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

NIST’s Digital Identity Guidelines Update – Kicking off Revision 4!

NIST Information Technology Lab

This webinar is being recorded

12 January 2023

Welcome & Session Overview

David Temoshok, NIST SP 800-63 Program Lead

Why are we here today?

Purpose:

➢ To kick off the public comment period for NIST SP 800-63 Revision 4!

➢ To provide you with insight into our proposed changes

➢ To enumerate the public comment process and timeline

Outcomes:

✓ You will have an understanding of the changes to revision 4 as well as the drivers that resulted in the proposed changes

✓ You will have insights into the areas where NIST is seeking specific input for the final version of the revision

✓ You will have details on the comment period and how to submit comments to the NIST team

What will we be discussing?

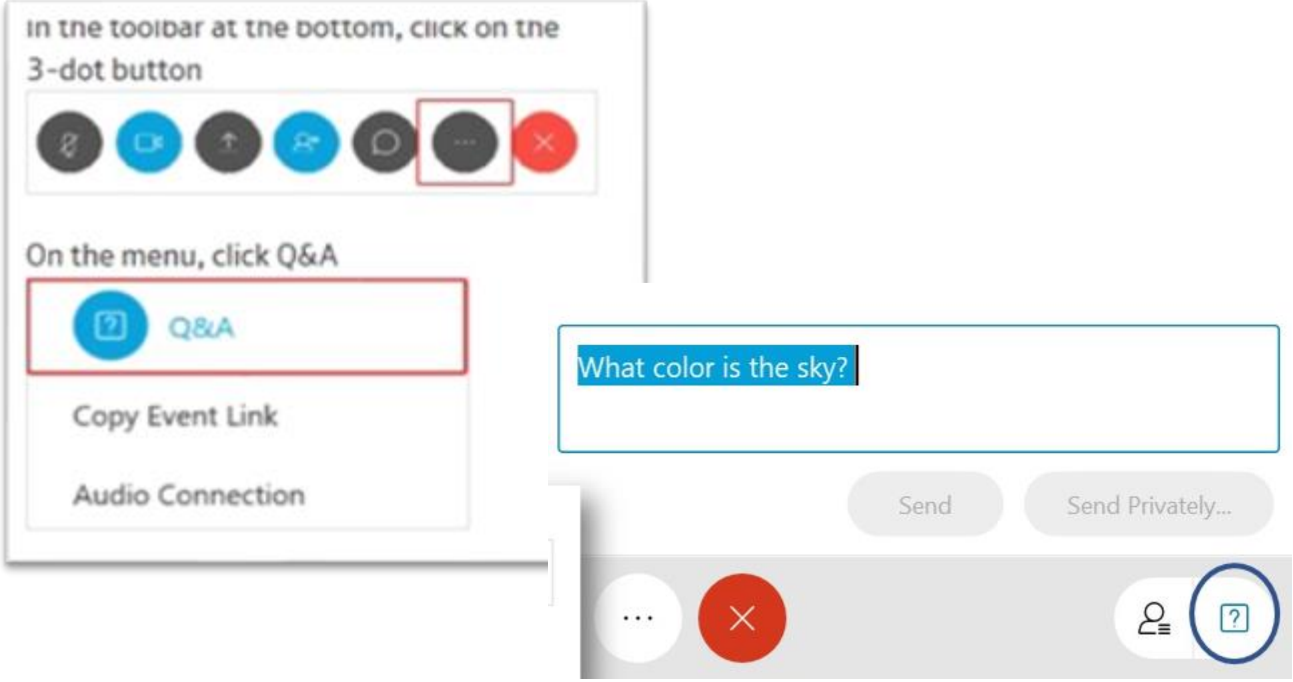
Item	Speaker	Time
Welcome	David Temoshok	5 minutes
Opening Remarks	Kevin Stine	5 minutes
Introduction – NIST and the Digital Identity Guidelines	Ryan Galluzzo	10 minutes
Changes to Base Document	Connie LaSalle	30 minutes
Changes to 63A	David Temoshok	45 minutes
Break 2:45 – 3:00		
Changes to 63B & 63C	Andy Regenscheid	45 minutes
Key Dates & Next Steps	Ryan Galluzzo	

Questions and Answers: Due to the high registration volume we will be using the Q&A feature on Webex. Please submit questions there. We will attempt to answer as many as possible.

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**.
5. We will answer as many questions as we are able during Q&A sessions.



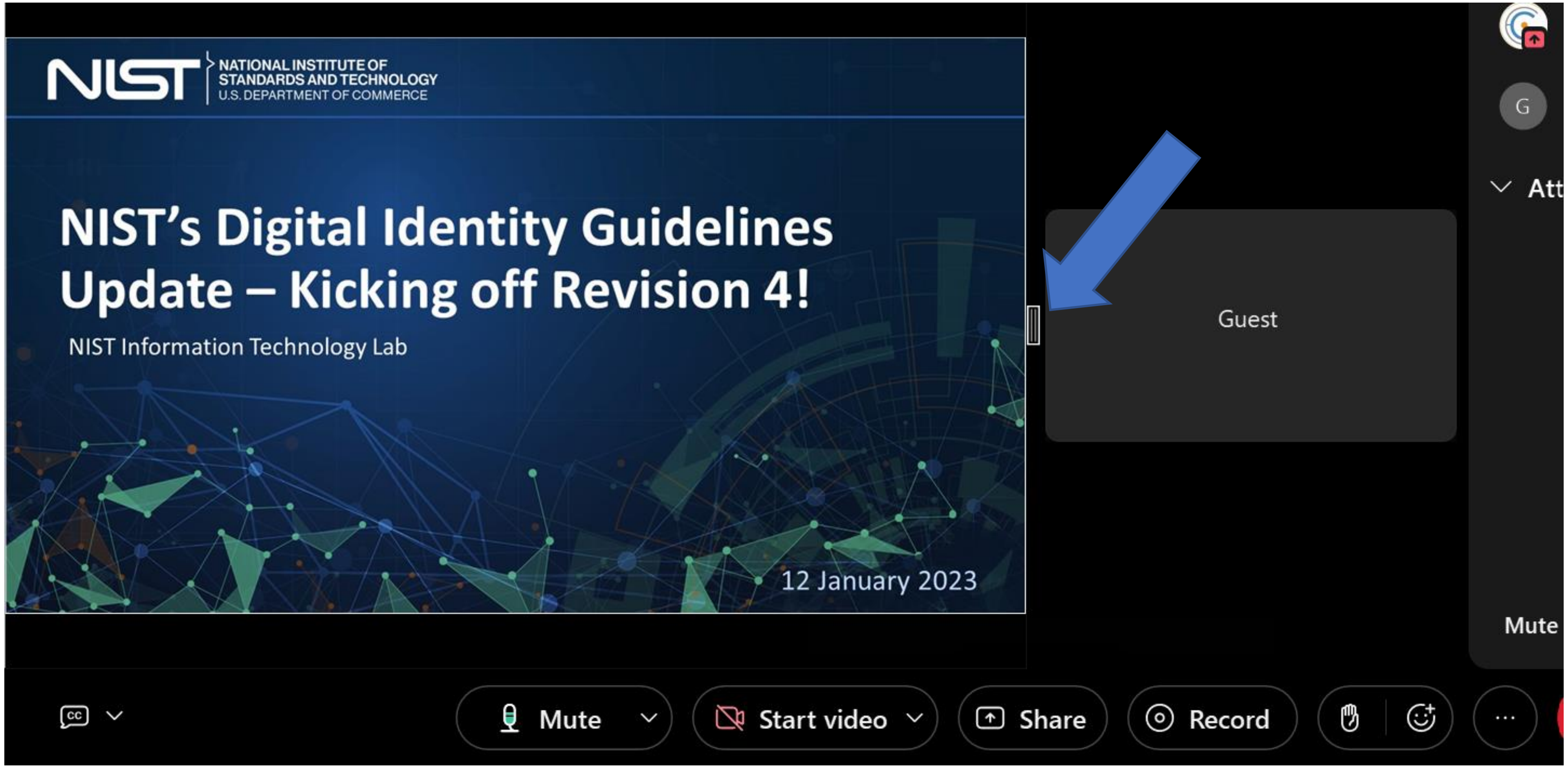
In the toolbar at the bottom, click on the 3-dot button

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.



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

NIST's Digital Identity Guidelines Update – Kicking off Revision 4!

NIST Information Technology Lab

12 January 2023

Opening Remarks

Kevin Stine, Chief of the Applied Cybersecurity Division

Introduction – NIST and the Digital Identity Guidelines

Ryan Galluzzo, Digital Identity Program Lead, Applied Cybersecurity Division

What is NIST?

Mission: To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Vision: NIST will be the world's leader in creating critical measurement solutions and promoting equitable standards. Our efforts stimulate innovation, foster industrial competitiveness, and improve the quality of life.

NIST is the US Government's primary agency for measurement, research, and standards development from manufacturing, to quantum computing, to cybersecurity…and nearly everything in between

What is NIST's Role in Digital Identity?

NIST's role is to…

- **Create Guidelines by way of** NIST Special Publication 800 series – for example NIST Special Publication 800-63: Digital Identity Guidelines. These are mandatory for federal agencies and widely adopted by commercial entities.
- **Develop Standards** such as Federal Information Processing Standards (FIPS) and contribute to international standards such as those developed in ISO, IETF, W3C, FIDO, and IETF.
- **Conduct foundational and applied research** to advance knowledge of Digital Identity Technology and Processes and bridge the gap between standards, guidance, and implementation.
- **Enhance Metrology** of identity systems to better understand performance, security, and equity of digital identity implementation.

