Mon, 30 Jan 2017 13:49:11 -0500

# DRAFT NIST Special Publication 800-63A

# Digital Identity Guidelines

## Enrollment and Identity Proofing Requirements

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

COMPUTER SECURITY

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

# DRAFT NIST Special Publication 800-63A

# Digital Identity Guidelines

## Enrollment and Identity Proofing Requirements

Paul A. Grassi
*Applied Cybersecurity Division*
*Information Technology Laboratory*

James L. Fenton
*Altmode Networks*
*Los Altos, CA*

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
Mary F. Theofanos
*Information Access Division*
*Information Technology Laboratory*

Month TBD 2017

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

## 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. § 3541 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 800-63-3
Natl. Inst. Stand. Technol. Spec. Publ. 800-63-3, xxx pages (MonthTBD 2017)
CODEN: NSPUE2

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 (http://csrc.nist.gov/publications).

## 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 SP 800-63-1 and SP 800-63-2.

## Keywords

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

## Acknowledgements

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. 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.

## Audience

## Compliance with NIST Standards and Guidelines

## Conformance Testing

## Trademark Information

## 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

1. Purpose

2. Introduction

3. Definitions and Abbreviations

4. Identity Assurance Level Requirements

5. Identity Resolution, Validation and Verification

6. Derived Identity

7. Threats and Security Considerations

8. Privacy Considerations

9. Usability Considerations

10. References

# 1. Purpose

*This section is informative.*

This document provides requirements for enrollment and identity proofing of subscribers 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 an individual 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 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., Know Your Customer requirements in the financial community) 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 user executing a transaction, but not know the real life identity of the user. For example, in order to maintain integrity of the service, it may be desirable to know the home ZIP Code of a user for purposes of census taking or petitioning an elected official but where it is not necessary or desirable to know the underlying identity of the person. IALs provide a method for expressing the level of assurance (LOA) associated with attributes established by the CSP during the proofing process.

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

| 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 Identity | Normative |
| 7. Threats and Security Considerations | Informative |
| 8. Privacy Considerations | Informative |
| 9. Usability Considerations | Informative |
| 10. References | Informative |

## 2.1. Expected Outcomes of Identity Proofing

The objective of identity proofing is to:

- 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 authentication process are self-asserted or should be treated as self-asserted.

**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.

**IAL3** - Physical presence is required for identity proofing. Identifying attributes must be verified by an authorized and trained representative of the CSP. As with IAL2, attributes could be asserted by CSPs to RPs in support of pseudonymous identity with verified attributes.

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 an RP needs a valid birthdate but no other personal details, the RP should leverage a CSP to request just the birthdate of the subscriber. It is preferred for the RP to ask the CSP for an attribute claim. For example, if an RP needs to know if a claimant is older than 18 they should request a Boolean value, not the entire birthdate in order to evaluate age.

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 is given in Section 4 and Section 5.

# 3. Definitions and Abbreviations

*This section is informative.*

There is a wide variety of terms used in the area of digital identity. While the definitions of many terms are consistent with earlier versions of Special Publication (SP) 800-63, some have changed in this revision. Since there is no single, consistent definition of many of these terms, careful attention to how the terms are defined here is warranted.

The definitions in this section are primarily those that are referenced in this document. Refer to the other documents in the SP 800-63 document family for additional definitions and abbreviations specific to their content.

### Address of Record

The validated and verified location (physical or digital) where an individual can receive communications using approved mechanisms.

### Applicant

A subject undergoing the processes of registration and identity proofing.

### Asymmetric Keys

Two related keys, consisting of a public key and a private key, that are used to perform complementary operations such as encryption and decryption or signature verification and generation.

### Attack

An attempt by an unauthorized individual to defeat security controls. For example, to cause a credential service provider to register an impostor as the subscriber.

### Attacker

A party who acts with malicious intent to compromise an information system.

### Attribute

A quality or characteristic ascribed to or associated with someone or something.

### Attribute Claim

A statement asserting a property of a subscriber without necessarily containing identity information, independent of format. For example, for the attribute ‘birthday’, a claim could be ‘older than 18’ or ‘born in December’.

### Attribute Value

A complete statement asserting a property of a subscriber, independent of format. For example, for the attribute ‘birthday’, a value could be ‘12/1/1980’ or ‘December 1, 1980’.

### Authentication

The process of establishing confidence in the identity of users or information systems.

