NIST Special Publication 800-63A

Digital Identity Guidelines

Enrollment and Identity Proofing

Paul A. Grassi
James L. Fenton

Privacy Authors:
Naomi B. Lefkovitz
Jamie M. Danker

Usability Authors:
Yee-Yin Choong
Kristen K. Greene
Mary F. Theofanos

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

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-63A

Digital Identity Guidelines

Enrollment and Identity Proofing

Paul A. Grassi
Applied Cybersecurity Division
Information Technology Laboratory

James L. Fenton
Altmode Networks
Los Altos, Calif.

Privacy Authors:
Naomi B. Lefkovitz
Applied Cybersecurity Division
Information Technology Laboratory

Jamie M. Danker
National Protection and Programs Directorate
Department of Homeland Security

Usability Authors:
Yee-Yin Choong
Kristen K. Greene
Information Access Division
Information Technology Laboratory

Mary F. Theofanos
Office of Data and Informatics
Material Measurement Laboratory

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

June 2017

U.S. Department of Commerce

Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq*., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-63A
Natl. Inst. Stand. Technol. Spec. Publ. 800-63A, 44 pages (June 2017)
CODEN: NSPUE2

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

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Comments on this publication may be submitted to dig-comments@nist.gov:

All comments are subject to release under the Freedom of Information Act (FOIA)

National Institute of Standards and Technology
Attn: Applied Cybsersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
Email: dig-comments@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

These guidelines provide technical requirements for federal agencies implementing digital identity services and are not intended to constrain the development or use of standards outside of this purpose. This guideline focuses on the enrollment and verification of an identity for use in digital authentication. Central to this is a process known as identity proofing in which an applicant provides evidence to a credential service provider (CSP) reliably identifying themselves, thereby allowing the CSP to assert that identification at a useful identity assurance level. This document defines technical requirements for each of three identity assurance levels. This publication supersedes corresponding sections of NIST Special Publication (SP) 800-63-2.

Keywords

authentication; credential service provider; electronic authentication; digital authentication; electronic credentials; digital credentials; identity proofing; federation.

Acknowledgments

The authors would like to acknowledge the contributions and guidance of our international peers, including Adam Cooper, Alastair Treharne, and Julian White from the Cabinet Office, United Kingdom, and Tim Bouma from the Treasury Board of Canada Secretariat, Government of Canada, Kaitlin Boeckl for her artistic contributions to all volumes in the SP 800-63 suite, and the contributions of our many reviewers, including Joni Brennan from the Digital ID & Authentication Council of Canada (DIACC), Ben Piccarreta and Ellen Nadeau from NIST, and Danna Gabel O'Rourke from Deloitte & Touche LLP. In addition, special thanks to the Federal Privacy Council's Digital Authentication Task Force for the contributions to the development of privacy requirements and considerations.

The authors would also like to acknowledge the thought leadership and innovation of the original authors: Donna F. Dodson, Elaine M. Newton, Ray A. Perlner, W. Timothy Polk, Sarbari Gupta, and Emad A. Nabbus. Without their tireless efforts, we would not

have had the incredible baseline from which to evolve 800-63 to the document it is today.

Requirements Notation and Conventions

The terms “SHALL” and “SHALL NOT” indicate requirements to be followed strictly in order to conform to the publication and from which no deviation is permitted

The terms “SHOULD” and “SHOULD NOT” indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited.

The terms “MAY” and “NEED NOT” indicate a course of action permissible within the limits of the publication.

The terms “CAN” and “CANNOT” indicate a possibility and capability, whether material, physical or causal or, in the negative, the absence of that possibility or capability.

Table of Contents

List of Figures

List of Tables

Errata

This table contains changes that have been incorporated into Special Publication 800-171. Errata updates can include corrections, clarifications, or other minor changes in the publication that are either editorial or substantive in nature.

Date	Type	Change	Page
	Editorial	Made minor grammatical edits throughout the document.	N/A
	Substantive	Added ‘approved’ before cryptographic in describing valid identity evidence	Table 5-1
	Editorial	Changed ‘Normative’ to ‘Informative’	Table 2-1
	Substantive	Changed to informative section	5
	Substantive	Updated the section to be normative	6

1 Purpose

This section is informative

This document provides requirements for enrollment and identity proofing of applicants that wish to gain access to resources at each Identity Assurance Level (IAL). The requirements detail the acceptability, validation, and verification of identity evidence that will be presented by a subscriber to support their claim of identity. This document also details the responsibilities of Credential Service Providers (CSPs) with respect to establishing and maintaining enrollment records and binding authenticators (either CSP-issued or subscriber-provided) to the enrollment record.

2 Introduction

This section is informative.

One of the challenges associated with digital identity is the association of a set of online activities with a single specific entity. While there are situations where this is not required or is even undesirable (e.g., use cases where anonymity or pseudonymity are required), there are others where it is important to reliably establish an association with a real-life subject. Examples include obtaining health care and executing financial transactions. There are also situations where the association is required for regulatory reasons (e.g., the financial industry's 'Know Your Customer' requirements, established in the implementation of the USA PATRIOT Act of 2001) or to establish accountability for high-risk actions (e.g., changing the release rate of water from a dam).

There are also instances where it is desirable for a relying party (RP) to know something about a subscriber executing a transaction, but not know their real-life identity. For example, it may be desirable to only know a subscriber's home ZIP code for purposes of census-taking or petitioning an elected official. In both instances, the ZIP code is sufficient to deliver the service; it is not necessary or desirable to know the underlying identity of the person.

The following table states which sections of this document are normative and which are informative:

Table 2-1 Normative and Informative Sections of SP 800-63A

Section Name	Normative/Informative
1. Purpose	Informative
2. Introduction	Informative
3. Definitions and Abbreviations	Informative
4. Identity Assurance Level Requirements	Normative
5. Identity Resolution, Validation, and Verification	Normative
6. Derived Credentials	Informative
7. Threats and Security Considerations	Informative
8. Privacy Considerations	Informative
9. Usability Considerations	Informative
10. References	Informative

2.1 Expected Outcomes of Identity Proofing

When a subject is identity proofed, the expected outcomes are:

- Resolve a claimed identity to a single, unique identity within the context of the population of users the CSP serves.
- Validate that all supplied evidence is correct and genuine (e.g., not counterfeit or misappropriated).

- Validate that the claimed identity exists in the real world.
- Verify that the claimed identity is associated with the real person supplying the identity evidence.

2.2 Identity Assurance Levels

Assurance in a subscriber's identity is described using one of three IALs:

IAL1: There is no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the subject's activities are self-asserted or should be treated as self-asserted (including attributes a CSP asserts to an RP). Self-asserted attributes are neither validated nor verified.

IAL2: Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. IAL2 introduces the need for either remote or physically-present identity proofing. Attributes could be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes. A CSP that supports IAL2 can support IAL1 transactions if the user consents.

IAL3: Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained CSP representative. As with IAL2, attributes could be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes. A CSP that supports IAL3 can support IAL1 and IAL2 identity attributes if the user consents.

At IAL2 and IAL3, pseudonymity in federated environments is enabled by limiting the number of attributes sent from the CSP to the RP, or the way they are presented. For example, if a RP needs a valid birthdate but no other personal details, the RP should leverage a CSP to request just the birthdate of the subscriber. Wherever possible, the RP should ask the CSP for an attribute reference. For example, if a RP needs to know if a claimant is older than 18 they should request a boolean value, not the entire birthdate, to evaluate age. Conversely, it may be beneficial to the user that uses a high assurance CSP for transactions at lower assurance levels. For example, a user may maintain an IAL3 identity, yet should be able to use their CSP for IAL2 and IAL1 transactions.

Since the individual will have undergone an identity proofing process at enrollment, transactions with respect to individual interactions with the CSP may not necessarily be pseudonymous.

Detailed requirements for each of the IALs are given in Section 4 and Section 5.

3 Definitions and Abbreviations

See SP 800-63, Appendix A for a complete set of definitions and abbreviations.

4 Identity Assurance Level Requirements

This section contains both normative and informative material.

This document describes the common pattern in which an applicant undergoes an identity proofing and enrollment process whereby their identity evidence and attributes are collected, uniquely resolved to a single identity within a given population or context, then validated and verified. See SP 800-63-3 Section 6.1 for details on how to choose the most appropriate IAL. A CSP may then bind these attributes to an authenticator (described in SP 800-63B).

Identity proofing's sole objective is to ensure the applicant is who they claim to be to a stated level of certitude. This includes presentation, validation, and verification of the minimum attributes necessary to accomplish identity proofing. There may be many different sets that suffice as the minimum, so CSPs should choose this set to balance privacy and the user's usability needs, as well as the likely attributes needed in future uses of the digital identity. For example, such attributes — to the extent they are the minimum necessary — could include:

1. Full name
2. Date of birth
3. Home Address

This document also provides requirements for CSPs collecting additional information used for purposes other than identity proofing.