NIST's ongoing initiatives include…

- Updating NIST SP 800-63, *Digital Identity Guidelines* and NIST 800-157, *Guidelines for Derived Personal Identity Verification Credentials* to address new technology and challenges.
- Creating new guidelines for PIV Federation in SP 800-217 to promote greater cross agency interoperability.
- Developing Mobile Driver's License standards in conjunction ISO/IEC to advance deployment and adoption of the technology.
- Researching Identity Verification, fraud management, and Attribute Validation technology to set the foundation for future guidelines and standards engagement.
- Developing Zero Trust reference implementations to advance critical national cybersecurity priorities.

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?

In conjunction with feedback from our 2020 Call for Comments, NIST focused on a few core "design principles" to drive our updated requirements and considerations:

- **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.**

OUR WORLD HAS CHANGED IN PROFOUND WAYS SINCE 2017; IT IS TIME FOR OUR GUIDANCE TO CHANGE TOO…

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

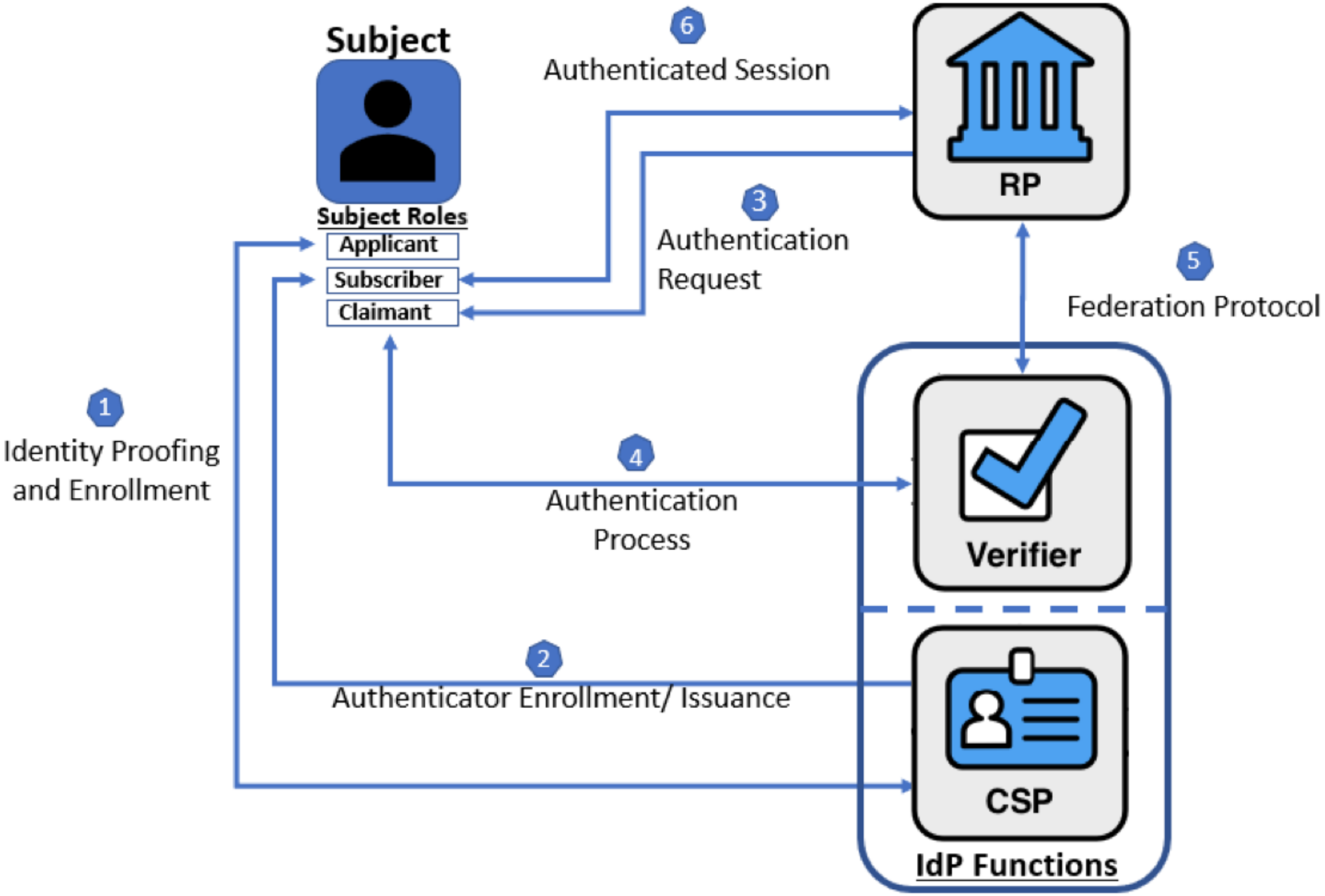
- There will still be emphasis on balancing risks to each of these critical components of identity and solution delivery and volumes continue to include specific requirements and considerations…we’ve just taken things one step further to consider equitable access!

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

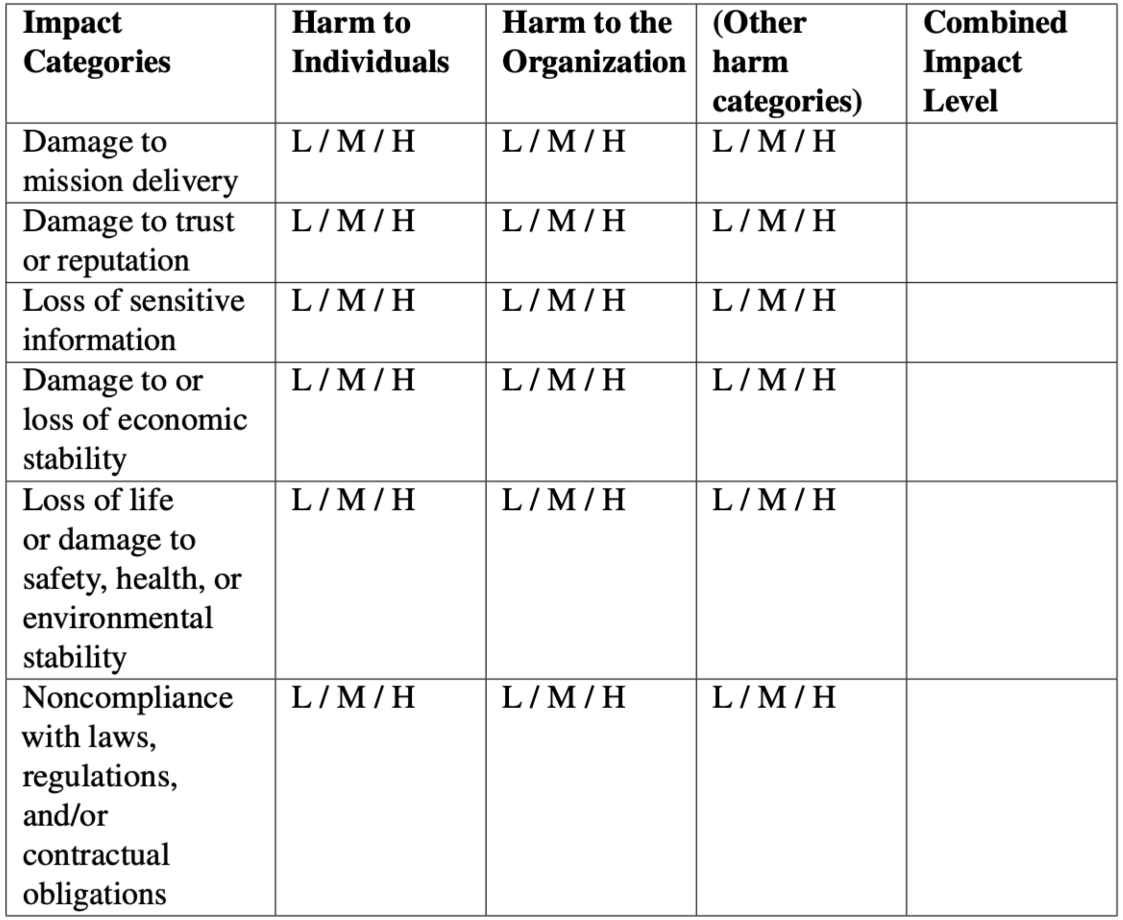
- **Introduces and describes foundational concepts, roles, and responsibilities referenced throughout all volumes, framed within the context of a digital identity model.**
- Provides a risk assessment methodology and a risk-based process of selecting assurance levels for identity proofing, authentication,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



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.