### Authentication Protocol

A defined sequence of messages between a claimant and a verifier that demonstrates that the claimant has possession and control of one or more valid authenticators to establish his/her identity. Secure authentication protocols also demonstrate to the claimant that he or she is communicating with the intended verifier.

### Authenticator

Something that a claimant possesses and controls that is used to authenticate the claimant’s identity. In previous editions of SP 800-63, this was referred to as a *token*.

### Authenticity

The property that data originated from its purported source.

### Authoritative Source

An entity that has access to, or verified copies of, a sufficient amount of accurate information from an issuing source such that a CSP can confirm the validity of the identity evidence supplied by an applicant during identity proofing. An issuing source may also be an authoritative source. Often, authoritative sources are determined by a policy decision of the agency or CSP before they can be used in the validation phase of identity proofing.

### Biometrics

Automated recognition of individuals based on their behavioral and biological characteristics.

In this document, biometrics may be used to unlock authenticators and prevent repudiation of registration.

### Claimant

A party whose identity is to be verified using one or more authentication protocols.

### Claimed Address

The physical location asserted by a subject at which they can be reached. It includes the residential street address of an individual and may also include the mailing address of the individual.

For example, a person with a foreign passport, living in the U.S., will need to give an address when going through the identity proofing process. This address would not be an “address of record” but a “claimed address.”

### Claimed Identity

A declaration of unvalidated and unverified personal attributes by the applicant.

### Credential

An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to an authenticator possessed and controlled by a subscriber.

While common usage often assumes that the credential is maintained by the subscriber, this document also uses the term to refer to electronic records maintained by the CSP which establish a binding between the subscriber’s authenticator and identity.

### Credential Service Provider (CSP)

A trusted entity that issues or registers subscriber authenticators and issues electronic credentials to subscribers. The CSP may encompass verifiers that it operates. A CSP may be an independent third party, or may issue credentials for its own use.

### Derived Credential

A credential issued based on proof of possession and control of an authenticator associated with a previously issued credential, so as not to duplicate the identity proofing process.

### Digital Authentication

The process of establishing confidence in user identities electronically presented to an information system. In previous editions of SP 800-63, this was referred to as *Electronic Authentication*.

### Digital Signature

An asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature. Digital signatures provide authenticity protection, integrity protection, and non-repudiation but not confidentiality protection.

### Electronic Authentication (E-Authentication)

See *Digital Authentication*.

### Enrollment

The process through which an applicant applies to become a subscriber of a CSP and an RA validates the identity of the applicant on behalf of the CSP.

### Identity

A set of attributes that uniquely describe a person within a given context.

### Identity Assurance Level (IAL)

A category that conveys the degree of confidence that the applicant's claimed identity is their real identity.

### Identity Proofing

The process by which a CSP collects and verifies information about a person for the purpose of issuing credentials to that person.

### Issuing Source

An authority that is responsible for the generation of data or documents that can be used as identity evidence.

### Knowledge Based Verification (KBV)

Identity verification method based on knowledge of private information associated with the claimed identity. This is often referred to as knowledge based authentication (KBA) or knowledge based proofing (KBP).

### Network

An open communications medium, typically the internet, that is used to transport messages between the claimant and other parties. Unless otherwise stated, no assumptions are made about the security of the network; it is assumed to be open and subject to active (i.e., impersonation, man-in-the-middle, session hijacking) and passive (i.e., eavesdropping) attack at any point between the parties (e.g., claimant, verifier, CSP or RP).

### Personally Identifiable Information (PII)

As defined by OMB Circular [A-130], Personally Identifiable Information is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

### Practice Statement

A formal statement of the practices followed by the parties to an authentication process (e.g., CSP or verifier). It usually describes the policies and practices of the parties and can become legally binding.

### Protected Session

A session wherein messages between two participants are encrypted and integrity is protected using a set of shared secrets called session keys.

A participant is said to be *authenticated* if, during the session, they prove possession of one or more authenticators in addition to the session keys, and if the other party can verify the identity associated with the authenticator(s). If both participants are authenticated, the protected session is said to be *mutually authenticated*.

### Pseudonym

A name other than a legal name.

### Public Key

The public part of an asymmetric key pair that is used to verify signatures or encrypt data.

### Remote

(*As in remote authentication or remote transaction*) An information exchange between network-connected devices where the information cannot be reliably protected end-to-end by a single organization's security controls.

Note: Any information exchange across the Internet is considered remote.

