuals, other organizations and the nation.
- Addition of continuous evaluation and integration with organization cybersecurity and fraud teams to identify and mitigate new threats, attacks, and risks.

xAL Selection:

- Revised xAL selection process to incorporate expanded impact analysis for equity, privacy, usability, and agency mission.



Impact Categories	Harm to Individuals	Harm to the Organization	(Other harm categories)	Combined Impact Level
Damage to mission delivery	L / M / H	L / M / H	L / M / H	
Damage to trust r reputation	L / M / H	L / M / H	L / M / H	
ss of sensitive formation	L / M / H	L / M / H	L / M / H	
mage to or ss of economic bility	L / M / H	L / M / H	L / M / H	
ss of life damage to fety, health, or vironmental bility	L / M / H	L / M / H	L / M / H	
Noncompliance with laws, regulations, and/or contractual obligations	L / M / H	L / M / H	L / M / H	

Comment Period Major Topics - Overview

1. Digital Identity Model
2. Risk Management Process
3. Continuous Evaluation & Improvement

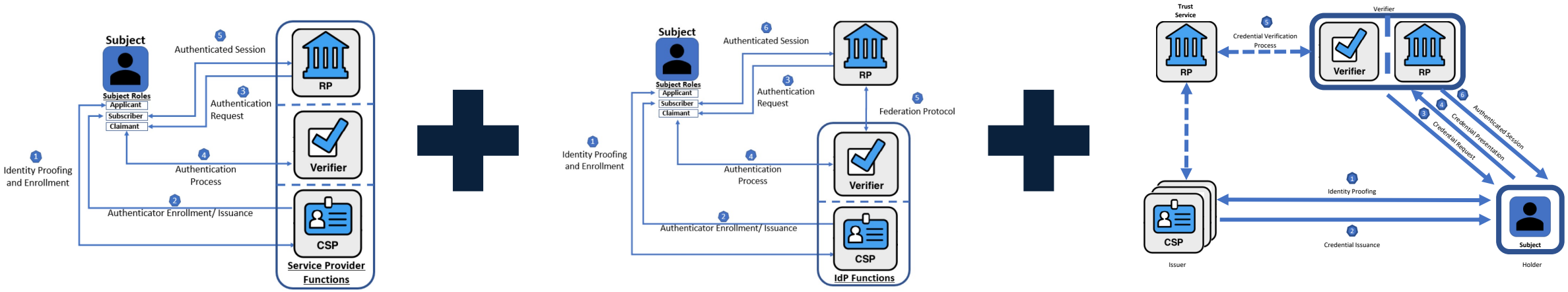
Topic 1: Digital Identity Model

What we've heard:

- Requests to account for the issuer-holder-verifier model envisioned for verifiable credentials

What we are considering:

- Updated model/s that account for a range of implementations, responsibility models, and contexts