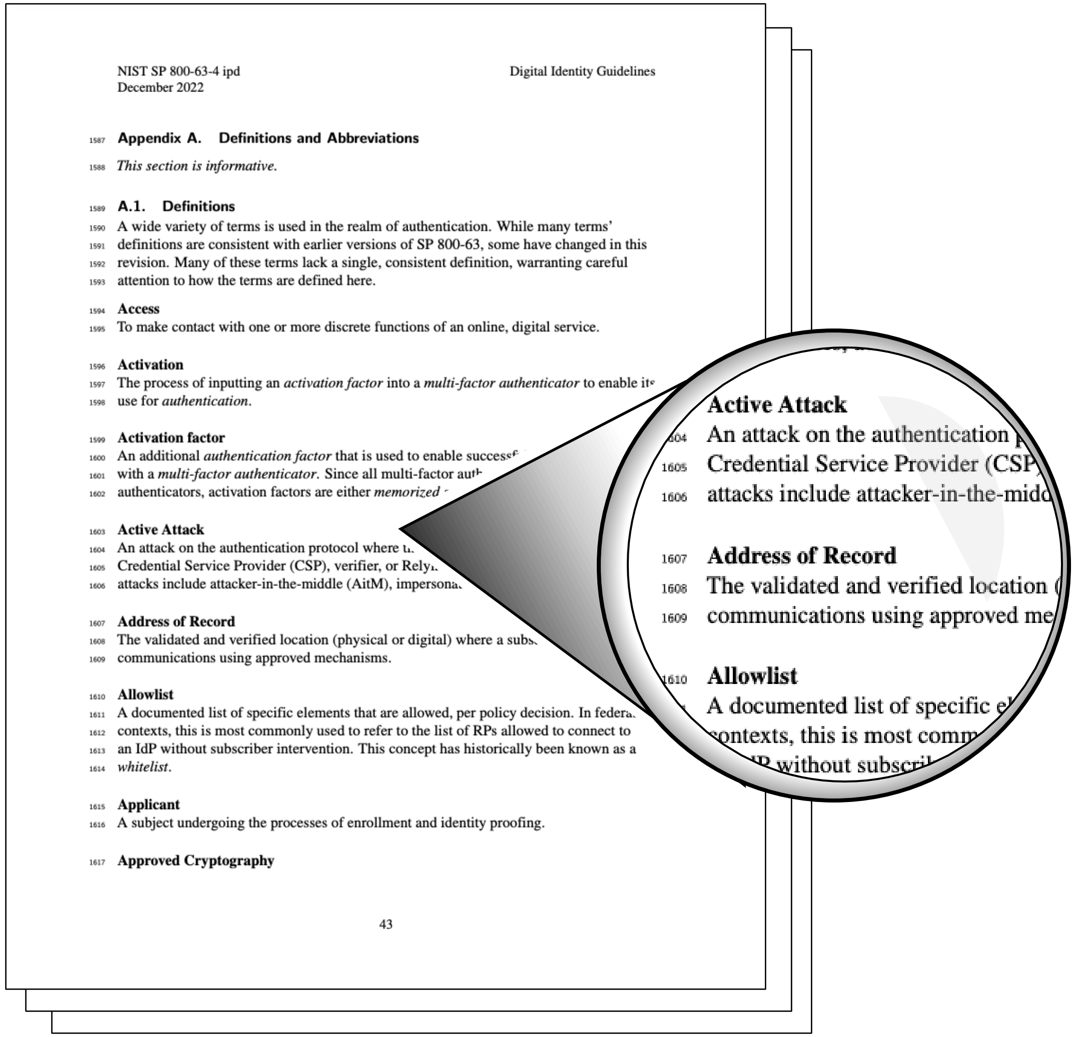
Table 1. Impact Categories



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 or reputation	L / M / H	L / M / H	L / M / H	
Loss of sensitive information	L / M / H	L / M / H	L / M / H	
Damage to or loss of economic stability	L / M / H	L / M / H	L / M / H	
Loss of life or damage to safety, health, or environmental stability	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	

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.**



NIST SP 800-63-4 ipd
December 2022

Digital Identity Guidelines

Appendix A. Definitions and Abbreviations

This section is informative.

A.1. Definitions

A wide variety of terms is used in the realm of authentication. While many terms' definitions are consistent with earlier versions of SP 800-63, some have changed in this revision. Many of these terms lack a single, consistent definition, warranting careful attention to how the terms are defined here.

Access
To make contact with one or more discrete functions of an online, digital service.

Activation
The process of inputting an *activation factor* into a *multi-factor authenticator* to enable its use for *authentication*.

Activation factor
An additional *authentication factor* that is used to enable successf
with a *multi-factor authenticator*. Since all multi-factor auth
authenticators, activation factors are either *memorized*

Active Attack
An attack on the authentication protocol where th
Credential Service Provider (CSP), verifier, or Relyi
attacks include attacker-in-the-middle (AitM), imperson

Address of Record
The validated and verified location (physical or digital) where a subs
communications using approved mechanisms.

Allowlist
A documented list of specific elements that are allowed, per policy decision. In federa
contexts, this is most commonly used to refer to the list of RPs allowed to connect to an IdP without subscriber intervention. This concept has historically been known as a *whitelist*.

Applicant
A subject undergoing the processes of enrollment and identity proofing.

Approved Cryptography

43

Active Attack
An attack on the authentication p
Credential Service Provider (CSP)
attacks include attacker-in-the-midd

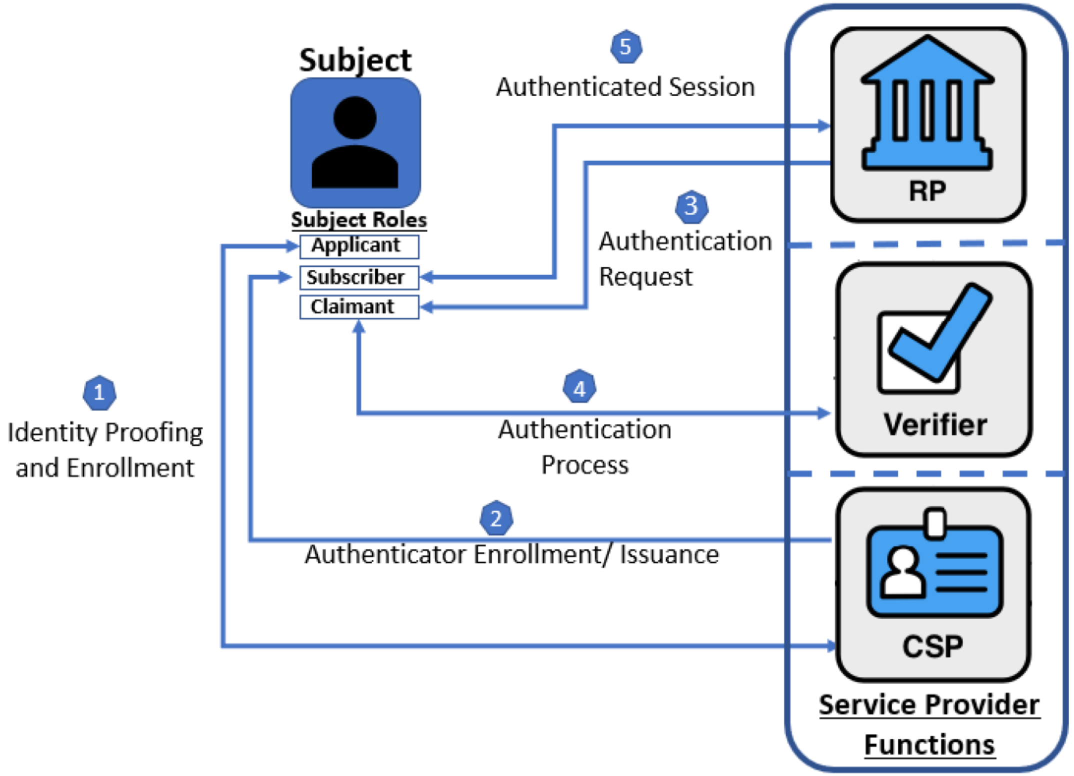
Address of Record
The validated and verified location (
communications using approved me

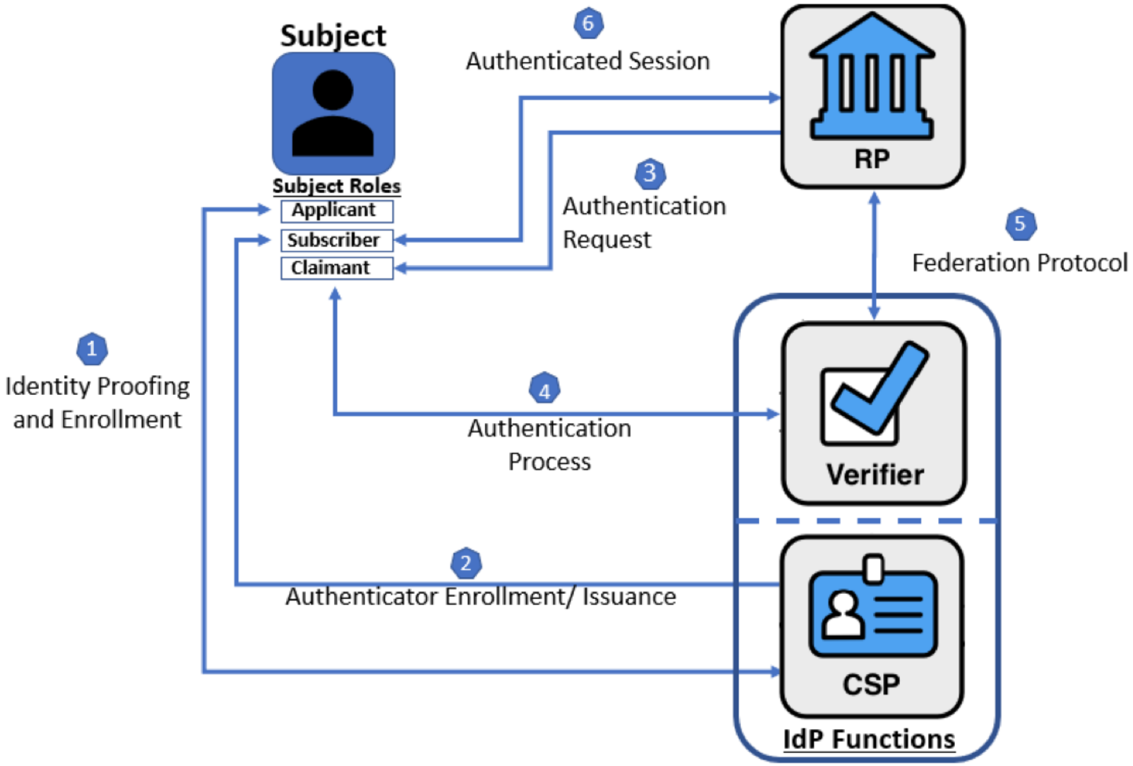
Allowlist
A documented list of specific el
contexts, this is most comm
IdP without subscri

Key Changes – 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.