### Social Engineering

The act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust.

### Subscriber

A subject who has had their credential bound to an authenticator by a CSP.

### Token

See *Authenticator*.

### Trust Anchor

A public or symmetric key that is trusted because it is directly built into hardware or software, or securely provisioned via out-of-band means, rather than because it is vouched for by another trusted entity (e.g. in a public key certificate).

### Valid

In reference to an ID, the quality of not being expired or revoked.

### Virtual In-Person Proofing

A remote identity proofing process that employs physical, technical and procedural measures that provide sufficient confidence that the remote session can be considered equivalent to a physical, in-person identity proofing process.

# 4. Identity Assurance Level Requirements

*This section is normative.*

This document describes the common pattern in which a subject (referred to as an applicant at this stage) undergoes an identity proofing and enrollment process in which their identity evidence and attributes are collected, uniquely resolved to a single identity within a given population or context, then validated and verified. A CSP may then bind these attributes to an authenticator (described in [SP 800-63B] (sp800-63b.html)).

The only outcome of identity proofing is to ensure that the applicant is who they claim to be. This includes presentation, validation, and verification of the minimum attributes necessary to accomplish identity proofing. As an example, such core attributes, to the extent they are the minimum necessary, could include:

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

It is permissible for the CSP to collect additional information in the process of identity proofing an applicant, provided validation and verification follow the requirements contained herein, and the applicant explicitly consents to the CSP collecting and storing the attributes.

## 4.1. Process Flow

Figure 4-1 outlines the basic flow for Identity Proofing and Enrollment, to include the corresponding sections with normative requirements.

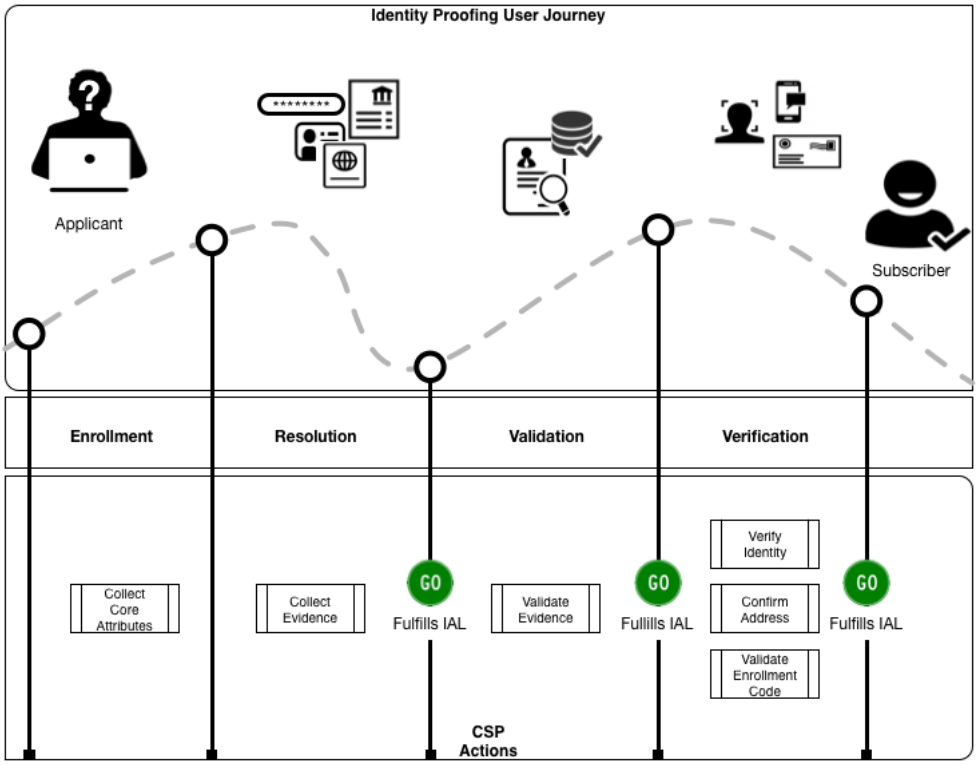


**Figure 4-1. The Identity Proofing Process**

## 4.2. General Requirements

Table 4-1 lists strict adherence to M-04-04 LOAs, mapping the corresponding IALs.