4.1 Process Flow

This section is informative.

Figure 4-1 outlines the basic flow for identity proofing and enrollment.

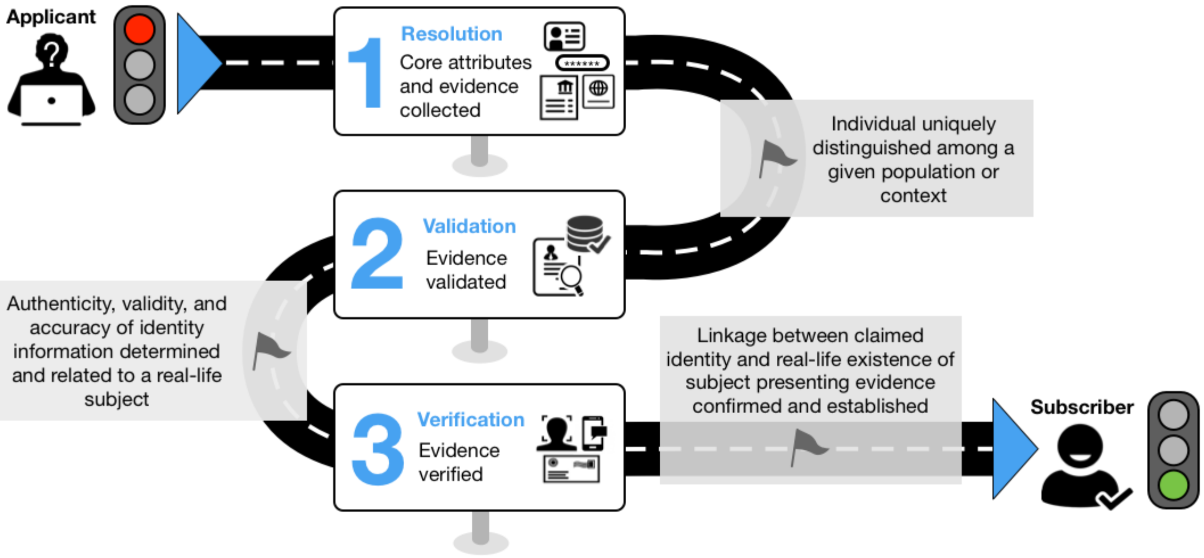
Applicant
1
Resolution
Core attributes and evidence collected
Individual uniquely distinguished among a given population or context
2
Validation
Evidence validated
Authenticity, validity, and accuracy of identity information determined and related to a real-life subject
Linkage between claimed identity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

Figure 4-1 The Identity Proofing User Journey

The following provides a sample of how a CSP and an applicant interact during the identity proofing process:

1. **Resolution**
   a. The CSP collects PII from the applicant, such as name, address, date of birth, email, and phone number.
   b. The CSP also collects two forms of identity evidence, such as a driver's license and a passport. For example, using the camera of a laptop, the CSP can capture a photo of both sides of both pieces of identity evidence.
2. **Validation**
   a. The CSP validates the information supplied in 1a by checking an authoritative source. The CSP determines the information supplied by the applicant matches their records.
   b. The CSP checks the images of the license and the passport, determines there are no alterations, the data encoded in the QR codes matches the plain-text information, and that the identification numbers follow standard formats.
   c. The CSP queries the issuing sources for the license and passport and validates the information matches.
3. **Verification**
   a. The CSP asks the applicant for a photo of themselves to match to the license and passport.
   b. The CSP matches the pictures on the license and the passport to the applicant picture and determines they match.
   c. The CSP sends an enrollment code to the validated phone number of the applicant, the user provides the enrollment code to the CSP, and the CSP confirms they match, verifying the user is in possession and control of the validated phone number.

d. The applicant has been successfully proofed.

Note: The identity proofing process can be delivered by multiple service providers. It is possible, but not expected, that a single organization, process, technique, or technology will fulfill these process steps.

4.2 General Requirements

This section is normative.

The following requirements apply to any CSP performing identity proofing at IAL2 or IAL3.

1. Identity proofing SHALL NOT be performed to determine suitability or entitlement to gain access to services or benefits.
2. Collection of PII SHALL be limited to the minimum necessary to validate the existence of the claimed identity and associate the claimed identity with the applicant providing identity evidence for appropriate identity resolution, validation, and verification. This MAY include attributes that correlate identity evidence to authoritative sources and to provide RPs with attributes used to make authorization decisions.
3. The CSP SHALL provide explicit notice to the applicant at the time of collection regarding the purpose for collecting and maintaining a record of the attributes necessary for identity proofing, including whether such attributes are voluntary or mandatory to complete the identity proofing process, and the consequences for not providing the attributes.
4. The CSP SHALL NOT use attributes collected and maintained in the identity proofing process for any purpose other than identity proofing, authentication, or attribute assertions, or to comply with law or legal process unless the CSP provides clear notice and obtains consent from the subscriber for additional uses. CSPs SHALL NOT make consent with these additional purposes a condition of the service.
5. The CSP SHALL provide mechanisms for redress of applicant complaints or problems arising from the identity proofing. These mechanisms SHALL be easy for applicants to find and use. The CSP SHALL assess the mechanisms for their efficacy in achieving resolution of complaints or problems.
6. The identity proofing and enrollment processes SHALL be performed according to an applicable written policy or *practice statement* that specifies the particular steps taken to verify identities. The *practice statement* SHALL include control information detailing how the CSP handles proofing errors that result in an applicant not being successfully enrolled. For example, the number of retries allowed, proofing alternatives (e.g., in-person if remote fails), or fraud counter-measures when anomalies are detected.
7. The CSP SHALL maintain a record, including audit logs, of all steps taken to verify the identity of the applicant and SHALL record the types of identity evidence presented in the proofing process. The CSP SHALL conduct a risk management process, including assessments of privacy and security risks to determine:
    a. Any steps that it will take to verify the identity of the applicant beyond any mandatory requirements specified herein;

b. The PII, including any biometrics, images, scans, or other copies of the identity evidence that the CSP will maintain as a record of identity proofing (Note: Specific federal requirements may apply.); and

c. The schedule of retention for these records (Note: CSPs may be subject to specific retention policies in accordance with applicable laws, regulations, or policies, including any National Archives and Records Administration (NARA) records retention schedules that may apply).

8. All PII collected as part of the enrollment process SHALL be protected to ensure confidentiality, integrity, and attribution of the information source.

9. The entire proofing transaction, including transactions that involve a third party, SHALL occur over an authenticated protected channel.

10. The CSP SHOULD obtain additional confidence in identity proofing using fraud mitigation measures (e.g., inspecting geolocation, examining the device characteristics of the applicant, evaluating behavioral characteristics, checking vital statistic repositories such as the Death Master File [DMF], so long as any additional mitigations do not substitute for the mandatory requirements contained herein. In the event the CSP uses fraud mitigation measures, the CSP SHALL conduct a privacy risk assessment for these mitigation measures. Such assessments SHALL include any privacy risk mitigations (e.g., risk acceptance or transfer, limited retention, use limitations, notice) or other technological mitigations (e.g., cryptography), and be documented per requirement 4.2(7) above.

11. In the event a CSP ceases to conduct identity proofing and enrollment processes, the CSP SHALL be responsible for fully disposing of or destroying any sensitive data including PII, or its protection from unauthorized access for the duration of retention.

12. Regardless of whether the CSP is an agency or private sector provider, the following requirements apply to the agency offering or using the proofing service:

d. The agency SHALL consult with their Senior Agency Official for Privacy (SAOP) to conduct an analysis determining whether the collection of PII to conduct identity proofing triggers Privacy Act requirements.

e. The agency SHALL publish a System of Records Notice (SORN) to cover such collection, as applicable.

f. The agency SHALL consult with their SAOP to conduct an analysis determining whether the collection of PII to conduct identity proofing triggers E-Government Act of 2002 requirements.

g. The agency SHALL publish a Privacy Impact Assessment (PIA) to cover such collection, as applicable.

13. The CSP SHOULD NOT collect the Social Security Number (SSN) unless it is necessary for performing identity resolution, and identity resolution cannot be accomplished by collection of another attribute or combination of attributes.

4.3 Identity Assurance Level 1

This section is normative.

A CSP that supports only IAL1 CSP SHALL NOT validate and verify attributes.

1. The CSP MAY request zero or more self-asserted attributes from the applicant to support their service offering.
2. An IAL2 or IAL3 CSP SHOULD support RPs that only require IAL1, if the user consents.

4.4 Identity Assurance Level 2

This section is normative.

IAL2 allows for **remote** or **in-person** identity proofing. IAL2 supports a wide range of acceptable identity proofing techniques in order to increase user adoption, decrease false negatives (legitimate applicants that cannot successfully complete identity proofing), and detect to the best extent possible the presentation of fraudulent identities by a malicious applicant.