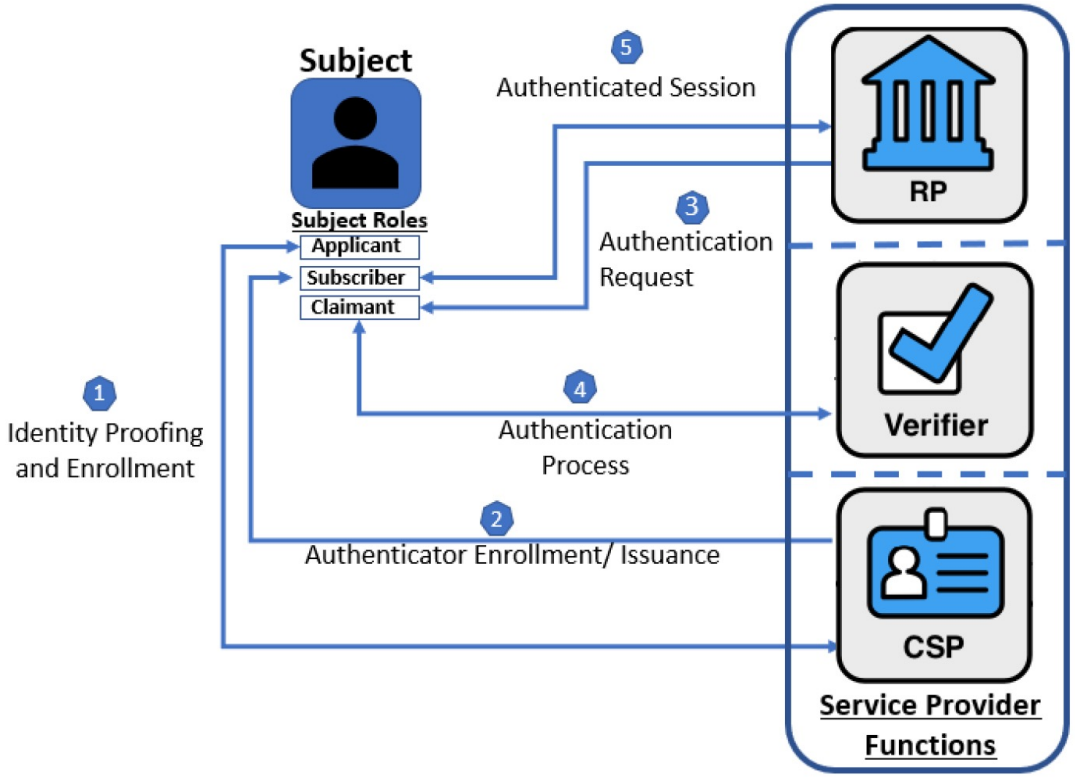


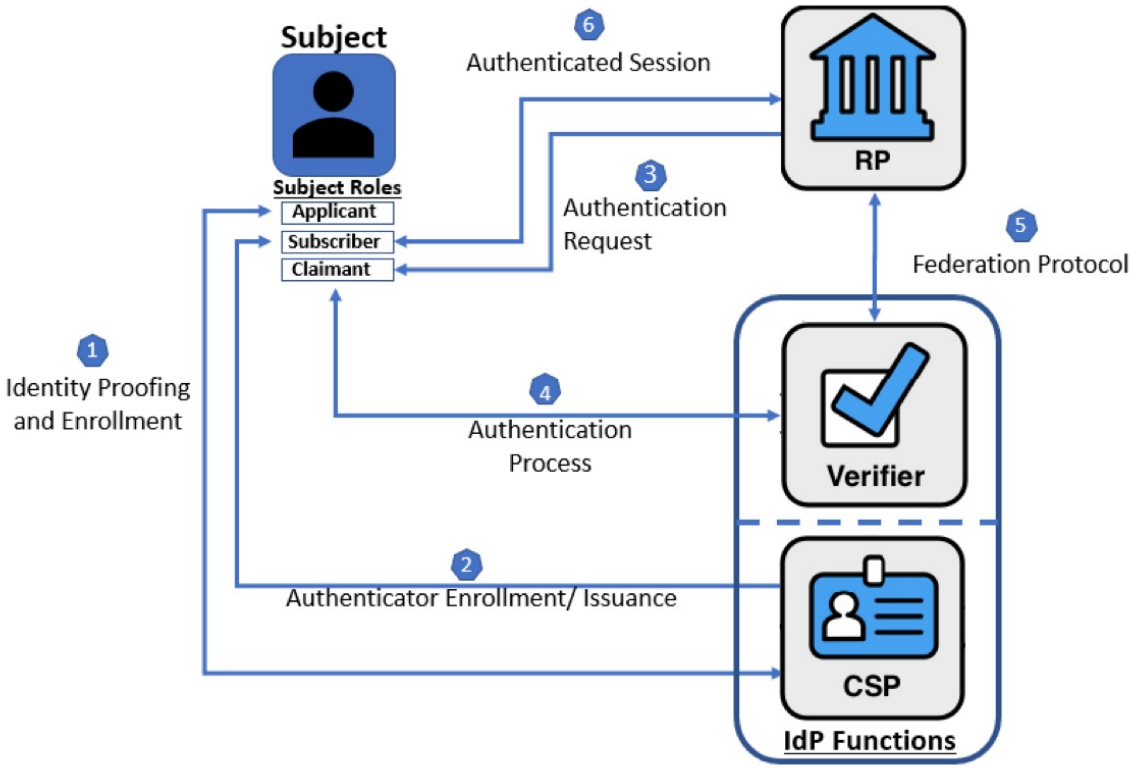
Topic 1: Digital Identity Model

Reminder: Key Changes from Rev. 3 – 800-63 Base Volume…

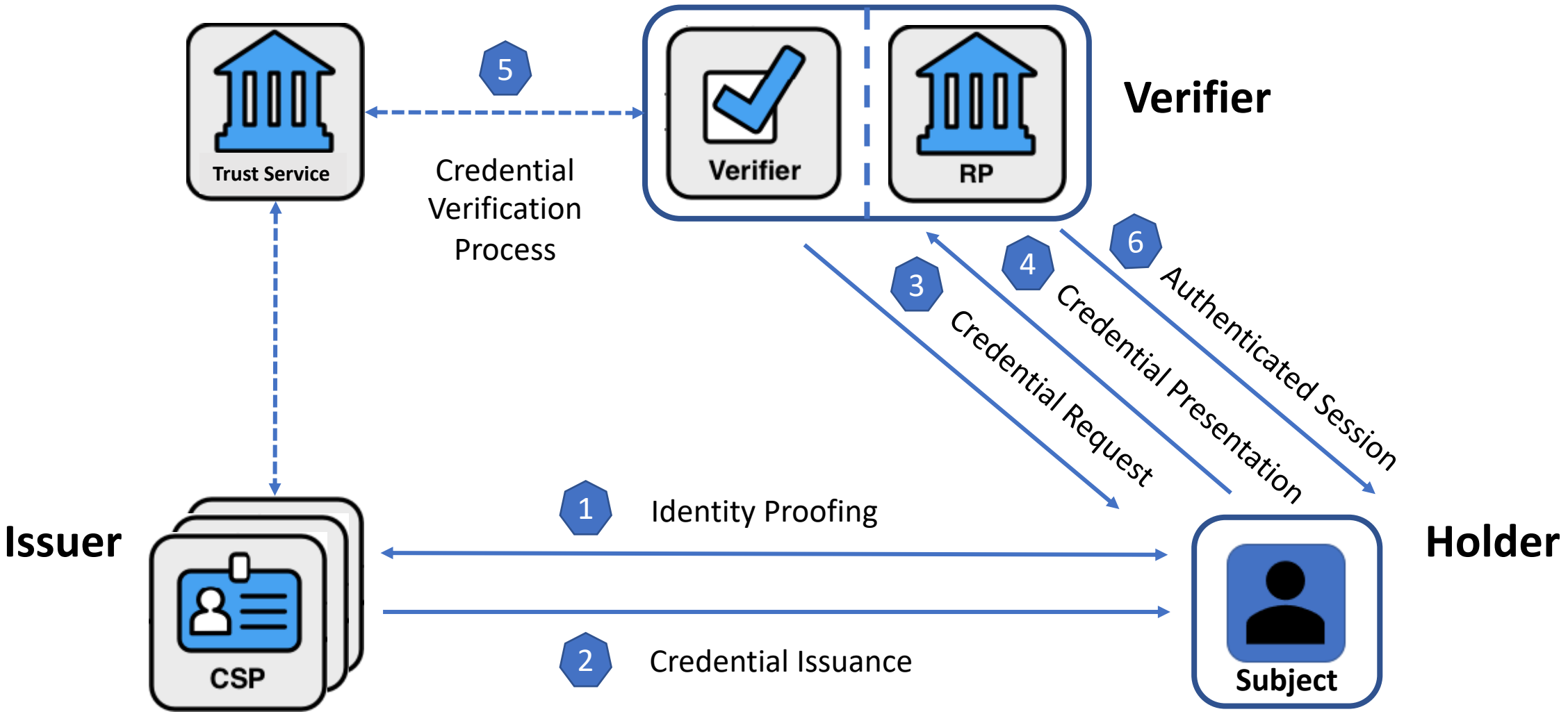
Updated Digital identity Model

- Updated Digital Identity Model to better illustrate participant roles and functions and provide a separate model for federation.