**Table 4-1. Legacy M-04-04 IAL Requirements**

| M-04-04 Level of Assurance (LOA) | Identity Assurance Level (IAL) |
|---|---|
| 1 | 1 |
| 2 | 2 |
| 3 | 2 |

| M-04-04 Level of Assurance (LOA) | Identity Assurance Level (IAL) |
|---|---|
| 4 | 3 |

However, Table 4-2 shows the expanded set of IALs that are allowable to meet M-04-04 LOAs. Agencies SHALL select the corresponding IAL based on the impact of a proofing failure. Agencies SHALL consider the privacy risks of stronger identity proofing and SHALL NOT select an IAL that is higher than necessary for the business purpose of the digital service.

**Table 4-2. Recommended M-04-04 IAL Requirements**

| M-04-04 Level of Assurance | Identity Assurance Level |
|---|---|
| 1 | 1 |
| 2 | 1 or 2 |
| 3 | 1 or 2 |
| 4 | 1, 2 or 3 |

The following requirements apply to any CSP performing identity proofing at IAL2 or 3.

1. Identity proofing SHALL NOT be performed to determine suitability/entitlement to gain access to services or benefits.
2. The CSP SHOULD NOT collect the SSN unless it is necessary for performing identity resolution and cannot be accomplished by collection of another attribute or combination of attributes.
3. Collection of PII SHALL be limited to the minimum necessary to validate the existence of the claimed identity and associate the claimed identity to the applicant providing identity evidence based on best available practices for appropriate identity resolution, validation, and verification.
4. The CSP SHALL provide explicit notice at the time of collection to the applicant regarding the purpose for collecting and maintaining a record of the attributes necessary for identity proofing, including whether the such attributes are voluntary or mandatory in order to complete the identity proofing transactions and the consequences for not providing the attributes.
5. The CSP SHALL NOT use attributes collected and maintained in the identity proofing process for any purpose other than identity proofing, authentication, authorization 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 a condition of the service.
6. The CSP SHALL provide effective mechanisms for redress of applicant complaints or problems arising from the identity proofing. These mechanisms SHALL be easy for applicants to find and access.
7. 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.
8. The CSP SHALL maintain a record 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 privacy risk assessment 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: Specific National Archives and Records Administration (NARA) records retention schedules may apply.
9. All PII collected as part of the enrollment process SHALL be protected to ensure confidentiality, integrity, and attribution of the information source.
10. The entire proofing transaction, including transactions that involve a third party, SHALL occur over an Authenticated Protected Channel.
11. The CSP SHOULD obtain additional confidence in remote identity proofing using fraud mitigation measures, for example inspecting geolocation, examining the device characteristics of the applicant, evaluating behavioral characteristics, or checking vital statistic repositories such as the Death Master File (https://www.ssdmf.com/Library/InfoManage/Guide.asp?FolderID=1), so long as any additional mitigations do not substitute for the mandatory requirements contained herein and the CSP SHALL conduct a privacy risk assessment of these mitigation measures. Such assessments SHOULD include any privacy risk mitigations (e.g., limited retention, use limitations, notice, etc.) or other technological mitigations (e.g. cryptography).

12. 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.
13. 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:

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

b) The agency SHALL publish a System of Records Notice (SORN) to cover such collections, as applicable. c) The agency SHALL consult with their SAOP to conduct an analysis to determine whether the collection of PII to conduct identity proofing triggers the requirements of the E-Government Act of 2002. d) The agency SHALL publish a Privacy Impact Assessment (PIA) to cover such collections, as applicable.

## 4.3. Identity Assurance Level 1

The CSP SHALL NOT proof applicants. Applicants MAY self-assert zero or more attributes to the CSP.

## 4.4. Identity Assurance Level 2

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 MAY exceed these requirements.

A CSP SHOULD implement identity proofing in accordance with 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

#### 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. See Section 5.1 for general resolution requirements.

#### 4.4.1.2. Evidence Requirements

See Section 5.2, Identity Evidence Validation for more information on acceptable identity evidence.

- One (1) piece of SUPERIOR or STRONG evidence **if** the issuing source of the evidence, during its identity proofing event, confirmed the claimed identity by collecting two (2) or more forms of SUPERIOR or STRONG evidence; **OR**
- Two (2) pieces of STRONG evidence; **OR**
- One (1) piece of STRONG evidence plus two (2) pieces of ADEQUATE evidence.

#### 4.4.1.3. Validation Requirements

See Section 5.2, Identity Evidence Validation for more information on acceptable identity evidence.