A CSP SHALL proof according to the requirements in Section 4.4.1 or Section 4.4.2. A CSP SHOULD implement identity proofing in accordance Section 4.4.1 Depending on the population the CSP serves, the CSP MAY implement identity proofing in accordance with Section 4.4.2.

4.4.1 IAL2 Conventional Proofing Requirements

The following sections provide requirements for resolution, evidence collection, validation, verification, and presence. They also explore biometric collection and security controls.

4.4.1.1 Resolution Requirements

Collection of PII SHALL be limited to the minimum necessary to resolve to a unique identity in a given context. This MAY include the collection of attributes that assist in data queries. See Section 5.1 for general resolution requirements.

4.4.1.2 Evidence Collection Requirements

The CSP SHALL collect the following from the applicant:

1. One piece of SUPERIOR or STRONG evidence **if** the evidence's issuing source, during its identity proofing event, confirmed the claimed identity by collecting two or more forms of SUPERIOR or STRONG evidence **and** the CSP validates the evidence directly with the issuing source; **OR**
2. Two pieces of STRONG evidence; **OR**
3. One piece of STRONG evidence plus two pieces of FAIR evidence

See Section 5.2.1 Identity Evidence Quality Requirements for more information on acceptable identity evidence.

4.4.1.3 Validation Requirements

The CSP SHALL validate identity evidence as follows:

Each piece of evidence SHALL be validated with a process that can achieve the same strength as the evidence presented. For example, if two forms of STRONG identity evidence are presented, each piece of evidence will be validated at a strength of STRONG.

See Section 5.2.2 Validating Identity Evidence for more information on validating identity evidence.

4.4.1.4 Verification Requirements

The CSP SHALL verify identity evidence as follows:

1. At a minimum, the applicant's binding to identity evidence must be verified by a process that is able to achieve a strength of STRONG.
2. Knowledge-based verification (KBV) SHALL NOT be used for in-person (physical or supervised remote) identity verification.

See Section 5.3 Identity Verification for more information on acceptable identity evidence.

4.4.1.5 Presence Requirements

The CSP SHALL support in-person or remote identity proofing. The CSP SHOULD offer both in-person and remote proofing.

4.4.1.6 Address Confirmation

1. Valid records to confirm address SHALL be issuing source(s) or authoritative source(s).
2. The CSP SHALL confirm address of record. The CSP SHOULD confirm address of record through validation of the address contained on any supplied, valid piece of identity evidence. The CSP MAY confirm address of record by validating information supplied by the applicant that is not contained on any supplied piece of identity evidence.
3. Self-asserted address data that has not been confirmed in records SHALL NOT be used for confirmation.
4. **If CSP performs in-person proofing (physical or supervised remote):**
   a. The CSP SHOULD send a notification of proofing to a confirmed address of record.
   b. The CSP MAY provide an enrollment code directly to the subscriber if binding to an authenticator will occur at a later time.
   c. The enrollment code SHALL be valid for a maximum of 7 days.
5. **If the CSP performs remote proofing (unsupervised):**
   a. The CSP SHALL send an enrollment code to a confirmed address of record for the applicant.

b. The applicant SHALL present a valid enrollment code to complete the identity proofing process.

c. The CSP SHOULD send the enrollment code to the postal address that has been validated in records. The CSP MAY send the enrollment code to a mobile telephone (SMS or voice), landline telephone, or email if it has been validated in records.

d. If the enrollment code is also intended to be an authentication factor, it SHALL be reset upon first use.

e. Enrollment codes sent to a postal address of record SHALL be valid for a maximum of 10 days but MAY be made valid up to 30 days via an exception process to accommodate addresses outside the contiguous United States. Enrollment codes sent by telephone SHALL be valid for a maximum of 10 minutes. Enrollment codes sent via email SHALL be valid for a maximum of 24 hours.

f. The CSP SHALL ensure the enrollment code and notification of proofing are sent to different addresses of record. For example, if the CSP sends an enrollment code to a phone number validated in records, a proofing notification will be sent to the postal address validated in records or obtained from validated and verified evidence, such as a driver's license.

Note: Postal address is the preferred method of sending any communications, including enrollment code and notifications, with the applicant. However, these guidelines support any confirmed address of record, whether physical or digital.

4.4.1.7 Biometric Collection

The CSP MAY collect biometrics for the purposes of non-repudiation and re-proofing. See SP 800-63B, Section 5.2.3 for more detail on biometric collection.

4.4.1.8 Security Controls

The CSP SHALL employ appropriately tailored security controls, to include control enhancements, from the moderate or high baseline of security controls defined in SP 800-53 or equivalent federal (e.g., FEDRAMP) or industry standard. The CSP SHALL ensure that the minimum assurance-related controls for *moderate-impact* systems or equivalent are satisfied.

4.4.2 IAL2 Trusted Referee Proofing Requirements

In instances where an individual cannot meet the identity evidence requirements specified in Section 4.4.1, the agency MAY use a trusted referee to assist in identity proofing the applicant. See Section 5.3.4 for more details.

4.5 Identity Assurance Level 3

This section is normative.

IAL3 adds additional rigor to the steps required at IAL2, to include providing further evidence of superior strength, and is subject to additional and specific processes (including the use of biometrics) to further protect the identity and RP from impersonation, fraud, or other significantly harmful damages. Biometrics are used to detect fraudulent enrollments, duplicate enrollments, and as a mechanism to re-establish binding to a credential. In addition, identity proofing at IAL3 is performed in-person (to include supervised remote). See Section 5.3.3 for more details.

4.5.1 Resolution Requirements

Collection of PII SHALL be limited to the minimum necessary to resolve to a unique identity record. This MAY include the collection of attributes that assist in data queries. See Section 5.1 for general resolution requirements.

4.5.2 Evidence Collection Requirements

The CSP SHALL collect the following from the applicant:

1. Two pieces of SUPERIOR evidence; **OR**
2. One piece of SUPERIOR evidence and one piece of STRONG evidence **if** the issuing source of the STRONG evidence, during its identity proofing event, confirmed the claimed identity by collecting two or more forms of SUPERIOR or STRONG evidence **and** the CSP validates the evidence directly with the issuing source; **OR**
3. Two pieces of STRONG evidence plus one piece of FAIR evidence.

See Section 5.2.1 Identity Evidence Quality Requirements for more information on acceptable identity evidence.

4.5.3 Validation Requirements

The CSP SHALL validate identity evidence as follows:

Each piece of evidence must be validated with a process that is able to achieve the same strength as the evidence presented. For example, if two forms of STRONG identity evidence are presented, each piece of evidence will be validated at a strength of STRONG.

See Section 5.2.2 Validating Identity Evidence for more information on validating identity evidence

4.5.4 Verification Requirements

The CSP SHALL verify identity evidence as follows:

1. At a minimum, the applicant’s binding to identity evidence must be verified by a process that is able to achieve a strength of SUPERIOR.
2. KBV SHALL NOT be used for in-person (physical or supervised remote) identity verification.

See Section 5.3 Identity Verification for more information on acceptable identity evidence.

4.5.5 Presence Requirements

The CSP SHALL perform all identity proofing steps with the applicant in-person. See Section 5.3.3 for more details.

4.5.6 Address Confirmation

1. The CSP SHALL confirm address of record. The CSP SHOULD confirm address of record through validation of the address contained on any supplied, valid piece of identity evidence. The CSP MAY confirm address of record by validating information supplied by the applicant, not contained on any supplied, valid piece of identity evidence.
2. Self-asserted address data SHALL NOT be used for confirmation.
3. A notification of proofing SHALL be sent to the confirmed address of record.
4. The CSP MAY provide an enrollment code directly to the subscriber if binding to an authenticator will occur at a later time. The enrollment code SHALL be valid for a maximum of 7 days.

4.5.7 Biometric Collection

The CSP SHALL collect and record a biometric sample at the time of proofing (e.g., facial image, fingerprints) for the purposes of non-repudiation and re-proofing. See Section 5.2.3 of SP 800-63B for more detail on biometric collection.

4.5.8 Security Controls

The CSP SHALL employ appropriately tailored security controls, to include control enhancements, from the high baseline of security controls defined in SP 800-53 or an equivalent federal (e.g., FEDRAMP) or industry standard. The CSP SHALL ensure that the minimum assurance-related controls for *high-impact* systems or equivalent are satisfied.

4.6 Enrollment Code

This section is normative.

An enrollment code allows the CSP to confirm that the applicant controls an address of record, as well as offering the applicant the ability to reestablish binding to their enrollment record. Binding NEED NOT be completed in the same session as the original identity proofing transaction.

An enrollment code SHALL be comprised of one of the following:

1. Minimally, a random six character alphanumeric or equivalent entropy. For example, a code generated using an approved random number generator or a serial number for a physical hardware authenticator.
2. A machine-readable optical label, such as a QR Code, that contains data of similar or higher entropy as a random six character alphanumeric.