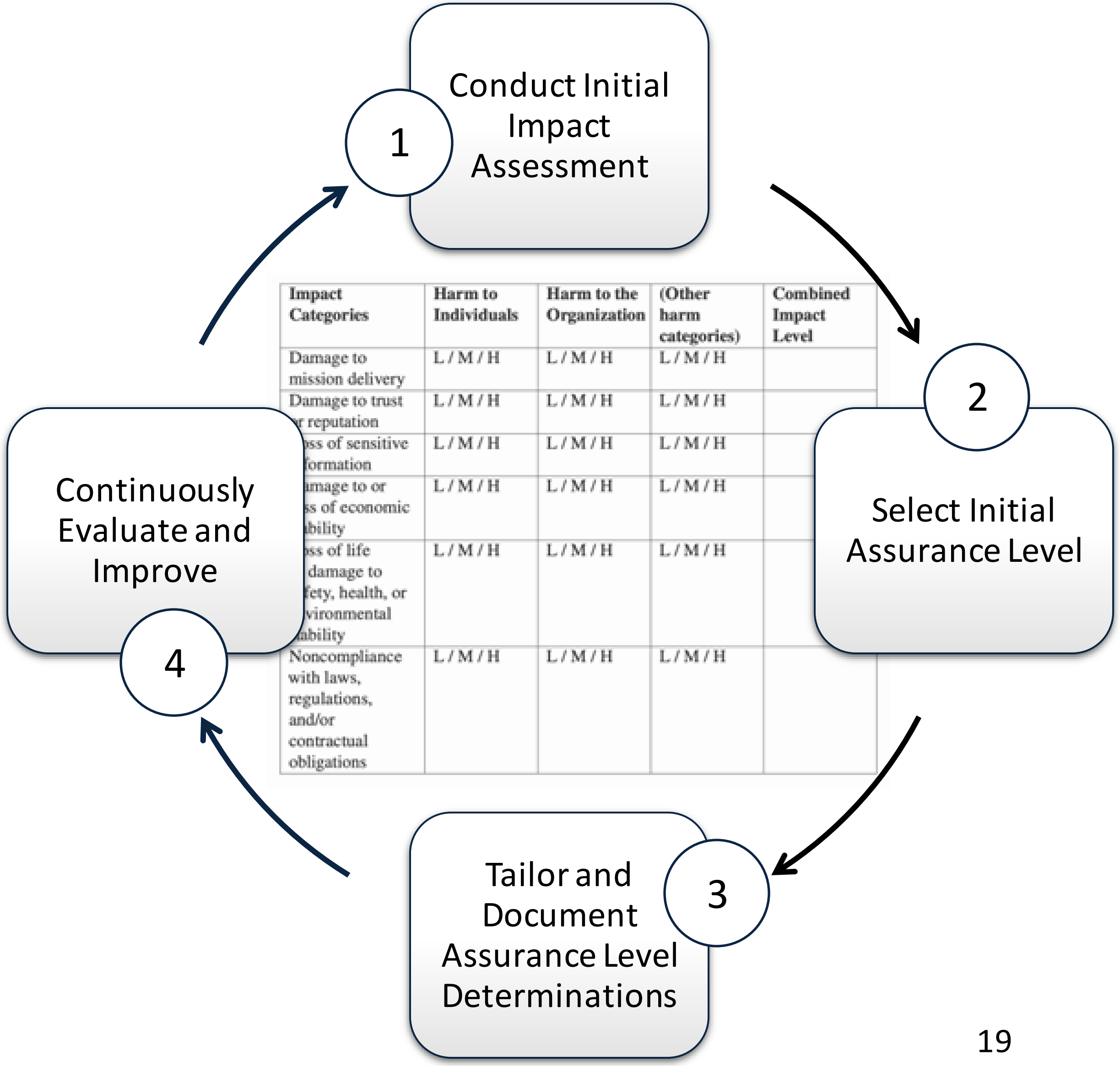
Key Changes – 800-63 Base Volume

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.


1
Conduct Initial Impact Assessment
2
Select Initial Assurance Level
3
Tailor and Document Assurance Level Determinations
4
Continuously Evaluate and Improve

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 ability	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	

Key Questions – 800-63 Base Volume

Risk Management:

- What additional guidance or direction can be provided to integrate digital identity risk with enterprise risk management?
- How might equity, privacy, and usability impacts be integrated into the assurance level selection process and digital identity risk management model?
- How might risk analytics and fraud mitigation techniques be integrated into the selection of different identity assurance levels? How can we qualify or quantify their ability to mitigate overall identity risk?

Across All Volumes:

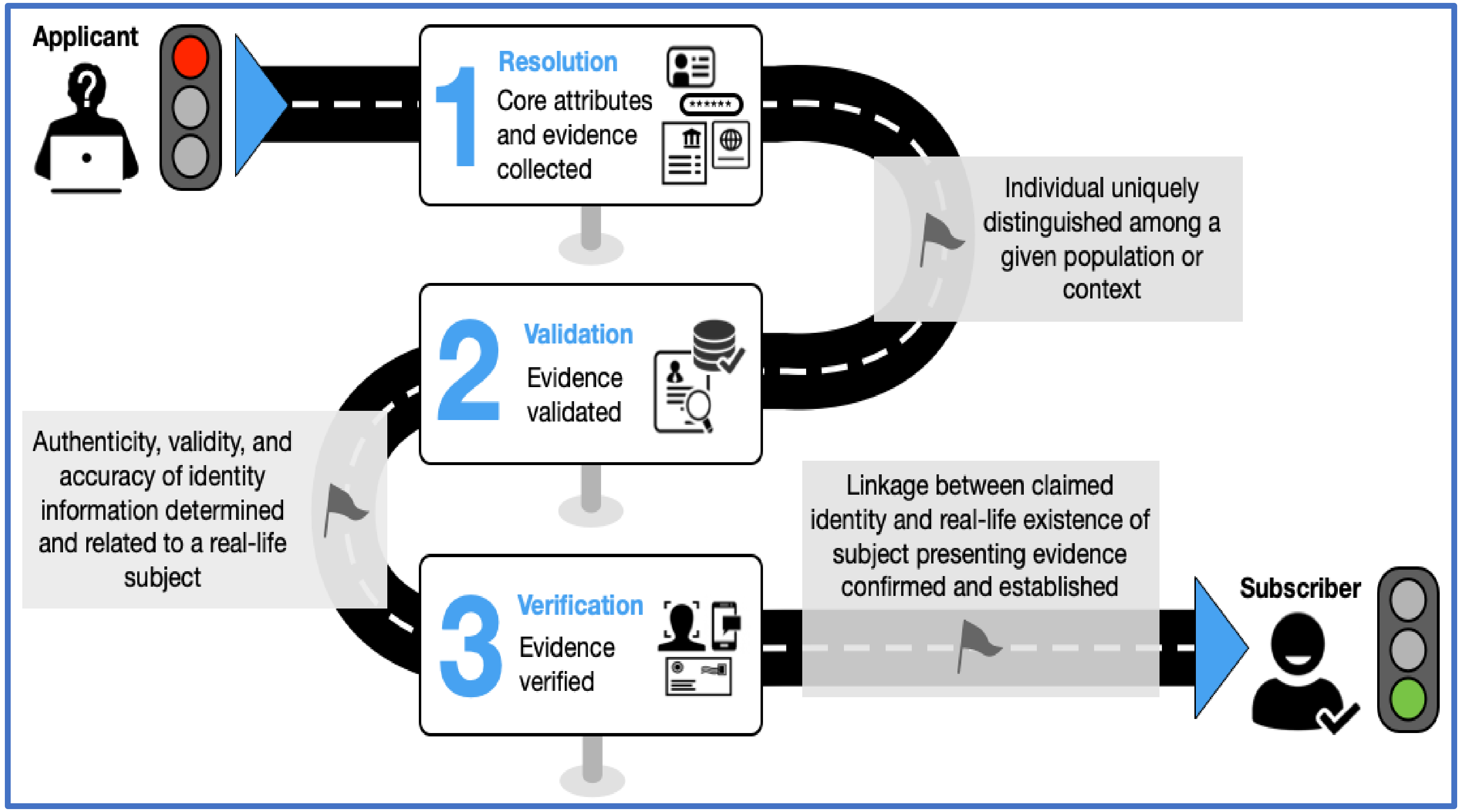
- Does the guidance sufficiently address privacy and equity?
- What equity assessment methods, impact evaluation models, or metrics could we reference to better support organizations in preventing or detecting disparate impacts that could arise as a result of identity verification technologies or processes?
- What specific implementation guidance, reference architectures, metrics, or other supporting resources may enable more rapid adoption and implementation of Revision 4 and future iterations of the Digital Identity Guidelines?
- What applied research and measurement efforts would provide the greatest impact on the identity market and advancement of these guidelines?