- Each piece of evidence SHALL 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.
- Validation against a third party data service SHALL NOT be used for more than one piece of presented identity evidence.

#### 4.4.1.4. Verification Requirements

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

At a minimum, the applicant must be verified by a process that is able to achieve a strength of STRONG.

#### 4.4.1.5. Presence Requirements

The CSP SHOULD perform identity proofing in-person. The CSP MAY perform remote identity proofing. The CSP SHOULD offer both in-person and remote proofing.

#### 4.4.1.6. Address Confirmation

- The CSP SHALL confirm address of record through validation of the address contained on any supplied, valid piece of identity evidence.
- Self-asserted address data that has not been confirmed in records SHALL NOT be used for confirmation.
- **If CSP performed in-person proofing:**
  - The CSP SHOULD send a notification of proofing to the address of record.
  - 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
- **If the CSP performed remote proofing:**
  - The CSP SHALL send an enrollment code to an address of record of the applicant.
  - The applicant SHALL present a valid enrollment code to complete the identity proofing process.
  - The CSP SHOULD send the enrollment code to the physical mailing address that has been verified in records. The CSP MAY send the enrollment code to a mobile telephone (SMS or voice), landline telephone, or email that has been verified in records.
  - If the enrollment code is also intended to be an authentication factor, it SHALL be reset upon first use.
  - Enrollment codes sent by means other than physical mail SHALL be valid for a maximum of 10 minutes; those sent to a postal address of record SHALL be valid for a maximum of 7 days but MAY be made valid up to 21 days via an exception process to accommodate addresses outside the direct reach of the U.S. Postal Service.
  - If delivery of the enrollment code was sent to an address of record that is not physical mail, the CSP SHALL send notification of proofing to a different address of record than the destination of the enrollment code. For example, if the CSP sends an enrollment code to a mobile phone of record, a notification of proofing will be sent to the physical address in records or obtained from validated and verified evidence, such as a driver's license.

#### 4.4.1.7. Biometric Collection

The CSP MAY collect biometrics for the purposes of non-repudiation and re-proofing. See [Section 5.2.3 of SP 800-63B] (sp800-63b.html#biometric_use) for more detail on biometric collection.

#### 4.4.1.8. Security Controls

The CSP SHOULD employ appropriately tailored security controls from the moderate baseline of security controls defined in [SP 800-53] or equivalent industry standard and SHOULD ensure that the minimum requirements associated with the *moderate* baseline 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 enrollee. See Section 5.3.4. for more details.

## 4.5. Identity Assurance Level 3

IAL3 adds additional rigor to the steps required at IAL2, to include providing further evidence of superior strength, and is subjected 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. In addition, identity proofing at IAL3 is performed in-person. See Section 5.3.3 for more details. A CSP MAY exceed these requirements.

### 4.5.1. Resolution Requirements

Collection of PII SHALL be limited to the minimum necessary to resolve to a unique identity record. See Section 5.1 for general resolution requirements.

### 4.5.2. Evidence Requirements

See Section 5.2, Identity Evidence Validation for more information on acceptable identity evidence.

- Two (2) or more pieces of SUPERIOR evidence; **OR**
- One (1) piece of SUPERIOR evidence and one (1) piece of STRONG evidence **if** the issuing source of the evidence, during its identity proofing event, confirmed the claimed identity by collecting two (2) or more forms of SUPERIOR or STRONG evidence; **OR**
- Two (2) pieces of STRONG evidence plus one (1) piece of ADEQUATE evidence.

### 4.5.3. Validation Requirements

See Section 5.2, Identity Evidence Validation for more information on acceptable identity evidence.

- 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 evidence will be validated at a strength of STRONG.
- Validation against a third party data service SHALL only be used for one piece of presented identity evidence.

#### 4.5.4. Verification Requirements

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

- At a minimum, the applicant must be verified by a process that is able to achieve a strength of SUPERIOR.

#### 4.5.5. Presence Requirements

All identity proofing steps SHALL be performed in person. See Section 5.3.3 for more details.

Remote proofing SHALL NOT be allowed.

#### 4.5.6. Address Confirmation

- The CSP SHALL confirm address of record through validation of the address contained on any supplied, valid piece of identity evidence.
- Self-asserted address data SHALL NOT be used for confirmation.
- A notification of proofing SHALL be sent to the confirmed address of record.
- 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) the purposes of non-repudiation and re-proofing. See [Section 5.2.3 of SP 800-63B] (sp800-63b.html#biometric_use) for more detail on biometric collection.