4.7 Summary of Requirements

This section is informative.

Table 4-1 summarizes the requirements for each of the authenticator assurance levels.

Table 4-1 IAL Requirements Summary

Requirement	IAL1	IAL2	IAL3
Presence	No Requirements	In-person and unsupervised remote.	In-person and supervised remote.
Resolution	No Requirements	• The minimum attributes necessary to accomplish identity resolution. • KBV may be used for added confidence.	Same as IAL2
Evidence	No identity evidence is collected.	• One piece of SUPERIOR or STRONG evidence depending on strength of original proof and validation occurs with issuing source, **OR** • Two pieces of STRONG evidence, **OR** • One piece of STRONG evidence plus two (2) pieces of FAIR evidence.	• Two pieces of SUPERIOR evidence, **OR** • One piece of SUPERIOR evidence and one piece of STRONG evidence depending on strength of original proof and validation occurs with issuing source, **OR** • Two pieces of STRONG evidence plus one piece of FAIR evidence.
Validation	No validation	Each piece of evidence must be validated with a process that is able to achieve the same strength as the evidence presented.	Same as IAL2

Verification	No verification	Verified by a process that is able to achieve a strength of STRONG.	Verified by a process that is able to achieve a strength of SUPERIOR.

Address Confirmation	No requirements for address confirmation	Required. Enrollment code sent to any address of record. Notification sent by means different from enrollment code.	Required. Notification of proofing to postal address.

Biometric Collection	No	Optional	Mandatory

Security Controls	N/A	• SP 800-53 • Moderate Baseline (or equivalent federal or industry standard).	• SP 800-53 • High Baseline (or equivalent federal or industry standard).

5 Identity Resolution, Validation, and Verification

This section is normative.

This section lists the requirements to resolve, validate, and verify an identity and any supplied identity evidence. The requirements are intended to ensure the claimed identity is the actual identity of the subject attempting to enroll with the CSP and that scalable attacks affecting a large population of enrolled individuals require greater time and cost than the value of the resources the system is protecting.

5.1 Identity Resolution

The goal of identity resolution is to uniquely distinguish an individual within a given population or context. Effective identity resolution uses the smallest set of attributes necessary to resolve to a unique individual. It provides the CSP an important starting point in the overall identity proofing process, to include the initial detection of potential fraud, but in no way represents a complete and successful identity proofing transaction.

1. Exact matches of information used in the proofing process can be difficult to achieve. The CSP MAY employ appropriate matching algorithms to account for differences in personal information and other relevant proofing data across multiple forms of identity evidence, issuing sources, and authoritative sources. Matching algorithms and rules used SHOULD be available publicly or, at minimum, to the relevant community of interest. For example, they may be included as part of the written policy or *practice statement* referred to in Section 4.2.
2. KBV (sometimes referred to as knowledge-based authentication) has historically been used to verify a claimed identity by testing the knowledge of the applicant against information obtained from public databases. The CSP MAY use KBV to resolve to a unique, claimed identity.

5.2 Identity Evidence Collection and Validation

The goal of identity validation is to collect the most appropriate identity evidence (e.g., a passport or driver’s license) from the applicant and determine its authenticity, validity, and accuracy. Identity validation is made up of three process steps: collecting the appropriate identity evidence, confirming the evidence is genuine and authentic, and confirming the data contained on the identity evidence is valid, current, and related to a real-life subject.

5.2.1 Identity Evidence Quality Requirements

This section provides quality requirements for identity evidence collected during identity proofing.

Table 5-1 lists strengths, ranging from unacceptable to superior, of identity evidence that is collected to establish a valid identity. Unless otherwise noted, to achieve a given strength the evidence SHALL, at a minimum, meet all the qualities listed.

Table 5-1 Strengths of Identity Evidence

Strength	Qualities of Identity Evidence
Unacceptable	No acceptable identity evidence provided.
Weak	• The issuing source of the evidence did not perform identity proofing. • The issuing process for the evidence means that it can reasonably be assumed to have been delivered into the possession of the applicant. • The evidence contains: ○ At least one reference number that uniquely identifies itself or the person to whom it relates, **OR** ○ The issued identity evidence contains a photograph or biometric template (of any modality) of the person to whom it relates.
Fair	• The issuing source of the evidence confirmed the claimed identity through an identity proofing process. • The issuing process for the evidence means that it can reasonably be assumed to have been delivered into the possession of the person to whom it relates. • The evidence: ○ Contains at least one reference number that uniquely identifies the person to whom it relates, **OR** ○ Contains a photograph or biometric template (any modality) of the person to whom it relates, **OR** ○ Can have ownership confirmed through KBV. • Where the evidence includes digital information, that information is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the claimed issuing source to be confirmed. • Where the evidence includes physical security features, it requires proprietary knowledge to be able to reproduce it. • The issued evidence is unexpired.
Strong	• The issuing source of the evidence confirmed the claimed identity through written procedures designed to enable it to form a reasonable belief that it knows the real-life identity of the person. Such procedures shall be subject to recurring oversight by regulatory or publicly-accountable institutions. For example, the Customer Identification Program guidelines established in response to the USA PATRIOT Act of 2001 or the Red Flags Rule, under Section 114 of the Fair and Accurate Credit Transaction Act of 2003 (FACT Act). • The issuing process for the evidence ensured that it was delivered into the possession of the subject to whom it relates.

	• The issued evidence contains at least one reference number that uniquely identifies the person to whom it relates. • The full name on the issued evidence must be the name that the person was officially known by at the time of issuance. Not permitted are pseudonyms, aliases, an initial for surname, or initials for all given names. • The: o Issued evidence contains a photograph or biometric template (of any modality) of the person to whom it relates, **OR** o Applicant proves possession of an AAL2 authenticator bound to an IAL2 identity, at a minimum. • Where the issued evidence includes digital information, that information is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the claimed issuing source to be confirmed. • Where the issued evidence contains physical security features, it requires proprietary knowledge and proprietary technologies to be able to reproduce it. • The evidence is unexpired.

Superior	• The issuing source of the evidence confirmed the claimed identity by following written procedures designed to enable it to have high confidence that the source knows the real-life identity of the subject. Such procedures shall be subject to recurring oversight by regulatory or publicly accountable institutions. • The issuing source visually identified the applicant and performed further checks to confirm the existence of that person. • The issuing process for the evidence ensured that it was delivered into the possession of the person to whom it relates. • The evidence contains at least one reference number that uniquely identifies the person to whom it relates. • The full name on the evidence must be the name that the person was officially known by at the time of issuance. Not permitted are pseudonyms, aliases, an initial for surname, or initials for all given names. • The evidence contains a photograph of the person to whom it relates. • The evidence contains a biometric template (of any modality) of the person to whom it relates. • The evidence includes digital information, the information is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the issuing source to be confirmed. • The evidence includes physical security features that require proprietary knowledge and proprietary technologies to be able to reproduce it. • The evidence is unexpired.

5.2.2 Validating Identity Evidence

Once the CSP obtains the identity evidence, the accuracy, authenticity, and integrity of the evidence and related information is checked against authoritative sources in order to determine that the presented evidence:

- Is genuine, authentic, and not a counterfeit, fake, or forgery;
- Contains information that is correct; and
- Contains information that relates to a real-life subject.

Table 5-2 lists strengths, ranging from unacceptable to superior, of identity validation performed by the CSP to validate the evidence presented for the current proofing session and the information contained therein.

Table 5-2 Validating Identity Evidence

Strength	Method(s) Performed by the CSP
Unacceptable	• Evidence validation was not performed, or validation of the evidence failed.
Weak	• All personal details from the evidence have been confirmed as valid by comparison with information held or published by an authoritative source.
Fair	• Attributes contained in the evidence have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s), **OR** • The evidence has been confirmed as genuine using appropriate technologies, confirming the integrity of physical security features and that the evidence is not fraudulent or inappropriately modified, **OR** • The evidence has been confirmed as genuine by trained personnel, **OR** • The evidence has been confirmed as genuine by confirmation of the integrity of cryptographic security features.

Strong	• The evidence has been confirmed as genuine: ○ using appropriate technologies, confirming the integrity of physical security features and that the evidence is not fraudulent or inappropriately modified, **OR** ○ by trained personnel and appropriate technologies, confirming the integrity of the physical security features and that the evidence is not fraudulent or inappropriately modified, **OR** ○ by confirmation of the integrity of cryptographic security features. • All personal details and evidence details have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s).

Superior	• The evidence has been confirmed as genuine by trained personnel and appropriate technologies including the integrity of any physical and cryptographic security features. • All personal details and evidence details from the evidence have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s).

Training requirements for personnel validating evidence SHALL be based on the policies, guidelines, or requirements of the CSP or RP.

5.3 Identity Verification

The goal of identity verification is to confirm and establish a linkage between the claimed identity and the real-life existence of the subject presenting the evidence.