NIST SP 800-63A: Enrollment and Identity Proofing

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

Volume Overview – 800-63 A

- Provides requirements and guidance for the key responsibilities of the Identity Service CSP for the identity proofing and enrollment of applicants in the CSP Identity Service.
- Provides identity proofing requirements for the 3 core process steps – identity resolution, identity validation, identity verification -- at each assurance level.
- Additional flexibility in remote identity proofing processes for individuals and CSPs.



Applicant
1 Resolution
Core attributes and evidence collected
Individual uniquely distinguished among a given population or context
2 Validation
Evidence validated
Authenticity, validity, and accuracy of identity information determined and related to a real-life subject
3 Verification
Evidence verified
Linkage between claimed identity and real-life existence of subject presenting evidence confirmed and established
Subscriber

Expanded Controls for all IALs

- **CSP Identity Service documentation**
    - Content requirements – complete service description, core attributes, identity evidence, processes for addressing identity proofing errors, processes for addressing fraudulent accounts, policy/practices for conducting privacy risk assessments and identity proofing equity assessments.
- **CSP Identity Service privacy risk assessment**
    - Performance and documentation of privacy risk assessments and associated mitigations for all PII processed (collected, used, retained, disclosed) from CSP Identity Service identity proofing processes.
- **CSP Identity Service assessment of risks to equitable treatment (all xAL)**
    - Assess Identity Service to identify any processes and technologies that could result in inequitable access, treatment, or outcomes for individuals or communities.
    - Aligned to EO 13985.
    - Document results of Identity Service risk assessments for potential inequitable treatment and steps to mitigate such risks.
- **Automated attack prevention**
    - Controls to prevent automated attacks on the identity proofing process.
    - Includes bot detection and mitigation, behavioral analytics; web application firewall settings; traffic analysis.

Controls for use of biometrics

- **Biometrics use, notice, and consent**
  - Publicly available notice for biometrics collection, use, retention, and deletion.
  - CSP must obtain consent before biometrics collection and use.
- **Biometrics retention and deletion**
  - Privacy risk assessment for all biometric information processed and retained.
  - If retained, documented retention period and deletion process.
  - Capability for subscribers to request deletion of biometric information.
- **Biometric performance testing**
  - Biometric algorithm testing by independent entity.
  - Assess biometric system performance across similar environmental and user base of operational conditions.
- **Biometrics performance metrics for identity proofing**
  - FMR: 1:10,000 or better; FNMR: 1:100.
- **Liveness detection capability for remote biometrics collection**

New IAL1

- **New IAL1 identity proofing process for lower assurance applications and increased flexibility.**
  - Current IAL1 provides no identity proofing, attributes are self-asserted and unvalidated.
  - New IAL1 provides range of acceptable techniques to detect potential fraudulent identities.
- **Maintains 3-step identity proofing process**
  - Identity resolution and evidence collection.
  - Evidence and attribute validation.
  - Verification of evidence and attribute to identity proofing applicant.

Requirement	IAL1
Presence	Remote or In-person
Resolution	Minimum attributes to accomplish resolution
Evidence	1 piece of SUPERIOR or 1 piece of STRONG plus 1 piece of FAIR
Validation	Evidence validated for genuineness, accuracy, and currency. All core attributes validated by authoritative or credible sources
Verification	Return of an enrollment code or demonstrated access to a digital account at AAL1/FAL1
Biometric Collection	Optional

Expanded Guidance for Identity Evidence

- **Digital identity evidence may be used for identity proofing at all IAL**
  - Physical evidence is documentary evidence presented for identity proofing, I.e., passport, driver's license.
  - Digital evidence may be a digital representation of physical evidence, a digital account, or other verifiable digital credential (e.g., mDL, PIV, verifiable credentials).
- **Expanded guidance for the characteristics of both physical and digital identity evidence**
  - Evidence characteristics are used to determine the acceptability of evidence and information presented during identity proofing processes.
- **Identity evidence strength qualities for UNACCEPTABLE and WEAK strength removed**
- **Digital identity evidence strength determined by same strength qualities as physical evidence**
- **New guidance for SUPERIOR evidence**
  - SUPERIOR evidence is evidence that is digitally signed by the issuing authority of the evidence.
  - SUPERIOR evidence is validated by verifying the digital signature of the evidence or data objects using the public key of the issuing authority.
  - Verifying the digital signature of SUPERIOR evidence provides assurance of the integrity and genuineness of the evidence and does not need any further validation from the issuing source.

Expanded Scope for Identity Attributes

- **Core attributes**
  - Core attributes are determined by the CSP.
  - Represent the subset of identity attributes needed by the CSP for identity resolution and identity proofing.
  - All core attributes must be validated for all IALs.
- **Attribute collection**
  - No change for data minimization requirement for attribute collection.
  - Attributes may be collected from presented identity evidence or through applicant self-assertion.

Expanded Scope for evidence and attribute validation

Authoritative Source	Credible Source
The issuing authority for the evidence or attribute or an entity that has direct linkage to the evidence or attribute information of an issuing source.	• **Has access to attribute information that was validated through an identity proofing process, or** • **Has access to attribute information that can be traced to an authoritative source, or** • **Maintains identity attribute information obtained from multiple sources that is checked for data correlation for accuracy, consistency, and currency.**

Trusted Referees and Applicant References

Use of Trusted Referees and Applicant References is intended to allow options to Applicants who otherwise would have difficulty meeting identity proofing requirements based on their circumstances.

Trusted Referees	Applicant References
Offering the use of Trusted Referees is required for CSP.	Use of applicant references is recommended but not required.
Acts as an agent of the CSP	NOT an agent of the CSP, has knowledge of applicant's identity and circumstances.
Trained to make risk-based decisions on applicant's identity, evidence and circumstances	Has knowledge of applicant's identity and circumstances and can provide documentation or vouch for applicant's identity, evidence and circumstances.
Is known, trained, and vetted by the CSP	Identity proofed at IAL of the applicant or higher.
Can be used in combination with or separate from the use of applicant references.	Intended to be used in combination with CSP trusted referee
	Use of Applicant References beyond identity proofing processes is outside the scope of SP 800-63.

Subscriber Accounts

- **Established by CSP for all Identity Service subscribers for all IAL**
  - Remains active through the subscriber’s lifecycle.
- **Subscriber account content:**
  - Unique identifier
  - Record of Identity proofing steps
  - IAL
  - Record of all authenticators registered to the subscriber
  - Subscriber consent provided for use of PII/attributes maintained in account
  - Validated attributes
- **Privacy risk assessment**
  - Privacy risk assessment required for PII maintained in subscriber accounts.
- **Subscriber access**
  - Subscriber MFA to access account.
  - CSP must provide capability for subscribers to **change/update/delete information in subscriber accounts**.

Targeted Issues for Comment/Feedback

- NIST sees a need for inclusion of an unattended, fully remote Identity Assurance Level (IAL) 2 identity proofing workflow that provides security and convenience but does not require face recognition. Accordingly, NIST seeks input on the following questions:

  - What technologies or methods can be applied to develop a remote, unattended IAL2 identity proofing process that demonstrably mitigates the same risks as the current IAL2 process?

  - Are these technologies supported by existing or emerging technical standards?

  - Do these technologies have established metrics and testing methodologies to allow for assessment of performance and understanding of impacts across user populations (e.g., bias in artificial intelligence)?

- What methods exist for integrating digital evidence (e.g., Mobile Driver's Licenses, Verifiable Credentials) into identity proofing at various identity assurance levels?

Targeted Issues for Comment/Feedback

- What are the impacts, benefits, and risks of specifying a set of requirements for CSPs to establish and maintain fraud detection, response, and notification capabilities?
  - Are there existing fraud checks (e.g., date of death) or fraud prevention techniques (e.g., device fingerprinting) that should be incorporated as baseline normative requirements? If so, at what assurance levels could these be applied?
  - How might emerging methods such as fraud analytics and risk scoring be further researched, standardized, measured, and integrated into the guidance in the future?
  - What accompanying privacy and equity considerations should be addressed alongside these methods?
- Are current testing programs for liveness detection and presentation attack detection sufficient for evaluating the performance of implementations and technologies?
- What impacts would the proposed biometric performance requirements for identity proofing have on real-world implementations of biometric technologies?