Topic 1: Digital Identity Model



Topic 2: Risk Assessment Process

What we've heard:

- Requests for more guidance on how to balance risk areas
- Requests for more guidance on how to assess equity
- The process is easy to understand …… The process is difficult to understand
- Bring back the decision trees ……. Thank you for removing the decision trees

What we are considering:

- Clarifications to the guidance itself (e.g., how to tailor)
- Supplemental implementation resources (e.g., DIRA template update, profiles of -63 based on context of use, playbooks, etc.)
- A visual aid that still allows for flexibility across contexts

Topic 3: Evaluation & Improvement

What we've heard:

- Be more explicit that equity is something to be continuously evaluated
- Provide some metrics for evaluation
- Consider risk scoring along gradients (e.g., percentiles vs. pass/fail)

What we are considering:

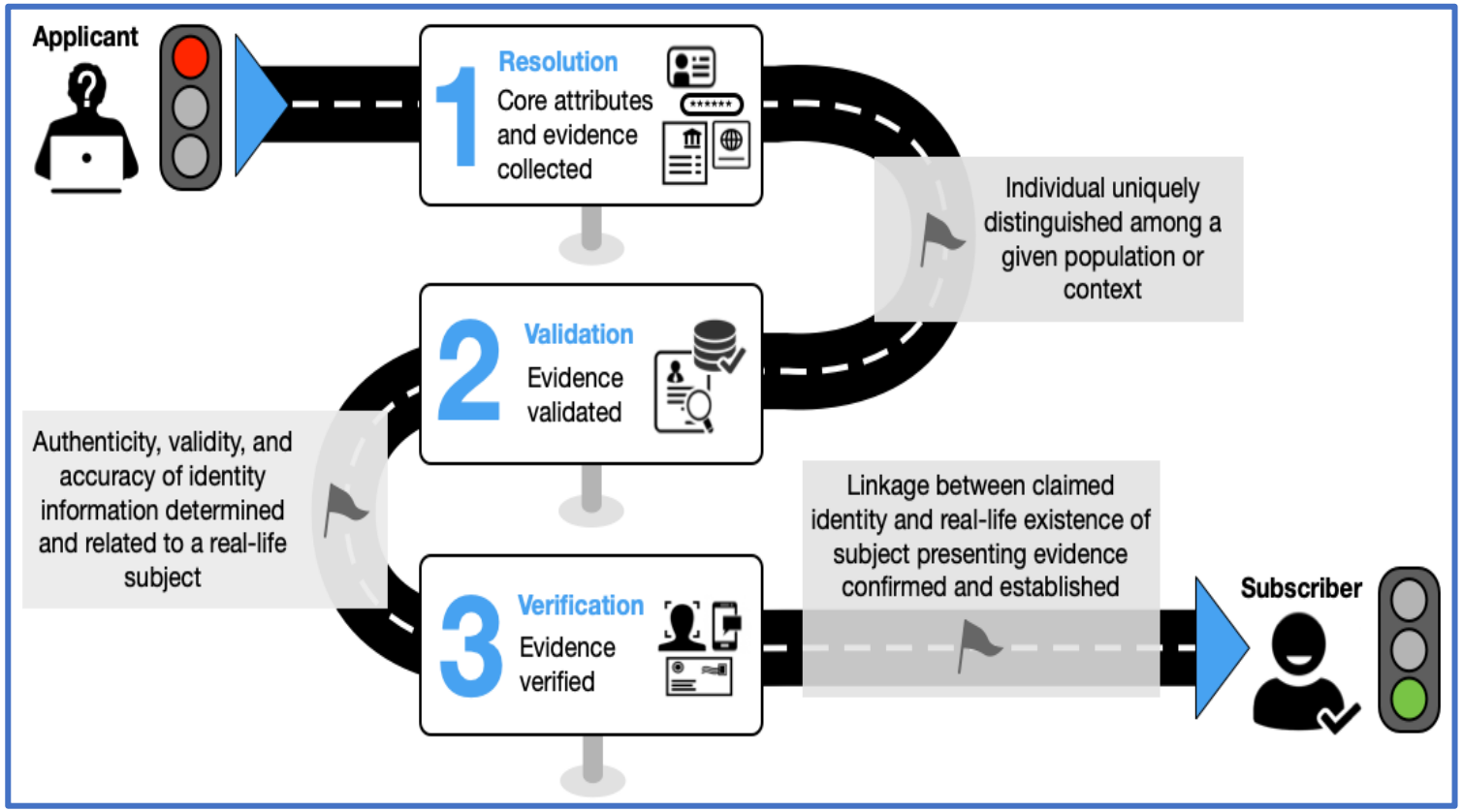
- More explicit language about how equity can be continuous evaluated and improved
- Potential informative examples of metrics that could be used, for instance:
  - *False Rejection Rates or Number of Attempts Before Successful Proofing*
  - *Call Center and Support Usage*
  - *MFA Type Usage*
  - *Evidence Type Usage*
  - *Identity Proofing Channel Usage and Corresponding Account Lockout or Reset Rates*
  - *Failure Points (across proofing steps)*
  - *Incident/Fraud Rates (suspected, confirmed)*

NIST SP 800-63A: Enrollment and Identity Proofing

Ryan Galluzzo, Identity Program Lead, Applied Cybersecurity Division

Volume Overview – 800-63 A

- Defines roles and responsibilities for identity proofing of applicants
- Defines process for proofing including three core process steps: resolution, validation, and verification
- Provides detailed requirements for each assurance level
- Provides requirements for privacy, equity, security, biometric usage.



Summary of Key Changes from Revision 3

- Revamps Risk Management and Assurance Selection Process
- New biometric requirements for proofing performance, testing, consent, retention
- Introduces digital evidence concept (e.g., mDL and Verifiable Credentials)
- Establishes a new Identity Assurance Level 1 where biometrics are optional
- Updates Trusted Referee and mandates it at the system level.
- Introduces the concept of an applicant reference.
- Provides requirements and considerations for equity impact assessments & design

Major Topics – What Did We Hear

- More consistent structure of requirements, particularly between remote, in-person, attended, and supervise remote in-person.
- Greater clarity on the roles played in identity proofing process (e.g., referees, attendants, and others).
- There needs to be greater detail on the use of both trusted referees and applicant references.
- More baseline fraud checks and fraud program requirements must be included for CSPs.
- IAL1 requirements and the balancing of usability and security

More consistent structure of requirements

What we've heard: The presentation of requirements for different methods of proofing (e.g., in-person, remote) are still not clear enough.