5.3.1 Identity Verification Methods

Table 5-3 details the verification methods necessary to achieve a given identity verification strength. The CSP SHALL adhere to the requirements in Section 5.3.2 if KBV is used to verify an identity.

Table 5-3 Verifying Identity Evidence

Strength	Identity Verification Methods
Unacceptable	Evidence verification was not performed or verification of the evidence failed. Unable to confirm that the applicant is the owner of the claimed identity.
Weak	The applicant has been confirmed as having access to the evidence provided to support the claimed identity.
Fair	• The applicant's ownership of the claimed identity has been confirmed by: ○ KBV. See Section 5.3.2. for more details, **OR** ○ a physical comparison of the applicant to the strongest piece of identity evidence provided to support the claimed identity. Physical comparison performed remotely SHALL adhere to all requirements as specified in SP 800-63B, Section 5.2.3, **OR** ○ biometric comparison of the applicant to the identity evidence. Biometric comparison performed remotely SHALL adhere to all requirements as specified in SP 800-63B, Section 5.2.3.
Strong	• The applicant's ownership of the claimed identity has been confirmed by: ○ physical comparison, using appropriate technologies, to a photograph, to the strongest piece of identity evidence provided to support the claimed identity. Physical comparison performed remotely SHALL adhere to all requirements as specified in SP 800-63B, Section 5.2.3, **OR** ○ biometric comparison, using appropriate technologies, of the applicant to the strongest piece of identity evidence provided to support the claimed identity. Biometric comparison performed remotely SHALL adhere to all

	requirements as specified in SP 800-63B, Section 5.2.3.

Superior	The applicant’s ownership of the claimed identity has been confirmed by biometric comparison of the applicant to the strongest piece of identity evidence provided to support the claimed identity, using appropriate technologies. Biometric comparison performed remotely SHALL adhere to all requirements as specified in SP 800-63B, Section 5.2.3.

5.3.2 Knowledge-Based Verification Requirements

The following requirements apply to the identity verification steps for IAL2 and IAL3. There are no restrictions for the use of KBV for identity resolution.

1. The CSP SHALL NOT use KBV to verify an applicant's identity against more than one piece of validated identity evidence.
2. The CSP SHALL only use information that is expected to be known only to the applicant and the authoritative source, to include any information needed to begin the KBV process. Information accessible freely, for a fee in the public domain, or via the black market SHALL NOT be used.
3. The CSP SHALL allow a resolved and validated identity to opt out of KBV and leverage another process for verification.
4. The CSP SHOULD perform KBV by verifying knowledge of recent transactional history in which the CSP is a participant. The CSP SHALL ensure that transaction information has at least 20 bits of entropy. For example, to reach minimum entropy requirements, the CSP could ask the applicant for verification of the amount(s) and transaction numbers(s) of a micro-deposit(s) to a valid bank account, so long as the total number of digits is seven or greater.
5. The CSP MAY perform KBV by asking the applicant questions to demonstrate they are the owner of the claimed information. However, the following requirements apply:
    a. KBV SHOULD be based on multiple authoritative sources.
    b. The CSP SHALL require a minimum of four KBV questions with each requiring a correct answer to successfully complete the KBV step.
    c. The CSP SHOULD require free-form response KBV questions. The CSP MAY allow multiple choice questions, however, if multiple choice questions are provided, the CSP SHALL require a minimum of four answer options per question.
    d. The CSP SHOULD allow two attempts for an applicant to complete the KBV. A CSP SHALL NOT allow more than three attempts to complete the KBV.
    e. The CSP SHALL time out KBV sessions after two minutes of inactivity per question. In cases of session timeout, the CSP SHALL restart the entire KBV process and consider this a failed attempt.
    f. The CSP SHALL NOT present a majority of diversionary KBV questions (i.e., those where "none of the above" is the correct answer).
    g. The CSP SHOULD NOT ask the same KBV questions in subsequent attempts.
    h. The CSP SHALL NOT ask a KBV question that provides information that could assist in answering any future KBV question in a single session or a subsequent session after a failed attempt.
    i. The CSP SHALL NOT use KBV questions for which the answers do not change (e.g., "What was your first car?").

j. CSP SHALL ensure that any KBV question does not reveal PII that the applicant has not already provided, nor personal information that, when combined with other information in a KBV session, could result in unique identification.

5.3.3 In-Person Proofing Requirements

In-person proofing can be satisfied in either of two ways:

- A physical interaction with the applicant, supervised by an operator.
- An remote interaction with the applicant, supervised by an operator, based on the specific requirements Section 5.3.3.2.

5.3.3.1 General Requirements

1. The CSP SHALL have the operator view the biometric source (e.g., fingers, face) for presence of non-natural materials and perform such inspections as part of the proofing process.
2. The CSP SHALL collect biometrics in such a way that ensures that the biometric is collected from the applicant, and not another subject. All biometric performance requirements in SP 800-63B, Section 5.2.3 apply.

5.3.3.2 Requirements for Supervised Remote In-Person Proofing

CSPs can employ remote proofing processes to achieve comparable levels of confidence and security to in-person events. The following requirements establish comparability between in-person transactions where the applicant is in the same physical location as the CSP to those where the applicant is remote.

Supervised remote identity proofing and enrollment transactions SHALL meet the following requirements, in addition to the IAL3 validation and verification requirements specified in Section 4.6:

1. The CSP SHALL monitor the entire identity proofing session, from which the applicant SHALL NOT depart — for example, by a continuous high-resolution video transmission of the applicant.
2. The CSP SHALL have a live operator participate remotely with the applicant for the entirety of the identity proofing session.
3. The CSP SHALL require all actions taken by the applicant during the identity proofing session to be clearly visible to the remote operator.
4. The CSP SHALL require that all digital verification of evidence (e.g., via chip or wireless technologies) be performed by integrated scanners and sensors.
5. The CSP SHALL require operators to have undergone a training program to detect potential fraud and to properly perform a virtual in-process proofing session.
6. The CSP SHALL employ physical tamper detection and resistance features appropriate for the environment in which it is located. For example, a kiosk located in a restricted area or one where it is monitored by a trusted individual requires less tamper detection than one that is located in a semi-public area such as a shopping mall concourse.

7. The CSP SHALL ensure that all communications occur over a mutually authenticated protected channel.

5.3.4 Trusted Referee Requirements

1. The CSP MAY use trusted referees — such as notaries, legal guardians, medical professionals, conservators, persons with power of attorney, or some other form of trained and approved or certified individuals — that can vouch for or act on behalf of the applicant in accordance with applicable laws, regulations, or agency policy. The CSP MAY use a trusted referee for both remote and in-person processes.
2. The CSP SHALL establish written policy and procedures as to how a trusted referee is determined and the lifecycle by which the trusted referee retains their status as a valid referee, to include any restrictions, as well as any revocation and suspension requirements.
3. The CSP SHALL proof the trusted referee at the same IAL as the applicant proofing. In addition, the CSP SHALL determine the minimum evidence required to bind the relationship between the trusted referee and the applicant.
4. The CSP SHOULD perform re-proofing of the subscriber at regular intervals defined in the written policy specified in item 1 above, with the goal of satisfying the requirements of Section 4.4.1.

5.3.4.1 Additional Requirements for Minors

1. The CSP SHALL give special consideration to the legal restrictions of interacting with minors unable to meet the evidence requirements of identity proofing to ensure compliance with the Children's Online Privacy Protection Act of 1998 (COPPA) [COPPA], and other laws, as applicable.
2. Minors under age 13 require additional special considerations under COPPA [COPPA], and other laws, to which the CSP SHALL ensure compliance, as applicable.
3. The CSP SHOULD involve a parent or legal adult guardian as a trusted referee for an applicant that is a minor, as described elsewhere in this section.

5.4 Binding Requirements

See SP 800-63B, Section 6.1 Authenticator Binding for instructions on binding authenticators to subscribers.

6 Derived Credentials

This section is informative.

Deriving credentials is based on the process of an individual proving to a CSP that they are the rightful subject of an identity record (i.e., a credential) that is bound to one or more authenticators they possess. This process is made available by a CSP that wants individuals to have an opportunity to obtain new authenticators bound to the existing, identity proofed record, or credential. As minimizing the number of times the identity proofing process is repeated benefits the individual and CSP, deriving identity is accomplished by proving possession and successful authentication of an authenticator that is already bound to the original, proofed digital identity.

The definition of derived in this section does *not* imply that an authenticator is cryptographically tied to a primary authenticator, for example deriving a key from another key. Rather, an authenticator can be derived by simply issuing on the basis of successful authentication with an authenticator that is already bound to a proofed identity, rather than unnecessarily repeating an identity proofing process.