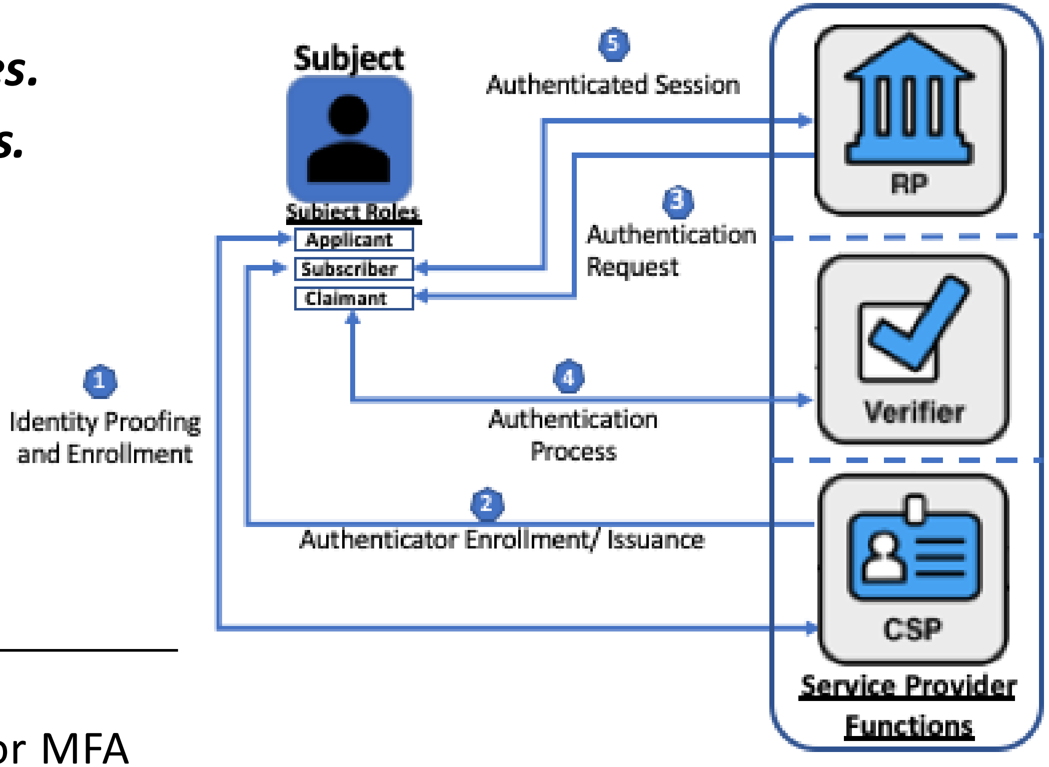
NIST SP 800-63B: Authentication and Lifecycle Management

Andrew Regenscheid, PIV Technical Lead, Computer Security Division

SP 800-63B Overview

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 – 800-63B Authentication

Concepts

- ***Phishing Resistance:*** expansion of verifier impersonation resistance.

Authenticator Guidelines

- ***Activation Secrets:*** for unlocking multifactor authenticators.
- ***Password Guidelines:*** strengthening previous recommendations.
- ***Out of Band:*** removed user comparison flow.
- ***Wireless Authenticators:*** wireless (e.g., Bluetooth, NFC) connections.
- ***Biometrics:*** updated biometric performance requirements and metrics.

Account and Lifecycle Management

- ***Account Recovery:*** provisions for subscribers without access to multiple authenticators.
- ***Authenticator Binding:*** new external binding flow.
- ***Equity Considerations:*** guidance for addressing equity impacts.

Phishing Resistance

Phishing attacks on authentication

- Trick users into revealing authenticators to an attacker.
- Steal static authenticators, e.g., passwords.
- Relay dynamic authenticators, e.g., OTP.

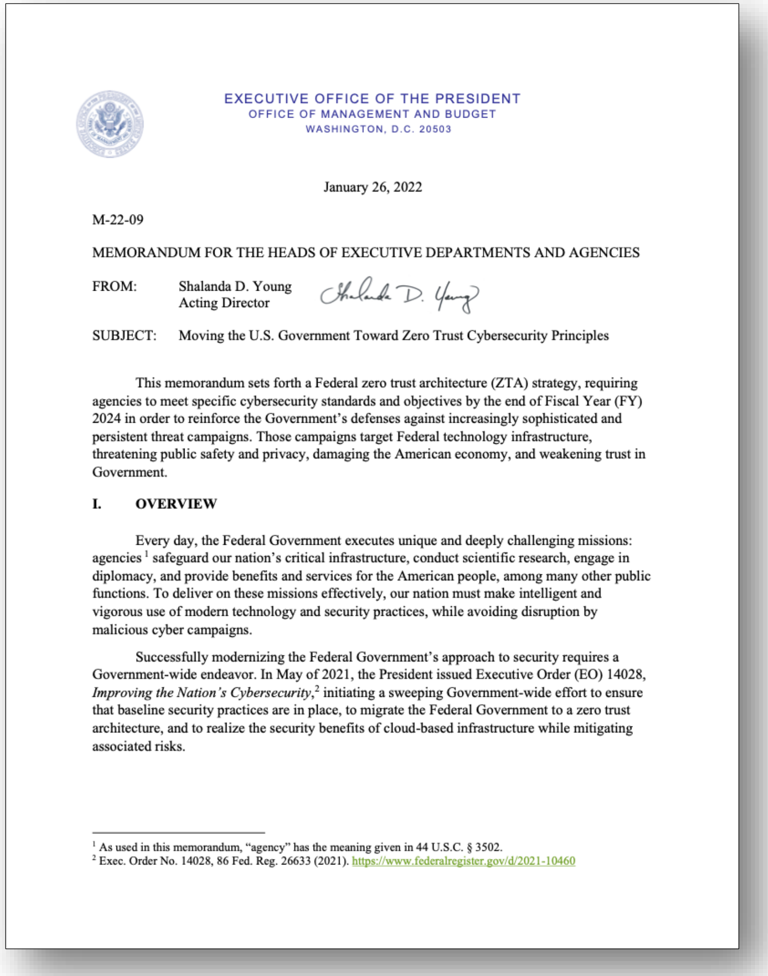
Phishing-resistant authentication methods

- ***Channel Binding***
  - Equivalent to *verifier impersonation resistance* in SP 800-63-3.
  - Binding authenticators to communications channel.
  - ***Example:*** Client-authenticated TLS.
- ***Verifier Name Binding***
  - Binding authenticators to domain name.
  - ***Example:*** WebAuthn/FIDO.

Phishing resistance **required** at AAL3, **recommended** at AAL2

OMB M-22-09 further requires federal agencies to offer a phishing-resistant authenticator option to public users →

OMB Memorandum M-22-09



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

January 26, 2022

M-22-09

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director
Shalanda D. Young

SUBJECT: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

This memorandum sets forth a Federal zero trust architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 in order to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns. Those campaigns target Federal technology infrastructure, threatening public safety and privacy, damaging the American economy, and weakening trust in Government.

I. OVERVIEW

Every day, the Federal Government executes unique and deeply challenging missions: agencies [1] safeguard our nation's critical infrastructure, conduct scientific research, engage in diplomacy, and provide benefits and services for the American people, among many other public functions. To deliver on these missions effectively, our nation must make intelligent and vigorous use of modern technology and security practices, while avoiding disruption by malicious cyber campaigns.

Successfully modernizing the Federal Government's approach to security requires a Government-wide endeavor. In May of 2021, the President issued Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*,[2] initiating a sweeping Government-wide effort to ensure that baseline security practices are in place, to migrate the Federal Government to a zero trust architecture, and to realize the security benefits of cloud-based infrastructure while mitigating associated risks.

[1] As used in this memorandum, "agency" has the meaning given in 44 U.S.C. § 3502.
[2] Exec. Order No. 14028, 86 Fed. Reg. 26633 (2021). https://www.federalregister.gov/d/2021-10460

Password/PIN Guidelines

- PINs/passwords used as local authenticator activation factors split apart from remotely-verified memorized secrets.
- **Activation Secrets:**
  - >= 6 characters in length.
  - 10 guess retry counter.
  - Blocklist of >10 common-used values.
- **Memorized Secrets/Passwords –** core requirements remain:
  - >= 8 characters in length.
  - Blocklist against commonly used, expected or compromised passwords.
  - Limit the number of failed authentication attempts.
  - Store memorized secrets in a form resistant to offline attacks.
- **Strengthened some previous recommendations to requirements:**
  - Offer guidance to subscribers on choosing a memorized secret.
  - Allow use of password managers.
  - No composition or password complexity rules.
  - No periodic password changes.

SMS and PSTN for OOB Authentication

- SMS/PSTN Out-of-Band Authentication remains restricted. **Restricted Authenticators:**
  - Must offer at least one alternative – OMB M-22-09 specifies ***phishing resistant*** option.
  - Must address additional risks and provide notice to users.
  - Must develop a migration plan.
- SMS/PSTN OOB Threats:
  - Account hijacking/SIM swap.
  - Network/SS7 routing attacks.
  - Capture/relay attacks.

- SMS/PSTN remains commonly used for authentication, proofing, and recovery.
- NIST continuing to evaluate the threats and potential mitigations.
  - e.g., account tenure and SIM swap detection

Biometrics in Authentication

- Draft SP 800-63B continues to allow the use of biometrics as part of MFA with a physical authenticator.
  - Generally expected to be locally verified as an activation factor.
  - Central verification allowed when using verified biometric sensors/devices.
- Updated Performance Metric:
  - **False Match Rate** of 1 in 10,000.
  - Aligns with related industry standards.
- Presentation Attack Detection (PAD):
  - PAD capabilities continue to be recommended.
  - References ISO/IEC 30107-3 for testing.
  - NIST is interested in the availability of test methods, certification programs, and authenticator products that address PAD.

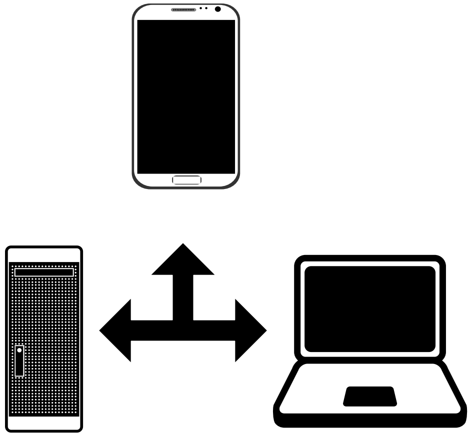
Cryptographic Authenticators

- Cryptographic authenticators historically used unique, device-specific keys.