#### 4.5.8. Security Controls

The CSP SHOULD employ appropriately tailored security controls from the High baseline of security controls defined in [SP 800-53] or an equivalent industry standard and SHOULD ensure that the minimum requirements associated with the *high* baseline are satisfied.

## 4.6. Enrollment Code

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

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

- Minimally, a random six character alphanumeric. For example, a code generated using a secure random cryptographic algorithm or a serial number for a physical hardware authenticator.
- 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 4-3 summarizes the requirements for each of the authenticator assurance levels:

**Table 4-3. IAL Requirements Summary**

| Requirement | IAL1 | IAL2 | IAL3 |
|---|---|---|---|
| Presence | No requirements | In-person and remote | In-person |
| Resolution | No requirements | The minimum attributes necessary to accomplish identity resolution. KBV may be used for added confidence. | |

| Requirement | IAL1 | IAL2 | IAL3 |
|---|---|---|---|
| Evidence | Identity evidence is not required | Two (2) pieces of STRONG evidence<br>**OR**<br>One (1) piece of STRONG evidence plus two (2) pieces of ADEQUATE evidence | One (1) piece of SUPERIOR evidence plus one (1) piece of STRONG evidence<br>**OR**<br>Two (2) pieces of STRONG evidence plus one (1) piece of ADEQUATE evidence |
| Validation | No validation of evidence is required | - 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 evidence will be validated at a strength of STRONG.<br><br>- Validation against a third party data service SHALL only be used for one piece of presented identity evidence. | Same as IAL2. |
| Verification | No verification of identity is required | - At a minimum, the applicant must be verified by a process that is able to achieve a strength of STRONG. | - At a minimum, the applicant must be verified by a process that is able to achieve a strength of SUPERIOR. |
| Address Confirmation | No requirements for address confirmation | - Self-asserted address data SHALL NOT be used for confirmation.<br>- An enrollment code consisting of at least 6 random digits SHALL be included in address confirmation.<br>- May be sent to a mobile telephone (SMS or voice), landline telephone, email, or physical mailing address obtained from records.<br>- If the enrollment code is also intended to be an authentication factor, it SHALL be reset upon first use.<br>- Enrollment codes sent by means other than physical mail SHALL be valid for a maximum of 10 minutes; those sent to a postal address of record SHALL be valid for a maximum of 7 days but MAY be made valid up to 21 days via an exception process to accommodate addresses outside the direct reach of the U.S. postal service.<br>- A notification of proofing SHALL be sent via a different address of record than the destination of the enrollment code | - The CSP SHALL confirm address of record through validation of the address contained on any supplied, valid piece of identity evidence. - Self-asserted address data SHALL NOT be used for confirmation. - A notification of proofing SHALL be sent to the confirmed address of record. |
| Biometric Collection | No | Yes | Yes |
| Security Controls | N/A | [SP 800-53] Moderate Baseline (or equivalent) | [SP 800-53] High Baseline (or equivalent) |

# 5. Identity Resolution, Validation, and Verification

*This section is normative.*

This section lists the steps a CSP SHALL follow to identity proof an individual to meet the requirements for each IAL. 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 a 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 among 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 could 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, authoritative records, and third party records. 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 referenced above.
2. KBV (sometimes referred to as KBA 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 Validation

The goal of identity validation is to collect from the applicant the most appropriate identity evidence (e.g., a passport or driver's license) 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 Characteristic Requirements

This section provides requirements on the properties and qualities of identity evidence at a given IAL.

#### 5.2.1.1. Scoring of Identity Evidence

Table 5-1 lists qualities, 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 properties listed.

**Table 5-1. Properties of Identity Evidence**

| Strength | Properties of Identity Evidence |
|---|---|
| Unacceptable | No compliance identity evidence provided. |
| Weak | - The issuing source of the evidence did not perform identity proofing.<br><br>- The issuing process for the evidence means that it can reasonably be assumed to have been delivered into the possession of a subject.<br><br>- The evidence contains at least one reference number that uniquely identifies itself or the subject to whom it relates.<br>**OR**<br>- The issued Identity Evidence contains a photograph, image, or biometric of the person to whom it relates. |