There are two specific use cases for deriving identity:

1. A *claimant* seeks to obtain a derived PIV, bound to their identity record, for use only within the limits and authorizations of having a PIV smartcard. *This use case is covered in SP 800-157, Guidelines for Derived Personal Identity Verification (PIV) Credentials.*
2. An *applicant* seeks to establish a credential with a CSP with which the individual does not have a pre-existing relationship. For example, an applicant wants to switch from one CSP to another, or have a separate authenticator from a new CSP for other uses (e.g., basic browsing vs. financial). *This use case is covered by allowable identity evidence in Section 5.2.*

As stated above, all requirements for PIV-derived credentials can be found in SP 800-157. For the second use case described above, this guideline does not differentiate between physical and digital identity evidence. Therefore it is acceptable, if the authenticator or an assertion generated by the primary CSP meet the requirements of Section 5, for them to be used at identity evidence for IAL2 and IAL3. In addition, any authenticators issued as a result of providing digital identity evidence are subject to the requirements of SP 800-63B.

7 Threats and Security Considerations

This section is informative.

There are two general categories of threats to the enrollment process: impersonation, and either compromise or malfeasance of the infrastructure provider. This section focuses on impersonation threats, as infrastructure threats are addressed by traditional computer security controls (e.g., intrusion protection, record keeping, independent audits) and are outside the scope of this document. For more information on security controls, see SP 800-53, *Recommended Security and Privacy Controls for Federal Information Systems and Organizations*.

Threats to the enrollment process include impersonation attacks and threats to the transport mechanisms for identity proofing, authenticator binding, and credential issuance. Table 7-1 lists the threats related to enrollment and identity proofing.

Table 7-1 Enrollment and Identity Proofing Threats

Activity	Threat/Attack	Example
Enrollment	Falsified identity proofing evidence	An applicant claims an incorrect identity by using a forged driver's license.
	Fraudulent use of another's identity	An applicant uses a passport associated with a different individual.
	Enrollment repudiation	A subscriber denies enrollment, claiming that they did not enroll with the CSP.

7.1 Threat Mitigation Strategies

Enrollment threats can be deterred by making impersonation more difficult to accomplish or by increasing the likelihood of detection. This recommendation deals primarily with methods for making impersonation more difficult; however, it does prescribe certain methods and procedures that may help prove who perpetrated an impersonation. At each level, methods are employed to determine that a person with the claimed identity exists, that the applicant is the person entitled to the claimed identity, and that the applicant cannot later repudiate the enrollment. As the level of assurance increases, the methods employed provide increasing resistance to casual, systematic, and insider impersonation. Table 7-2 lists strategies for mitigating threats to the enrollment and issuance processes.

Table 7-2 Enrollment and Issuance Threat Mitigation Strategies

Activity	Threat/Attack	Mitigation Strategy	Normative Reference(s)
Enrollment	Falsified identity proofing evidence	CSP validates physical security features of presented evidence.	4.4.1.3, 4.5.3, 5.2.2
		CSP validates personal details in the evidence with the issuer or other authoritative source.	4.4.1.3, 4.5.3, 4.5.6, 5.2.2.
	Fraudulent use of another's identity	CSP verifies identity evidence and biometric of applicant against information obtained from issuer or other authoritative source.	4.4.1.7, 4.5.7, 5.3
		Verify applicant-provided non-government-issued documentation (e.g., electricity bills in the name of the applicant with the current address of the applicant printed on the bill, or a credit card bill) to help achieve a higher level of confidence in the applicant's identity.	4.4.1.7, 4.5.7, 5.3
	Enrollment repudiation	CSP saves a subscriber's biometric.	4.4.1.7, 4.5.7

8 Privacy Considerations

This section is informative.

These privacy considerations provide information regarding the General Requirements set forth in Section 4.2.

8.1 Collection and Data Minimization

Section 4.2 requirement 2 permits the collection of only the PII necessary to validate the existence of the claimed identity and associate the claimed identity to the applicant, based on best available practices for appropriate identity resolution, validation, and verification. Collecting unnecessary PII can create confusion regarding why information not being used for the identity proofing service is being collected. This leads to invasiveness or overreach concerns, which can lead to loss of applicant trust. Furthermore, PII retention can become vulnerable to unauthorized access or use. Data minimization reduces the amount of PII vulnerable to unauthorized access or use, and encourages trust in the identity proofing process.

8.1.1 Social Security Numbers

Section 4.2 requirement 13 does not permit the CSP to collect the SSN unless it is necessary for performing identity resolution, when resolution cannot be accomplished by collection of another attribute or combination of attributes. Overreliance on the SSN can contribute to misuse and place the applicant at risk of harm, such as through identity theft. Nonetheless, the SSN may achieve identity resolution for RPs in particular federal agencies that use SSNs to correlate a subscriber to existing records. Thus, this document recognizes the role of the SSN as an identifier and makes appropriate allowance for its use.

Note: Evidence requirements at the higher IALs preclude using the SSN or the Social Security Card as acceptable identity evidence.

Prior to collecting the SSN for identity proofing, organizations need to consider any legal obligation to collect the SSN, the necessity of using the SSN for interoperability with third party processes and systems, or operational requirements. Operational requirements can be demonstrated by an inability to alter systems, processes, or forms due to cost or unacceptable levels of risk. Operational necessity is not justified by ease of use or unwillingness to change.

For federal agencies, the initial requirement in Executive Order (EO) 9397 to use the SSN as a primary means of identification for individuals working for, with, or conducting business with their agency, has since been eliminated. Accordingly, EO 9397 cannot be referenced as the sole authority establishing the collection of the SSN as necessary.

Federal agencies need to review any decision to collect the SSN relative to their obligation to reduce the collection and unnecessary use of SSNs under Office of Management and Budget policy.

8.2 Notice and Consent

Section 4.2 requirement 3 requires the CSP provide explicit notice to the applicant at the time of collection regarding the purpose for collecting and maintaining a record of the attributes necessary for identity proofing, including whether such attributes are voluntary or mandatory in order to complete the identity proofing transactions, and the consequences for not providing the attributes.

An effective notice will take into account user experience design standards and research, and an assessment of privacy risks that may arise from the collection. Various factors should be considered, including incorrectly inferring that applicants understand why attributes are collected, that collected information may be combined with other data sources, etc. An effective notice is never only a pointer leading to a complex, legalistic privacy policy or general terms and conditions that applicants are unlikely to read or understand.

8.3 Use Limitation

Section 4.2 requirement 4 does not permit the CSP to use attributes collected and maintained in the identity proofing process for any purpose other than identity proofing, authentication, authorization, or attribute assertions, related fraud mitigation, or to comply with law or legal process unless the CSP provides clear notice and obtains consent from the subscriber for additional uses.

Consult your SAOP if there are questions about whether proposed uses fall within the scope of these permitted uses. This notice should follow the same principles as described in Section 8.2 Notice and Consent and should not be rolled up into a legalistic privacy policy or general terms and conditions. Rather if there are uses outside the bounds of these explicit purposes, the subscriber should be provided with a meaningful way to understand the purpose for additional uses, and the opportunity to accept or decline. The CSP cannot make acceptance by the subscriber of additional uses a condition of providing identity proofing services.

8.4 Redress

Section 4.2 requirement 5 requires the CSP to provide effective mechanisms for redressing applicant complaints or problems arising from the identity proofing, and make the mechanisms easy for applicants to find and access.

The Privacy Act requires federal CSPs that maintain a system of records to follow procedures to enable applicants to access and, if incorrect, amend their records. Any Privacy Act Statement should include a reference to the applicable SORN(s), which provide the applicant with instructions on how to make a request for access or correction. Non-federal CSPs should have comparable procedures, including contact information for any third parties if they are the source of the information.

CSPs should make the availability of alternative methods for completing the process clear to users (e.g., in person at a customer service center, if available) in the event an applicant is unable to establish their identity and complete the registration process online.

Note: If the ID proofing process is not successful, CSPs should inform the applicant of the procedures to address the issue but should not inform the applicant of the specifics of why the registration failed (e.g., do not inform the applicant, "Your SSN did not match the one that we have on record for you"), as doing so could allow fraudulent applicants to gain more knowledge about the accuracy of the PII.

8.5 Privacy Risk Assessment

Section 4.2 requirement 7 and 10 require the CSP to conduct a privacy risk assessment. In conducting a privacy risk assessment, CSPs should consider:

1. The likelihood that the action it takes (e.g., additional verification steps or records retention) could create a problem for the applicant, such as invasiveness or unauthorized access to the information; and
2. The impact if a problem did occur. CSPs should be able to justify any response it takes to identified privacy risks, including accepting the risk, mitigating the risk, and sharing the risk. The use of applicant consent should be considered a form of sharing the risk, and therefore should only be used when an applicant could reasonably be expected to have the capacity to assess and accept the shared risk.