  Existing SP 800-63-3 Volume B Language:

  - *AAL2: "… SHALL NOT facilitate the cloning of the secret key onto multiple devices."*
  - *AAL3: "… use tamper-resistant hardware to encapsulate one or more secret keys unique to the authenticator"*

- New specifications and implementations challenging that paradigm.
  - ***Example:*** Backup-eligible WebAuthn credentials, i.e., passkeys



- Draft SP 800-63B-4:
  - Removes vague AAL2 language prohibiting facilitation of cloning.
  - Maintains non-exportable, hardware-protected keys at AAL3.
- NIST evaluating implications and seeking input across two use cases:
  - Syncable authenticators: Synced to devices belonging to same user.
  - Shareable authenticators: Facilitated sharing between users.

Account/Lifecycle Management

- **Session Management**
  - Reauthentication baselines remain per existing SP 800-63B-3 guidelines:
    - *AAL1:* 30 days.
    - *AAL2:* 12 hours, or 30 minutes inactivity.
    - *AAL3:* 12 hours, or after 15 minutes inactivity.
  - Real-world implementations will be driven by use case and mission needs.
  - NIST interested in feedback on these guidelines.
- **New Binding Flow: External Authenticator Binding**
  - ***Intended Use Case:*** Binding platform-based authenticators whose devices cannot directly use an existing authenticator.
    - e.g., Binding PIV credentials on mobile devices using an existing PIV card.
  - Process must mitigate phishing and relay threats.
- **Equity Considerations**
  - Potential for disparate impacts based on ***authenticator selection.***
  - ***Account recovery*** processes.

Targeted Issues for Comment/Feedback

- Are emerging authentication models and techniques – such as FIDO passkeys, Verifiable Credentials, and mobile driver's licenses – sufficiently addressed and accommodated, as appropriate, by the guidelines? What are the potential associated security, privacy, and usability benefits and risks?

- Are the controls for phishing resistance as defined in the guidelines for AAL2 and AAL3 authentication clear and sufficient?

- How are session management thresholds and reauthentication requirements implemented by agencies and organizations? Should NIST provide thresholds or leave session lengths to agencies based on applications, users, and mission needs?

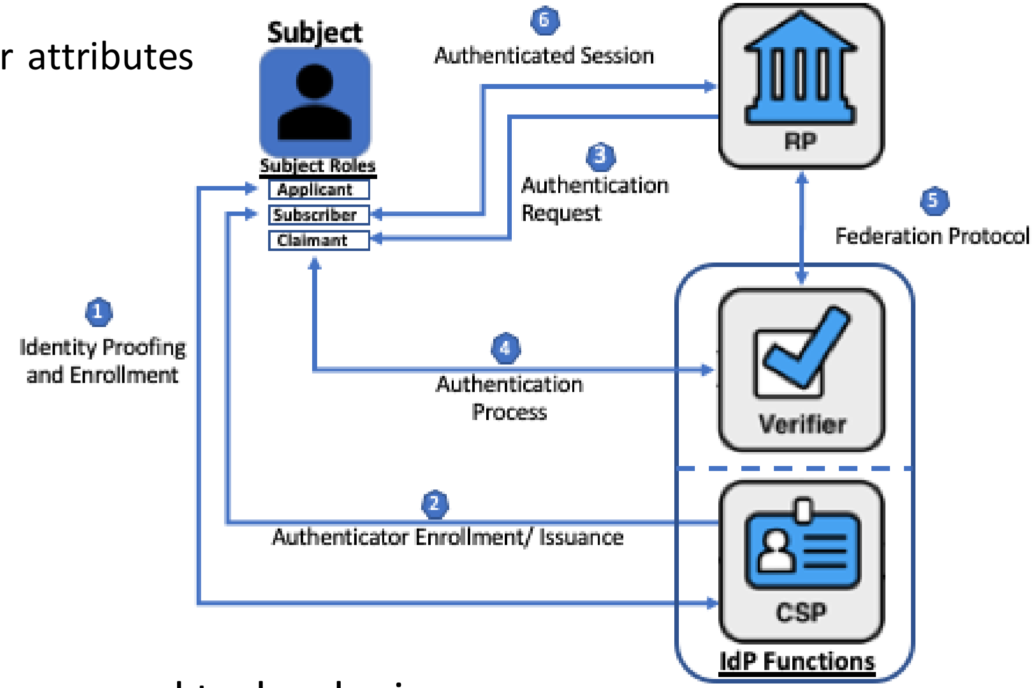
NIST SP 800-63C: Federation and Assertions

Andrew Regenscheid, PIV Technical Lead, Computer Security Division

SP 800-63C Overview

Scope: Federation and Assertions

- **Federation –** conveyance of authentication information and subscriber attributes across networked systems:
  - Between organizations.
  - Within an enterprise for Single Sign-on (SSO).
- **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 – 800-63C Federation and Assertions

- **Redefined FALs**
- **Bound Authenticators**
  - Guidance and requirements for the use of bound authenticators to bind subscribers to federated assertion transactions for high assurance federation use cases (FAL3).
- **Federation Trust Agreements**
  - Expanded guidance and requirements for federation trust agreements to address IdP and RP responsibilities.
  - Federation trust agreement requirements for processes for federated transactions, attribute collection and disclosure, and attribute and transaction protections.
- **Provisioning & Identity APIs**
  - Guidance and requirements for use of attribute and provisioning APIs.
  - Privacy requirements for IdPs and RPs use of attribute and provisioning APIs.
- **RP Subscriber Accounts**
  - Guidance and requirements for RP subscriber account establishment and maintenance for subscriber information, attributes, and consent agreements.
- **Equity Considerations for Federation Transactions and Processes**

Federation Assurance Levels

FAL	Trust Agreement	Registration	Injection Protection	Presentation
1	Dynamic or Static	Dynamic or Static	Recommended	Bearer Assertion
2	Static	Dynamic or Static	Required	Bearer Assertion
3	Static	Static	Required	Assertion and Bound Authenticator

Trust Agreements

The policy/procedures/responsibilities that describe the relationship between IdPs and RPs in a federation.

Updates

- Expanded trust agreement guidance addresses IdP and RP responsibilities:
  - Processes for federated transactions.
  - Attribute collection and disclosure.
  - Attribute and transaction protections.
- Dynamic establishment of trust agreement allowed at FAL1.
- Static establishment of trust agreement required at FAL2/FAL3.

Discovery and Registration

Establishment of cryptographic keys, access rights, and other information to allow IdPs and RPs to communicate securely.

Updates

- Dynamic registration allowed at FAL1/FAL2.
- Static registration required at FAL3.

Assertion Presentation

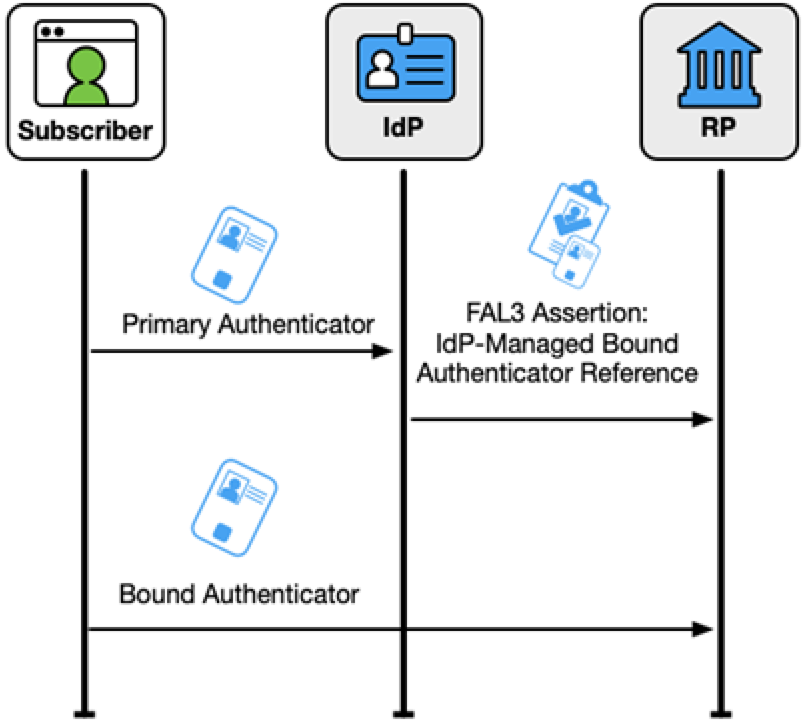
- **FAL1:** Bearer Assertions
  - **Objective:** Provide basic protections that support broad use cases and technologies.
  - Time-bound, audience-restricted assertions.
  - Signed by the IdP.
  - Issuer, signature, time window, and audience validated by RP upon receipt.

- **FAL2:** Injection-Protected Bearer Assertions
  - **Objective:** Protect RPs from assertion injection.
  - ***Assertion Injection:*** an attacker presenting an assertion outside a current federation request.
  - Recommends use of back-channel assertion presentation.