| Strength | Properties of Identity Evidence |
|---|---|
| Fair | - The issuing source of the evidence confirmed the claimed identity through an identity proofing process.<br><br>- The issuing process for the evidence means that it can reasonably be assumed to have been delivered into the possession of the subject to whom it relates.<br><br>- The evidence:<br>- contains at least one reference number that uniquely identifies the subject to whom it relates.<br>**OR**<br>- contains a photograph, image, or biometric of the person to whom it relates.<br>**OR**<br>- can have ownership confirmed through KBV.<br><br>- Where the evidence includes digital information, that information is protected using 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.<br><br>- Where the evidence includes physical security features, it requires proprietary knowledge to be able to reproduce it.<br><br>-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 true identity of the subject. 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)<br><br>- The issuing process for the evidence ensured that it was delivered into the possession of the subject to whom it relates.<br><br>-The issued evidence contains at least one reference number that uniquely identifies the subject to whom it relates.<br><br>- The applicant's full name on the issued evidence must be the name that the identity was officially known at the time of issuance. Pseudonyms, aliases, and initials for first given name and surname are not permitted.<br><br>- The issued evidence contains a photograph, image, or biometric of the person to whom it relates.<br>**OR**<br>- The applicant proves possession of an AAL2 authenticator bound to an IAL2 identity, at a minimum.<br><br>- Where the issued evidence includes digital information, that information is protected using 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.<br><br>-Where the issued evidence contains physical security features, it requires proprietary knowledge and proprietary equipment to be able to reproduce it.<br><br>- The evidence is unexpired. |

| Strength | Properties of Identity Evidence |
|---|---|
| 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 true identity of the subject. Such procedures shall be subject to recurring oversight by regulatory or publicly accountable institutions.<br><br>- The issuing source visually identified the applicant and performed further checks to confirm the existence of that identity.<br><br>- The issuing process for the evidence ensured that it was delivered into the possession of the subject to whom it relates.<br><br>- The evidence contains at least one reference number that uniquely identifies subject to whom it relates.<br><br>- The applicant's name on the evidence must be the name that the identity was officially known at the time of issuance. Pseudonyms, aliases, or initials for first given or surname are not permitted.<br><br>- The evidence contains a photograph/image of the person to whom it relates.<br><br>- The evidence contains a biometric of the person to whom it relates.<br><br>- The evidence includes digital information, the information is protected using proprietary cryptographic methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the issuing source to be confirmed.<br><br>- The evidence includes physical security features that requires proprietary knowledge and proprietary equipment to be able to reproduce it.<br><br>- The evidence is unexpired. |

### 5.2.2. Validating Identity Evidence

Once identity evidence is obtained by the CSP, 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.
- The information is correct.
- The information relates to a real-life subject.

#### 5.2.2.1. Methods to Perform Identity Evidence Validation

Table 5-2 lists qualities, ranging from unacceptable to superior, of identity validation that is 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 | - The evidence:<br>- details have been confirmed as valid by comparison with information held or published by the issuing source.<br>**OR**<br>- has been confirmed as genuine using appropriate equipment, confirming the integrity of physical security features and lack of fraudulent modification.<br>**OR**<br>- The evidence has been confirmed as genuine by trained personnel.<br>**OR**<br>- The issued evidence has been confirmed as genuine by confirmation of the integrity of cryptographic security features. |

| Strength | Method(s) performed by the CSP |
|---|---|
| Strong | - The evidence has been confirmed as genuine:<br>- using appropriate equipment, confirming the integrity of physical security features and lack of fraudulent modification.<br>**OR**<br>- by trained personnel and appropriate equipment, confirming the integrity of the physical security features and lack of fraudulent modification<br>**OR**<br>- by confirmation of the integrity of cryptographic security features.<br><br>- All personal details and evidence details have been confirmed as valid by comparison with information held or published by the issuing source. |
| Superior | - The evidence has been confirmed as genuine by trained personnel and appropriate equipment including the integrity of any physical and cryptographic security features.<br><br>- 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. |