What we are planning:

- Restructure all IAL requirements around an updated taxonomy of proofing
- Will cover: ***In-person Attended; In-Person Unattended; Remote Unattended; Remote Attended***
- Each assurance level will have requirements structured around these 4 methods
- Supervised remote identity proofing would be reframed consistent with this structure rather than a unique IAL3 process

More consistent structure of requirements

Type	Description
In-person Attended	Identity Proofing conducted in an in-person setting where the applicant completes the entire identity proofing process - to include resolution, validation, and verification – in the presence of a Proofing Agent in a controlled environment.
In-Person Unattended	Identity proofing conducted where an individual would interact with a kiosk, but where no interaction with an agent is required. The process is fully automated, but at a physical location approved by the CSP.
Remote Attended	Identity Proofing conducted where the applicant completes resolution, validation, and verification steps through a secure video session with a Proofing Agent. For IAL3 identity proofing, the mechanism to support remote unattended must be in a controlled environment, such as a secure facility or kiosk.
Remote Unattended	Identity Proofing conducted where the resolution, validation, and verification processes are completely automated and there is no Proofing Agent facilitating attending the proofing process.

Greater clarity on the roles in identity proofing

What we've heard: The roles being played by individuals that support the identity proofing process are not clear enough (e.g., a trusted referee v. a trained agent v. assistance)

What we are planning:

- Provide a section that covers the potential roles that are expected in support of identity proofing
- Tentatively will cover: ***Proofing Agent, Trusted Referee, Applicant Reference, and Process Assistant***
- The intent is to support clearer delineations between different types of proofing and who takes what actions within those processes

Greater clarity on the roles in identity proofing

Roles	Description
Proofing Agent	An agent of the CSP who is trained to attend identity proofing sessions and can make limited risk-based decisions – such as physically inspecting identity evidence and making physical comparisons of the applicant to identity evidence.
Trusted Referee	An agent of the CSP who is trained to make risk-based decisions regarding an applicant's identity proofing case when that applicant is unable to meet expected requirements of a defined IAL proofing process. The level of training is expected to be more substantial than that of an agent.
Applicant Reference	A representative of the applicant who can vouch for the identity of the applicant, specific attributes related to the applicant, or conditions relative to the context of the individual.
Process Assistant	An individual, whether offered by the CSP or the applicant, who provides support for the proofing process but does not support decision making or risk based evaluation. For example: translation, transcription, or accessibility support.

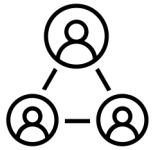
Additional Detail on TR & AR

What we've heard: Applicant Reference and Trusted Referee need more detail to support implementation.

What we are planning: Adding more detail!

Trusted Referee

- Policy and documentation
- Records management and retention
- Appropriate uses
- Communication of use to RPs
- Proofing/Onboarding of TRs
- Emphasizing role in support of exception an failure handling
- TRs are not just "attended proofing"



Applicant Reference

- Policy and documentation
- Evidence of relationship
- Records management and retention
- "Binding" the reference to applicant
- Possible uses of ARs
- Communication of AR usage to RP
- Risk assessment of AR usage
- Emphasize support for proofing ***not authorization to act for the applicant***

Additional Fraud Checks

What we've heard: Additional fraud checks are still needed, though there was limited consensus on what that should look like…

What we are considering:

- Require CSPs to have detection, prevention, and remediation capabilities
- Commenter suggestions under consideration:
  - Date of Death
  - Device & Account Tenure
  - Transaction Analytics (e.g., location, time, IP)
  - Fraud Indicator Checks (e.g., device finger print, consortium, investigative, or self-reported data, duplicate enrollments)
- Still determining Should v. Shall and per-level v. blanket
- Still determining additional AI and Privacy considerations relative to technology

Better balance of usability and security at IAL1

What we've heard: IAL1 and IAL2 are too similar and the level of friction remains high for both use cases

What we are considering at IAL1

- Adjusting requirements to focus more on scalable, automated, and synthetic attacks
- *Possible removal* of the requirement for document scanning of evidence
- *Likely* shifting the focus to the validation and verification of devices, digital evidence, and physical addresses (coupled with data validation)
- *Likely* adding notification of proofing requirement to strengthen reporting of incidents
- *Likely* augmenting with mandatory and optional fraud checks (e.g., Date of Death)

Other Topics or Changes

- **Core Attributes:** We will not define a baseline of core attributes due to business and application specific needs. We will provide informative examples.
- **Possession of a Digital Account**: Will be reframed as “Possession of Digital Evidence” to make clear that “accounts” would need to conform to evidence characteristics.
- **Evidence Examples**: We will provide examples of evidence. These examples will be informative.
- **Adjusting Fair Evidence**: Will be shifting the description to focus on types of evidence that can be validated and verified to provide more value to proofing
- **Cleaning up Address Confirmation**: Remains confusing to readers and overlaps with common forms of evidence
- **Non-Biometric Options**: Continuing to explore alternatives…
- **Including Binding @ Enrollment**: Shifting requirements for binding during enrollment from B to A; providing more specific requirements per IAL.

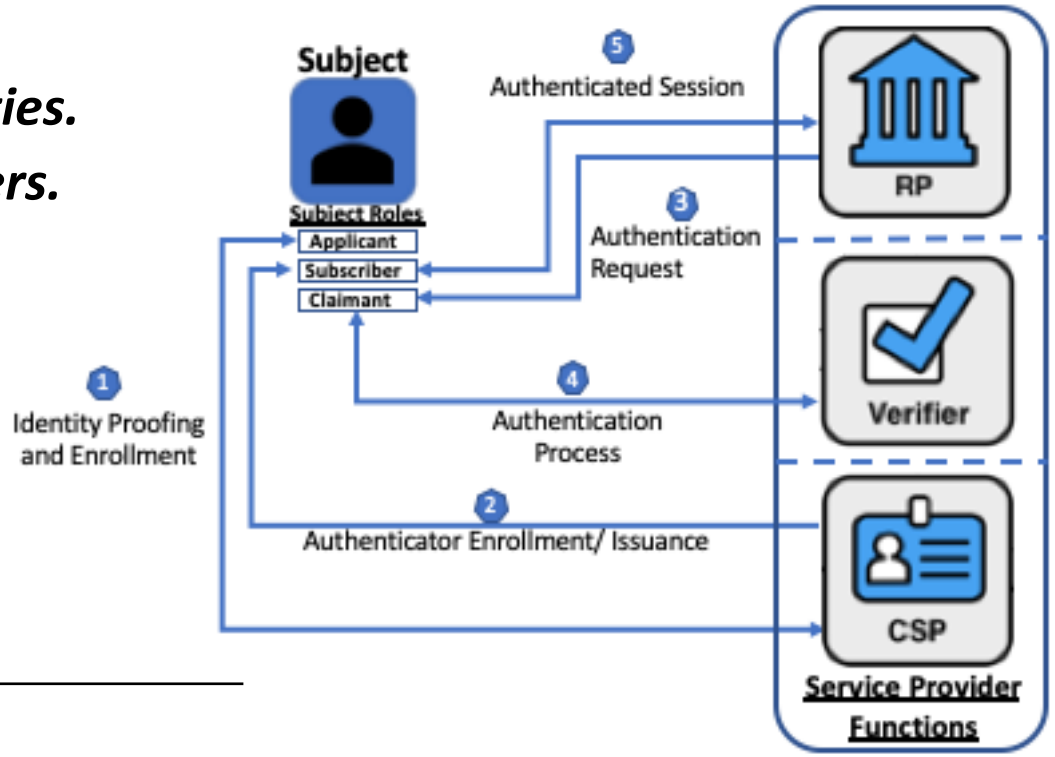
NIST SP 800-63B: Authentication and Lifecycle Management