- **FAL3:** Proof of Possession of a Bound Authenticator
  - **Objective:** Provide very strong assurance the party presenting an assertion to the RP is the identified subscriber.
  - 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

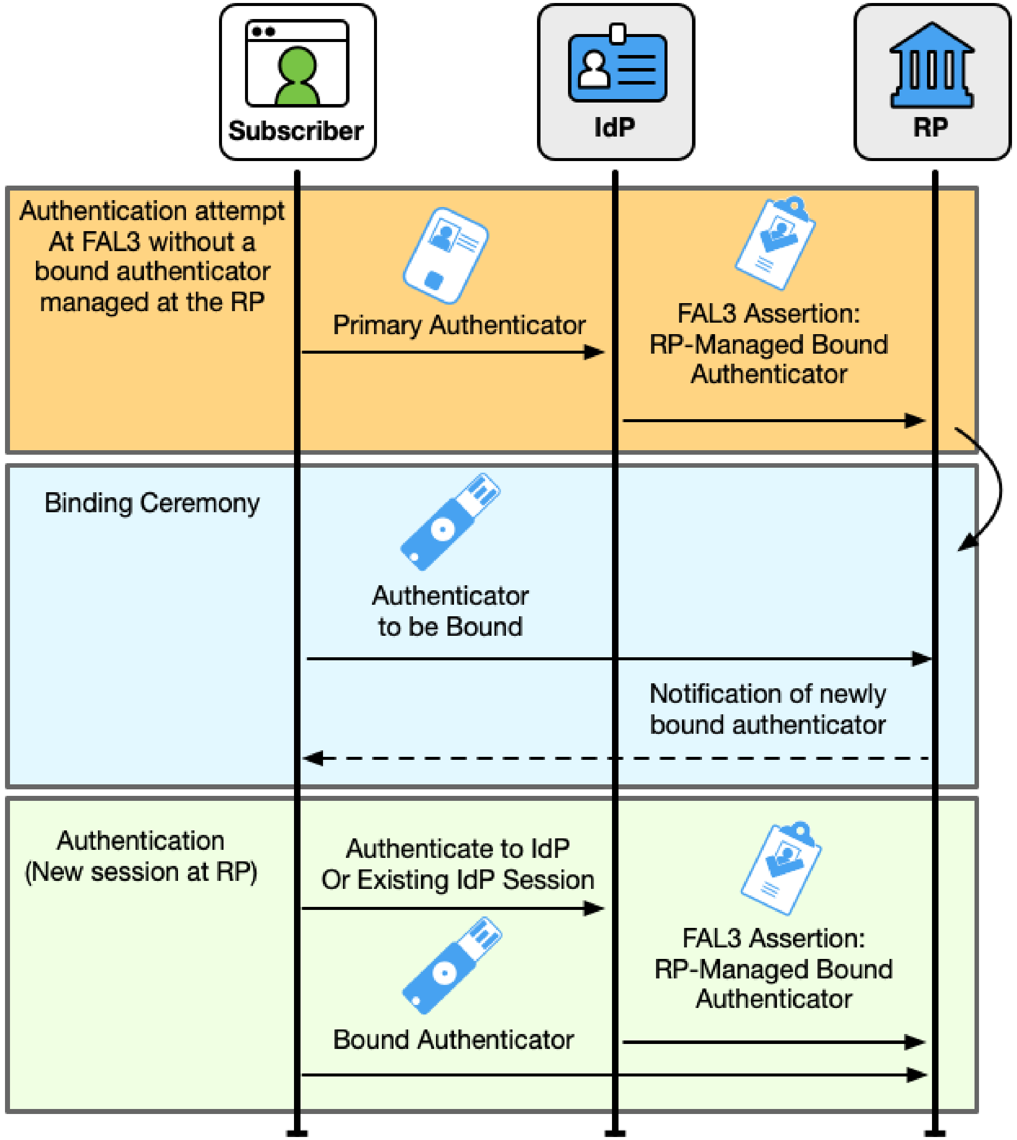
- IdP issues and manages an authenticator bound to the subscriber’s account.
- ***Authentication Process:***
    - Subscriber authentication to IdP using primary authenticator.
    - IdP assertion references identifier of bound authenticator.
    - RP verifies:
        - The contents of the assertion 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.
    - Phishing-resistant authentication process.



Similar to Holder-of-Key assertions described in SP 800-63-3.

Bound Authenticators – RP Managed

- RP binds an authenticator in the subscriber's 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 primary authenticator.
  - 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

Federation Lifecycle

- **Provisioning & Identity APIs**
  - Draft includes new guidance and requirements for use of attribute and provisioning APIs.
  - New privacy requirements for IdPs and RPs use of attribute and provisioning APIs.
- **RP Subscriber Accounts**
  - New guidance and requirements for RP subscriber account establishment and maintenance for subscriber information, attributes, and consent agreements.
- **Equity Considerations**

Targeted Issues for Comment/Feedback

- What additional privacy considerations (e.g., revocation of consent, limitations of use) may be required to account for the use of identity and provisioning APIs that had not previously been discussed in the guidelines?

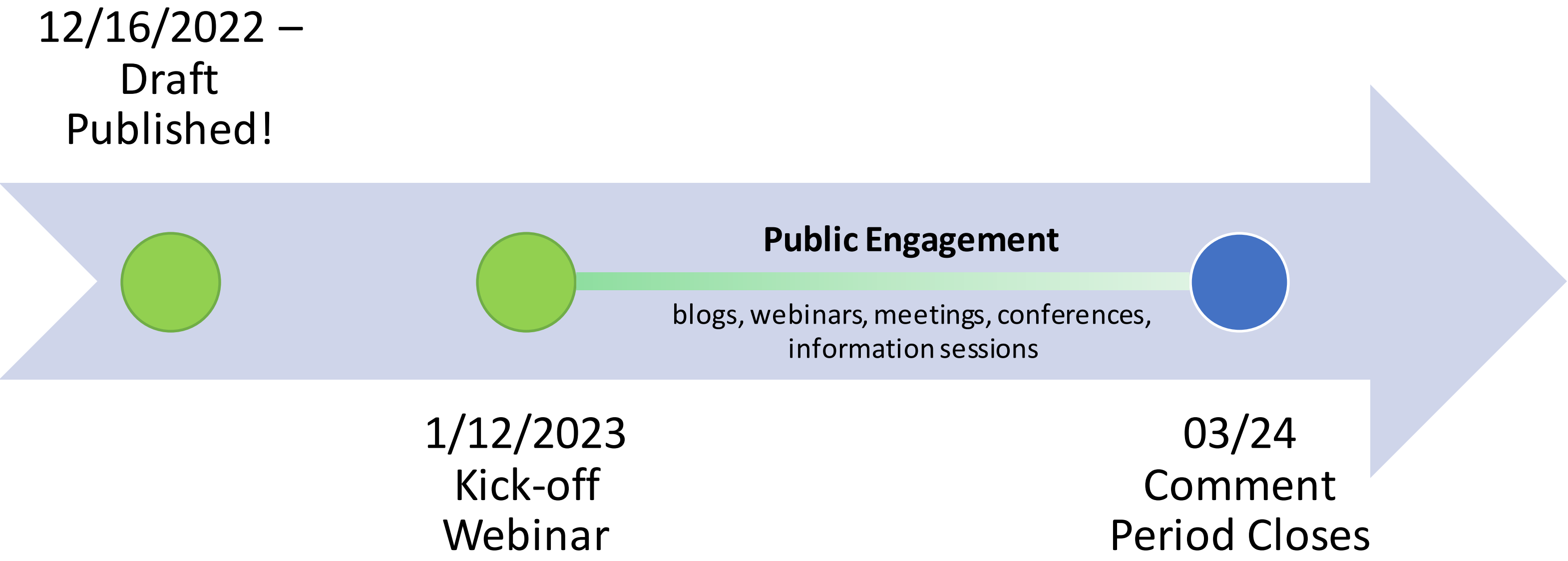
- Is the updated text and introduction of “bound authenticators” sufficiently clear to allow for practical implementations of federation assurance level (FAL) 3 transactions? What complications or challenges are anticipated based on the updated guidance?

Key Dates and Next Steps

Ryan Galluzzo, Digital Identity Program Lead, Applied Cybersecurity Division

Key Dates

The release of the draft on 12/16 kicked off a 90 day comment period to collect feedback and conduct engagement with the public, government, and industry.



12/16/2022 – Draft Published!

Public Engagement

blogs, webinars, meetings, conferences, information sessions

1/12/2023 Kick-off Webinar

03/24 Comment Period Closes

What happens during the public comment period?

- Active Engagement & Outreach
- Continued Research
- Management & Triage of Comments

What happens after the comment period?

- *End of comment period does not mean "end of discussion"*
- Review and adjudication of comments
- Engagement to clarify or elaborate
- Additional research on input
- Determination on path – final or another draft

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/

In Other News!

NIST Releases Two Draft Guidelines on Personal Identity Verification (PIV) Credentials!

- NIST is announcing the initial public drafts of NIST SP 800-157r1 (Revision 1), *Guidelines for Derived Personal Identity Verification (PIV) Credentials*, and NIST SP 800-217,*Guidelines for Personal Identity Verification (PIV) Federation*.
- These two SPs complement Federal Information Processing Standard (FIPS) 201-3, which defines the requirements and characteristics of government-wide interoperable identity credentials used by federal employees and contractors.
- **Submit public comments no later than 11:59 PM ET on March 24, 2023!**

NIST Cybersecurity Framework 2.0

- Journey to the NIST CSF 2.0 Workshop #2: February 15, 2023
- Check back HERE to read the CSF Concept Paper (forthcoming) in advance of the event