8.6 Agency Specific Privacy Compliance

Section 4.2 requirement 12 covers specific compliance obligations for federal CSPs. It is critical to involve your agency's SAOP in the earliest stages of digital authentication system development to assess and mitigate privacy risks and advise the agency on compliance requirements, such as whether or not the PII collection to conduct identity proofing triggers the Privacy Act of 1974 [Privacy Act] or the E-Government Act of 2002 [E-Gov] requirement to conduct a Privacy Impact Assessment. For example, with respect to identity proofing, it is likely that the Privacy Act requirements will be triggered and require coverage by either a new or existing Privacy Act system of records due to the collection and maintenance of PII or other attributes necessary to conduct identity proofing.

The SAOP can similarly assist the agency in determining whether a PIA is required. These considerations should not be read as a requirement to develop a Privacy Act SORN or PIA for identity proofing alone; in many cases it will make the most sense to draft a PIA and SORN that encompasses the entire digital authentication process or include the digital authentication process as part of a larger programmatic PIA that discusses the program or benefit the agency is establishing online access to.

Due to the many components of digital authentication, it is important for the SAOP to have an awareness and understanding of each individual component. For example, other privacy artifacts may be applicable to an agency offering or using proofing services such as Data Use Agreements, Computer Matching Agreements, etc. The SAOP can assist the agency in determining what additional requirements apply. Moreover, a thorough understanding of the individual components of digital authentication will enable the SAOP to thoroughly assess and mitigate privacy risks either through compliance processes or by other means.

9 Usability Considerations

This section is informative.

This section is intended to raise implementers' awareness of the usability considerations associated with enrollment and identity proofing (for usability considerations for typical authenticator usage and intermittent events, see SP 800-63B, Section 10.

ISO/IEC 9241-11 defines usability as the "extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use." This definition focuses on users, goals, and context of use as the necessary elements for achieving effectiveness, efficiency, and satisfaction. A holistic approach considering these key elements is necessary to achieve usability.

The overarching goal of usability for enrollment and identity proofing is to promote a smooth, positive enrollment process for users by minimizing user burden (e.g., time and frustration) and enrollment friction (e.g., the number of steps to complete and amount of information to track). To achieve this goal, organizations have to first familiarize themselves with their users.

The enrollment and identity proofing process sets the stage for a user's interactions with a given CSP and the online services that the user will access; as negative first impressions can influence user perception of subsequent interactions, organizations need to promote a positive user experience throughout the process.

Usability cannot be achieved in a piecemeal manner. Performing a usability evaluation on the enrollment and identity proofing process is critical. It is important to conduct usability evaluation with representative users, realistic goals and tasks, and appropriate contexts of use. The enrollment and identity proofing process should be designed and implemented so it is easy for users to do the right thing, hard to do the wrong thing, and easy to recover when the wrong thing happens.

From the user's perspective, the three main steps of enrollment and identity proofing are pre-enrollment preparation, the enrollment and proofing session, and post-enrollment actions. These steps may occur in a single session or there could be significant time elapsed between each one (e.g., days or weeks).

General and step-specific usability considerations are described in sub-sections below.

ASSUMPTIONS

In this section, the term "users" means "applicants" or "subscribers."

Guidelines and considerations are described from the users' perspective.

Accessibility differs from usability and is out of scope for this document. Section 508 was enacted to eliminate barriers in information technology and require federal agencies to make their electronic and information technology public content accessible to people with disabilities. Refer to Section 508 law and standards for accessibility guidance.

9.1 General User Experience Considerations During Enrollment and Identity Proofing

This sub-section provides usability considerations that are applicable across all steps of the enrollment process. Usability considerations specific to each step are detailed in Sections 9.2 to 9.4.

- To avoid user frustration, streamline the process required for enrollment to make each step as clear and easy as possible.
- Clearly communicate how and where to acquire technical assistance. For example, provide helpful information such as a link to online self-service feature, chat sessions, and a phone number for help desk support. Ideally, sufficient information should be provided to enable users to answer their own enrollment preparation questions without outside intervention.
- Clearly explain who is collecting their data and why. Also indicate the path their data will take, in particular where the data is being stored.
- Ensure all information presented is usable.
  - Follow good information design practice for all user-facing materials (e.g., data collection notices and fillable forms).
  - Write materials in plain language, typically at a 6th to 8th grade literacy level, and avoid technical jargon. Use active voice and conversational style, logically sequence main points, use the same word consistently rather than synonyms to avoid confusion, and use bullets, numbers, and formatting where appropriate to aid readability.
  - Consider text legibility, such as font style, size, color, and contrast with surrounding background. The highest contrast is black on white. Text legibility is important because users have different levels of visual acuity. Illegible text will contribute to user comprehension errors or user entry errors (e.g., when completing fillable forms).
  - Use sans serif font styles for electronic materials and serif fonts for paper materials.
  - When possible, avoid fonts that do not clearly distinguish between easily confusable characters (such as the letter “O” and the number “0”). This is especially important for enrollment codes.
  - Use a minimum font size of 12 points, as long as the text fits the display.
- Perform a usability evaluation for each step with representative users. Establish realistic goals and tasks, and appropriate contexts of use for the usability evaluation.

9.2 Pre-Enrollment Preparation

This section describes an effective approach to facilitate sufficient pre-enrollment preparation so users can avoid challenging, frustrating enrollment sessions. Ensuring

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

users are as prepared as possible for their enrollment sessions is critical to the overall success and usability of the enrollment and identity proofing process.

Such preparation is only possible if users receive the necessary information (e.g., required documentation) in a usable format in an appropriate timeframe. This includes making users aware of exactly what identity evidence will be required. Users do not need to know anything about IALs or whether the identity evidence required is scored as “fair,” “strong,” or “superior,” whereas organizations need to know what IAL is required for access to a particular system.

To ensure users are equipped to make informed decisions about whether to proceed with the enrollment process, and what will be needed for their session, provide users:

- Information about the entire process, such as what to expect in each step
    - Clear explanations of the expected timeframes to allow users to plan accordingly.
- Explanation of the need for — and benefits of — identity proofing to allow users to understand the value proposition.
- Information on the monetary amount and acceptable forms of payment, and if there is an enrollment fee. Offering a larger variety of acceptable forms of payment allows users to choose their preferred payment operation.
- Information on whether the user’s enrollment session will be in-person or in-person over remote channels, and whether a user can choose. Only provide information relevant to the allowable session option(s).
    - Information on the location(s), whether a user can choose their preferred location, and necessary logistical information for in-person or in-person over remote channels session. Note that users may be reluctant to bring identity evidence to certain public places (bank versus supermarket), as it increases exposure to loss or theft.
    - Information on the technical requirements (e.g., requirements for internet access) for remote sessions.
    - An option to set an appointment for in-person or in-person over remote channels identity proofing sessions to minimize wait times. If walk-ins are allowed, make it clear to users that their wait times may be greater without an appointment.
        - Provide clear instructions for setting up an enrollment session appointment, reminders, and how to reschedule existing appointments.
        - Offer appointment reminders and allow users to specify their preferred appointment reminder format(s) (e.g., postal mail, voicemail, email, text message). Users need information such as date, time, location, and a description of required identity evidence.
- Information on the allowed and required identity evidence and attributes, whether each piece is voluntary or mandatory, and the consequences for not providing the complete set of identity evidence. Users need to know the specific combinations of identity evidence, including requirements specific to a piece of identity evidence (e.g., a raised seal on a birth certificate). This is especially important due to potential difficulties procuring the necessary identity evidence.

- Where possible, implement tools to make it easier to obtain the necessary identity evidence.
- Inform users of any special requirements for minors and people with unique needs. For example, provide users with the information necessary to use trusted referees, such as a notary, legal guardian, or some other form of certified individual that can legally vouch for or act on behalf of the individual (see Section 5.3.4).
- If forms are required:
  - Provide fillable forms before and at the enrollment session. Do not require users to have access to a printer.
  - Minimize the amount of information users must enter on a form, as users are easily frustrated and more error-prone with longer forms. Where possible, pre-populate forms.

9.3 Enrollment Proofing Session

Usability considerations specific to the enrollment session include:

- Remind users at the start of the enrollment session of the enrollment session procedure, without expecting them to remember from the pre-enrollment preparation step. If the enrollment session does not immediately follow pre-enrollment preparation, it is especially important to clearly remind users of the typical timeframe to complete the proofing and enrollment phase.
  - Provide rescheduling options for in-person or in-person over remote channels.
  - Provide a checklist with the allowed and required identity evidence to ensure users have the requisite identity evidence to proceed with the enrollment session, including enrollment codes, if applicable. If users do not have the complete set of identity evidence, they must be informed regarding whether they can complete a partial identity proofing session.
  - Notify users regarding what information will be destroyed, what, if any, information will be retained for future follow-up sessions, and what identity evidence they will need to bring to complete a future session. Ideally, users can choose whether they would like to complete a partial identity proofing session.
  - Set user expectations regarding the outcome of the enrollment session as prior identity verification experiences may drive their expectations (e.g., receiving a driver's license in person, receiving a passport in the mail).
  - Clearly indicate whether users will receive an authenticator immediately at the end of a successful enrollment session, if users have to schedule an appointment to pick it up in person, or if users will receive it in the mail and when they can expect to receive it.
- During the enrollment session, there are several requirements to provide users with explicit notice at the time of identity proofing, such as what data will be retained on record by the CSP (see Section 4.2 and Section 8. for detailed requirements on notices). If CSPs seek consent from a user for additional attributes or uses of their attributes for any purpose other than identity proofing, authentication, authorization or attribute assertions, per 4.2 requirement (5), make CSPs aware that requesting

additional attributes or uses may be unexpected or may make users uncomfortable. If users do not perceive benefit(s) to the additional collection or uses, but perceive extra risk, they may be unwilling or hesitant to provide consent or continue the process. Provide users with explicit notice of the additional requirements.