Andrew Regenscheid, PIV Technical Lead, Computer Security Division

Volume Overview – 800-63B

Scope: Authentication and Lifecycle Management

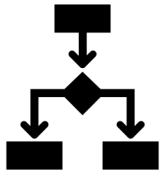
- Authenticators to authenticate ***subjects*** to ***relying parties.***
- Authentication processes and protocols used by ***verifiers.***
- Lifecycle:
  - Authenticator Selection and equity considerations
  - Authenticator Binding/Issuance
  - Session management
  - Account recovery



Authentication Assurance Levels

AAL1	• Single-factor authentication
AAL2	• Multifactor authentication • Supports implementation of EO 14028 and EO 13681 for MFA
AAL3	• Hardware-based, cryptographic multifactor authentication • Phishing resistant in support of OMB M -22-09 • Supported by PIV at federal agencies, consistent with HSPD-12

Key Changes from Revision 3



Defined Phishing Resistance (Channel or Domain Bound)

Removes restrictions on “cloning” of cryptographic authenticators at AAL2 to allow synching of keys

Eliminates the use of complexity and periodic changes of passwords

Updates requirements for activation secrets to distinguish device unlock v. over network

Updates performance requirements for biometric authenticators

Updates push authentication requirements to account for MFA exhaustion attacks

Maintains SMS to support usability of MFA for broadest range of users possible

Major Topics – What Did We Hear?

- Authentication Assurance Levels
- Phishing-Resistant Authentication
- Syncable Authenticators and Passkeys
- Session Management and Reauthentication
- Account Recovery

63B – Authenticator Assurance Levels

What we've heard:

- AAL2 includes a broad range of MFA methods with varying properties
- Suggestions to split AAL2 based on phishing-resistance property
- Questions/comments over phishing-resistance at AAL2

What we are considering:

- Requiring CSPs to offer a phishing-resistant authentication option at AAL2
- We are ***NOT*** creating additional assurance levels
- Organizations can choose to require phishing-resistant authentication at AAL2 for certain applications or use cases

63B – Syncable Authenticators

What we've heard:

- Questions over authenticators that allow export of secret/private keys, e.g., passkeys
- Suggestions to incorporate guidelines on cloud fabric used to back-up authenticator keys
- Need to address threats during account recovery flows

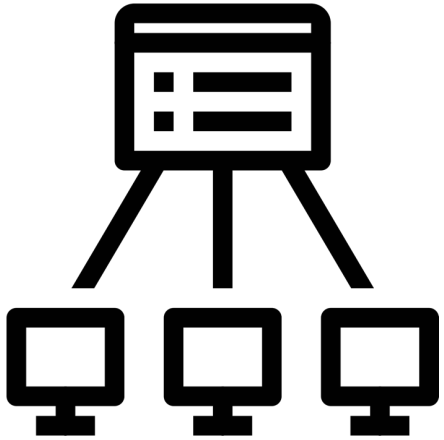
What we are considering:

- Clarifying 63B requirements for cryptographic and OOB authenticators to allow exportable secrets at AAL2, e.g., passkeys, OTP authenticator apps
- Describe threats/risks associated with syncing and/or sharing authenticators
- Adding guidance for organizations considering the use of syncable authenticators
    - Enterprise vs. consumer/BYOA considerations
    - Mobile Device Management policies
    - Controls/processes by cloud services to back-up, restore, and share authenticators

63B – Session Management

What we've heard:

- Questions/concerns regarding session lifetimes and inactivity timeouts
- Recommendations to incorporate other device/risk signals beyond time
- Consideration of managed devices enforcing local policies



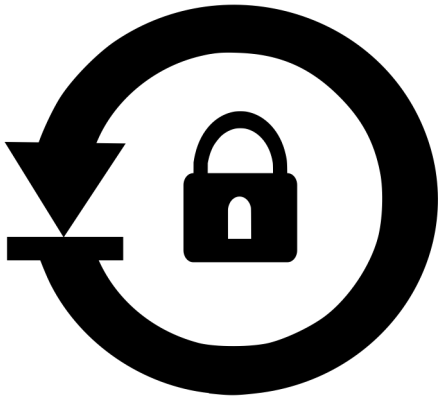
What we are considering:

- Retaining the session lifetimes (12 hours, and 30/15 minutes of inactivity at AAL2/3) as recommended baselines
- Developing guidance on tailoring session lifetimes and inactivity timeouts based on other controls, e.g.,
    - Device management and screen locks
    - Geolocation and time-based policies
    - Risk analytics

63B – Account Recovery

What we've heard:

- Questions on "abbreviated" proofing processes intended to support recovery
- Seeking additional options, traced to risks, for account recovery
- Desire to support recovery mechanisms for unproofed (i.e., IAL0) accounts



What we are considering:

- Developing account recovery processes for unproofed accounts
- Describing use of backup account recovery codes
- Clarifying recovery codes sent to digital/physical addresses
- Defining core elements of an "abbreviated" identity proofing process, to include a re-verification of identity

Other Topics or Changes

- **Authenticator Binding:**
  - Authenticator binding at enrollment will become part of proofing process in -63A
  - Expanding step-up binding processes (e.g., AAL2→ AAL3)

- **Passwords**:
  - Considering splitting password requirements for single-factor vs. multi-factor
  - Password hashing guidelines to recommend adopting updates to NIST cryptographic specifications

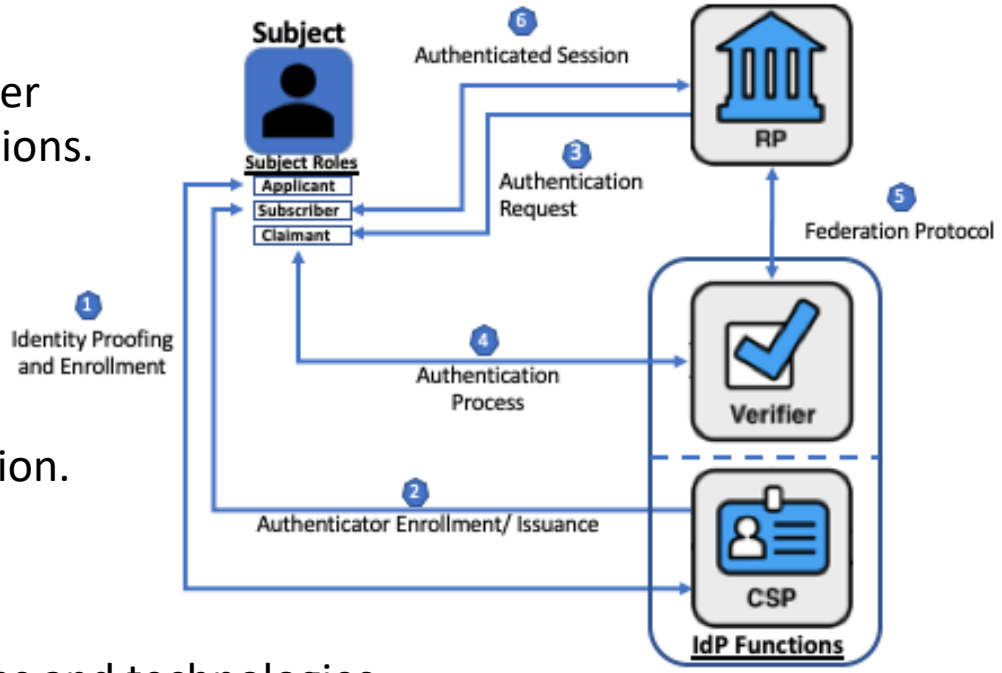
NIST SP 800-63C: Federation and Assertions

David Temoshok, NIST SP 800-63 Lead, Applied Cybersecurity Division

Overview

Scope: Federation and Assertions

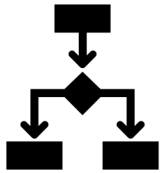
- **Federation –** conveyance of authentication attributes and subscriber attributes across networked systems– within and between organizations.
- **Trust establishment:** agreements between RPs and IdPs.
- **Registration:** secure communication between RPs and IdPs.
- **Assertions:** contents and presentation methods for assertions.
- **Privacy:** considerations for protecting personal subscriber information.



Federation Assurance Levels

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

Key Changes from Revision 3



Updated the FALs to make them clearer and more achievable

Added considerations for the use of provisioning and identity APIs

Incorporated discussion of trust agreements (e.g., trust frameworks)

Added concept of “Federated RP” account and associated controls

Added the concept of “bound authenticators” to FAL3

Adds equity Considerations for Federation Transactions and Processes

Major Comment Topics - Overview

- Guidance for treatment of verifiable credentials.
- Guidance for assertion attribute for IAL/AAL processes – validated/unvalidated attributes, compensating controls, use of Trusted Referee/Applicant Reference, phishing resistant MFA.
- 63C defined set of validated attributes.
- Additional guidance for bound authenticators.
- Clarify guidance for subscriber consent and authorized party for attribute release.
- Guidance for new concepts and terms.

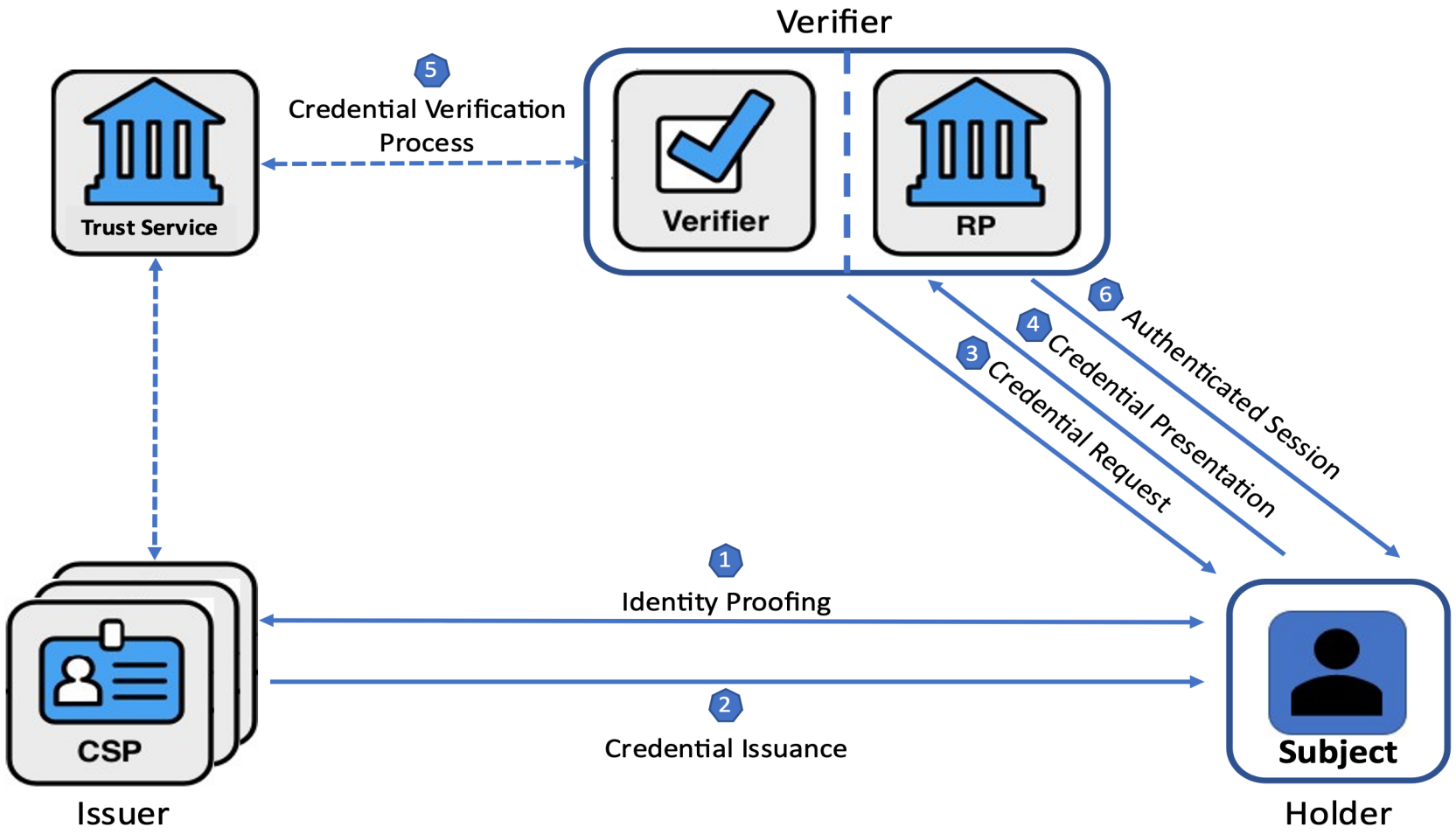
Guidance for treatment of verifiable credentials