- Avoid using KBV since it is extremely problematic from a usability perspective. KBV tends to be error-prone and frustrating for users given the limitations of human memory. If KBV is used, address the following usability considerations.
    - KBV questions should have relevance and context to users for them to be able to answer correctly.
    - Phrase KBV questions clearly, as ambiguity can lead to user errors. For example, when asking about a user's social security balance, clearly specify which time period as social security accounts fluctuate.
    - Prior to being asked KBV questions, users must be informed of:
        - The number of allowed attempts and remaining attempt(s).
        - The fact that KBV questions will change on subsequent attempts.
        - During the KBV session, provide timeout inactivity warnings prior to timeout.
- If an enrollment code is issued:
    - Notify users in advance that they will receive an enrollment code, when to expect it, the length of time for which the code is valid, and how it will arrive (e.g., physical mail, SMS, landline telephone, email, or physical mailing address).
    - When an enrollment code is delivered to a user, include instructions on how to use the code, and the length of time for which the code is valid. This is especially important given the short validity timeframes specified in Section 4.4.1.6.
    - If issuing a machine-readable optical label, such as a QR Code (see Section 4.6), provide users with information on how to obtain QR code scanning capabilities (e.g., acceptable QR code applications).
    - Inform users that they will be required to repeat the enrollment process if enrollment codes expire or are lost before use.
    - Provide users with alternative options as not all users are able to use this level of technology. For example, users may not have the technology needed for this approach to be feasible.
- At the end of the enrollment session,
    - If enrollment is successful, send users confirmation regarding the successful enrollment and information on next steps (e.g., when and where to pick up their authenticator, when it will arrive in the mail).
    - If enrollment is partially complete (due to users not having the complete set of identity evidence, users choosing to stop the process, or session timeouts), communicate to users:
        - what information will be destroyed;
        - what, if any, information will be retained for future follow-up sessions;
        - how long the information will be retained; and
        - what identity evidence they will need to bring to a future session.

- If enrollment is unsuccessful, provide users with clear instructions for alternative enrollment session types, for example, offering in-person proofing for users that can not complete remote proofing.

- If users receive the authenticator during the enrollment session, provide users information on the use and maintenance of the authenticator. For example, information could include instructions for use (especially if there are different requirements for first-time use or initialization), information on authenticator expiration, how to protect the authenticator, and what to do if the authenticator is lost or stolen.
- For both in-person and in-person proofing performed over remote channels enrollment sessions, additional usability considerations apply:
  - At the start of the enrollment session, operators or attendants need to explain their role to users (e.g., whether operators or attendants will walk users through the enrollment session or observe silently and only interact as needed).
  - At the start of the enrollment session, inform users that they must not depart during the session, and that their actions must be visible throughout the session.
  - When biometrics are collected during the enrollment session, provide users clear instructions on how to complete the collection process. The instructions are best given just prior to the process. Verbal instructions with corrective feedback from a live operator are the most effective (e.g., instruct users where the biometric sensor is, when to start, how to interact with the sensor, and when the biometric collection is completed).
- Since remote identity proofing is conducted online, follow general web usability principles. For example:
  - Design the user interface to walk users through the enrollment process.
  - Reduce users' memory load.
  - Make the interface consistent.
  - Clearly label sequential steps.
  - Make the starting point clear.
  - Design to support multiple platforms and device sizes.
  - Make the navigation consistent, easy to find, and easy to follow.

9.4 Post-Enrollment

Post-enrollment refers to the step immediately after enrollment but prior to typical usage of an authenticator (for usability considerations for typical authenticator usage and intermittent events, see SP800-63B, Section 10.1-10.3. As described above, users have already been informed at the end of their enrollment session regarding the expected delivery (or pick-up) mechanism by which they will receive their authenticator.

Usability considerations for post-enrollment include:

- Minimize the amount of time that users wait for their authenticator to arrive. Shorter wait times will allow users to access information systems and services more quickly.

- Inform users whether they need to go to a physical location to pick up their authenticators. The previously-identified usability considerations for appointments and reminders still apply.
- Along with the authenticator, give users information relevant to the use and maintenance of the authenticator; this may include instructions for use, especially if there are different requirements for first-time use or initialization, information on authenticator expiration, and what to do if the authenticator is lost or stolen.

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

10 References

This section is informative.

10.1 General References

[A-130] OMB Circular A-130, *Managing Federal Information as a Strategic Resource*, July 28, 2016, available at: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.

[COPPA] *Children's Online Privacy Protection Act of 1998 ("COPPA")*, 15 U.S.C. 6501-6505, 16 CFR Part 312, available at: https://www.law.cornell.edu/uscode/text/15/chapter-91.

[EO 9397] Executive Order 9397, *Numbering System for Federal Accounts Relating to Individual Persons*, November 22, 1943, available at: https://www.ssa.gov/foia/html/EO9397.htm.

[DMF] National Technical Information Service, *Social Security Death Master File*, available at: https://www.ssdmf.com/Library/InfoManage/Guide.asp?FolderID=1.

[E-Gov] *E-Government Act of 2002* (includes FISMA) (P.L. 107-347), December 2002, available at: http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf.

[FBCACP] *X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA)*, Version 2.30, October 5, 2016, available at: https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FBCA_CP.pdf.

[FBCASUP] *FBCA Supplementary Antecedent, In-Person Definition*, July 16, 2009.

[FEDRAMP] General Services Administration, *Federal Risk and Authorization Management Program*, available at: https://www.fedramp.gov/.

[GPG 45] UK Cabinet Office, Good Practice Guide 45, *Identity proofing and verification of an individual*, November 3, 2014, available at: https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual.

[M-03-22] OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 26, 2003, available at: https://georgewbush-whitehouse.archives.gov/omb/memoranda/m03-22.html.

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

[M-04-04] OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, December 16, 2003, available at: https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy04/m04-04.pdf.

[Privacy Act] *Privacy Act of 1974* (P.L. 93-579), December 1974, available at: https://www.justice.gov/opcl/privacy-act-1974.

[Red Flags Rule] 15 U.S.C. 1681m(e)(4), Pub. L. 111-319, 124 Stat. 3457, *Fair and Accurate Credit Transaction Act of 2003*, December 18, 2010, available at: https://www.ftc.gov/sites/default/files/documents/federal_register_notices/identity-theft-red-flags-and-address-discrepancies-under-fair-and-accurate-credit-transactions-act/071109redflags.pdf.

[Section 508] Section 508 Law and Related Laws and Policies (January 30, 2017), available at: https://www.section508.gov/content/learn/laws-and-policies.

10.2 Standards

[Canada] Government of Canada, *Guideline on Identity Assurance*, available at: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=30678&section=HTML.

[ISO 9241-11] International Standards Organization, ISO/IEC 9241-11 *Ergonomic requirements for office work with visual display terminals (VDTs) — Part 11: Guidance on usability*, March 1998, available at: https://www.iso.org/standard/16883.html.

10.3 NIST Special Publications

NIST 800 Series Special Publications are available at: http://csrc.nist.gov/publications/PubsSPs.html. The following publications may be of particular interest to those implementing systems of applications requiring e-authentication.

[SP 800-53] NIST Special Publication 800-53 Revision 4, *Recommended Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (updated January 22, 2015), https://doi.org/10.6028/NIST.SP.800-53r4.

[SP 800-63-3] NIST Special Publication 800-63-3, *Digital Identity Guidelines*, June 2017, https://doi.org/10.6028/NIST.SP.800-63-3.

[SP 800-63B] NIST Special Publication 800-63B, *Digital Identity Guidelines: Authentication and Lifecycle Management*, June 2017, https://doi.org/10.6028/NIST.SP.800-63b.

[SP 800-63C] NIST Special Publication 800-63C, *Digital Identity Guidelines: Assertions and Federation*, June 2017, https://doi.org/10.6028/NIST.SP.800-63c.

[SP 800-157] NIST Special Publication 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*, December 2014, http://doi.org/10.6028/NIST.SP.800-157.