What we've heard: 800-63-4 does not adequately address the treatment of mDLs and verifiable credentials.

What we are considering:

- Expand guidance in 800-63C s. 6 Assertions (s.6.3.1 Attribute Providers) to include processing of mDLs and verifiable credentials based on principles for assertion transactions. Likely in a separate section.
- Integrate mDL and VC model (Issuer, Verifier, Holder) into the digital identity models in 800-63 base volume sec. 4.1.
- Provide guidance for the presentation, verification, and processing of mDLs and VCs for identity proofing in 800-63A.

mDL/Verifiable Credential Digital Identity Model



Guidance for assertion attributes

What we've heard: Guidance is needed for IDP assertion attributes for IAL/AAL processes that impact RP acceptance – validated/unvalidated attributes, use of compensating controls, use of Trusted Referee/Applicant Reference, phishing-resistant MFA.

What we are considering:

- We are not intending to require assertion attribute processing requirements beyond IAL, AAL and FAL.
- We plan to expand guidance in 800 63C sections 5 and 6 for RP assertion requests and Federation Trust Agreements that attribute information needed by RPs for authorization such as IAL/AAL process requirements may be requested by RP assertion requests and built into Federation Trust Agreements.
- We look ahead to work with agencies to develop federation profiles for specific use cases/communities to support agency requirements and needs.

Define core attribute set for 800-63C

What we've heard: Guidance is needed to align and expand the 63A CSP/IDP requirement to define a set of validated core attributes for subscribers for 63C attribute sets asserted for federation.

What we are considering:

- We do not intend to define a standard set of core attributes in 800-63A or 63C.
- We do intend to address and align core attribute sets determined, documented, and validated by the CSP/IDP for identity proofing as a set of core validated attributes that can be included in Federation Trust Agreements and assertions.

Additional Guidance for Bound Authenticator

What we've heard: Need to clarify key requirements for bound authenticators including:

- Specify in 6.1.2 that bound authenticators are required for FAL3 and optional for FAL1/2.
- Types of binding required and permitted.
- Types of authenticators required and permitted.

What we are considering: We intend to provide additional guidance for bound authenticator requirements, types of binding and authenticators in descriptive text and use of examples.

Authorized Party for Attribute Release

What we've heard: Need to clarify requirements for the authorized party responsible for decisions/consent regarding the release of subscriber attributes.

What we are considering: We are intending to provide additional guidance for the requirements for the determination of the entity (IDP, attribute provider, subscriber) serving as the authorized party for both static and dynamic Trust Agreements.

Guidance for new concepts and terms

What we've heard: Need for guidance and definitions for new concepts and terms. Such as:

- Injection attacks, injection protections
- Federation authority
- Identity API, attribute API, provisioning API
- Authorized party
- Registration types and Trust Agreement.

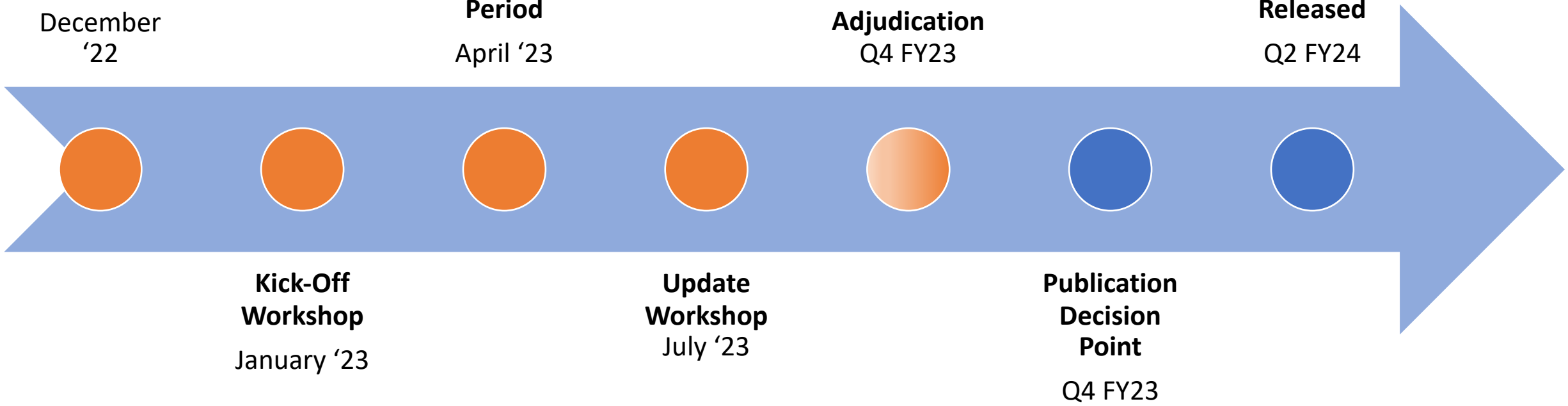
What we are considering:

- We intend to provide additional guidance as descriptive text, glossary definitions, and examples for new concepts and terms introduced in 800-63C.
- We also are intending to provide separate appendices for glossaries and terms definitions in each volume 800-63A, B, C for the specific terms used in those volumes. Base volume Appendix A Glossary will remain a consolidated presentation of definitions for terms across all volumes.

Key Dates and Next Steps

Ryan Galluzzo, Digital Identity Program Lead, Applied Cybersecurity Division

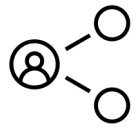
What's Next?



Some volumes will require a second public draft; to avoid implementation challenges all volumes will be issued as Final at the same time.

How Can You Get Involved?

Comment on our guidance! We have several open comment periods we need your feedback!



Engage at the NCCoE! From communities of interest to actual project participation there are multiple pathways to participate.

Participate in our Workshops! We have multiple events throughout the year to gain feedback, input, and insights from the community at large!

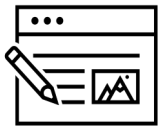
Email us and just say "hey!" We can be reached at dig-comments@nist.gov or email me directly at ryan.galluzzo@nist.gov

THANK YOU FOR ATTENDING AND PARTICIPATING!

Optional – Roadmap Discussion

What is NIST's Identity Program?

A multi-disciplinary team of IAM Experts, Cryptographers, Mathematicians, Privacy Engineers, Policy Advisors, Usability Specialists, and Biometrics Experts who…



Create Guidance

Develop Standards

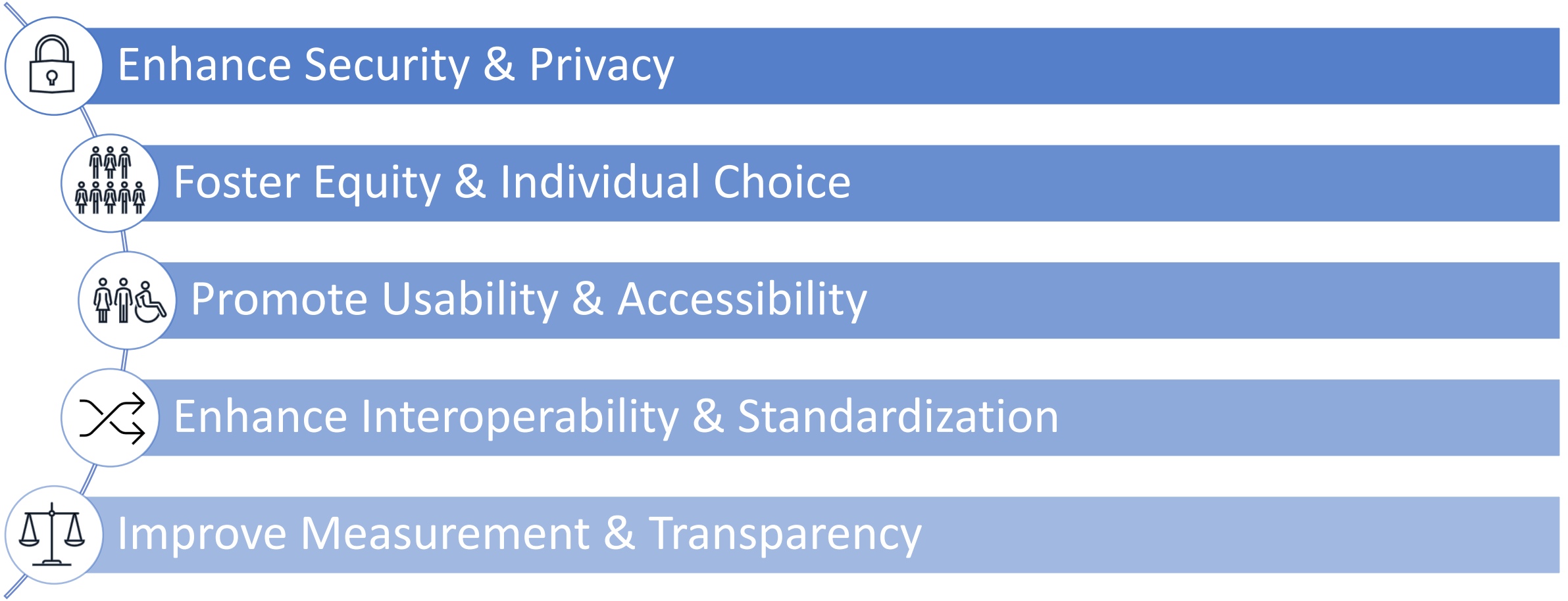
Conduct Foundational & Applied Research

Enhance Metrology

Enable "Transition to Practice"

NIST's IAM Roadmap codifies the work of this program and provides principles, objectives, and activities to guide efforts in the coming years…

What are our objectives?



How will we achieve these objectives?

- **Accelerate implementation and adoption of mDL and user controlled digital identities**
- **Expand and enhance biometric and identity measurement programs**
- **Promote technologies that enable authoritative attribute validation**
- **Advance secure, private, usable, and equitable identity proofing and fraud mitigation options**
- **Accelerate the use of phishing resistant, modern multi-factor authentication**
- **Modernize Federal PIV guidance and Infrastructure**
- **Advance dynamic authorization and access control schemes**
- **Promote greater federation & interoperability of identity solutions**

These Are Multi-Year Priorities That Will Define Research, Standards Engagement, and Development Activities Across NIST

Public Comment Contributions

The comment period closed on June 16th and we received feedback from a number of organizations

30+

Contributions

95% Industry

8 Different Org. Types

~20% Individual

- US Gov't
- Vendor
- Individual
- Consulting
- Healthcare
- Higher Ed
- Standards/Industry Body
- Advocacy

Comment Themes

We need more details and timelines!

Where is physical access control!?

Accessibility is discussed but there are no focused projects.

What about identity of NPEs!?

Additional focus on VC and Decentralized!

Include Privileged Access Management!

Updated threat models!

Next Steps


Triage Comments
Adjudicate Comments
Programmatic Review
Leadership Review
Final Roadmap Publication
Today
Q1 – FY24