## 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.

**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:<br>- KBV. See Section 5.3.2 for more details.<br>**OR**<br>- a physical comparison of the applicant to the identity evidence. Physical comparison performed remotely SHALL include presentation attack detection as specified in [SP 800-63B, Section 5.2.3] (sp800-63b.html/#biometric_use).<br>**OR**<br>- biometric comparison of the applicant to the identity evidence. Biometric comparison performed remotely SHALL adhere to the appropriate requirements as specified in [SP 800-63B, Section 5.2.3] (sp800-63b.html/#biometric_use). |
| Strong | - The applicant's ownership of the claimed identity has been confirmed by<br>- physical comparison, using appropriate equipment, to a photograph or image. Physical comparison performed remotely SHALL include presentation attack detection as specified in [SP 800-63B, Section 5.2.3] (sp800-63b.html/#biometric_use).<br>**OR**<br>- biometric comparison, using appropriate equipment, of the applicant to the identity evidence. Biometric comparison performed remotely SHALL adhere to the appropriate requirements as specified in [SP 800-63B, Section 5.2.3] (sp800-63b.html/#biometric_use). |
| Superior | - The applicant's ownership of the claimed identity has been confirmed by biometric comparison, using appropriate equipment, of the applicant to the identity evidence. Biometric comparison performed remotely SHALL adhere to the appropriate requirements as specified in [SP 800-63B, Section 5.2.3] (sp800-63b.html/#biometric_use). |

The CSP MAY use KBV to verify the identity of an applicant provided the requirements in Section 5.3.2 are met.

### 5.3.2. Knowledge Based Verification Requirements

The following requirements apply to the identity verification steps for IAL2 and 3. There are no restrictions for the use of KBV for identity resolution.

- KBV SHALL NOT be used if the CSP is not, or does not maintain a relationship with, an authoritative source.

- The CSP SHALL only use information that is expected to be known only to the applicant and the source, to include any information needed to begin the KBV process. Information accessible freely or for any fee in the public domain SHALL NOT be used.
- The CSP SHALL allow a resolved, validated, or verified identity to opt-out of KBV and leverage another process for verification.
- KBV SHOULD be based on multiple data sources.
- The CSP SHOULD perform KBV by verifying knowledge of recent transactional history that the CSP is a participant in. 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.
- 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:
  - The CSP SHALL require a minimum of four KBV questions with each requiring a correct answer to successfully complete the KBV step.
  - The CSP SHOULD require a free form response to a KBV question. The CSP MAY allow multiple choice answers, however, if multiple choice answer are provided, the CSP SHALL require a minimum of four answer options per question.
  - 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.
  - The CSP MAY use KBV to verify an applicant's identity against only one piece of validated identity evidence.
  - The CSP SHALL NOT present the majority of KBV questions as diversionary. For example, answers to KBV questions that include 'None of the Above', 'Not Applicable (N/A)', or similar to be regarded as correct.
  - The CSP SHOULD NOT ask the same KBV questions in subsequent attempts.
  - 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.
  - The CSP SHALL NOT use KBV questions for which the answers do not change regularly over a period of time (e.g., What was your first car?).
  - The CSP SHALL ensure that any KBV approach 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.
  - 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 session.

### 5.3.3. In-person Proofing Requirements

#### 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] (sp800-63b.html/#biometric_use) apply.

#### 5.3.3.2. Requirements for In-person Proofing Performed Over Remote Channels

It is possible for a CSP to achieve the security and confidence comparable to in-person proofing over remote channels. The following requirements establish comparability between in-person transactions where the enrollee in the same physical location as the CSP or when the enrollee is remote to the CSP.

Virtual in-person identity proofing and enrollment transaction 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 transaction, from which the applicant SHALL NOT depart during the identity proofing session. 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 enrollment and identity proofing session.
3. The CSP SHALL require all actions taken by the applicant during the enrollment and identity proofing process to be clearly visible to the remote operator. The operator SHALL direct the applicant, as required, to remove any doubt in the proofing process.
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 that are in the entire field of view of the camera and the remote, live operator.

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. A CSP MAY have an attendant participate in-person, at the same physical location as the applicant, for the entirety of the enrollment and identity proofing session.
7. 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 the concourse of a shopping mall.
8. The CSP SHALL ensure that all communications take place over a mutually-authenticated encrypted session.

#### 5.3.4. Trusted Referee Requirements

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.

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.

The CSP SHALL determine the minimum evidence required to bind the relationship between the trusted referee and the applicant.

The CSP MAY perform re-proofing of the subscriber on a regular basis, as defined by CSP policy, with the goal of satisfying the requirements of Section 4.4.1.

#### Considerations for Minors

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, and other laws, as applicable.

Minors under age 13 require additional special considerations under COPPA, and other laws, to which the CSP SHALL ensure compliance, as applicable.

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 800-63B, Section 6.1, Authenticator Binding (https://pages.nist.gov/800-63-3/sp800-63b.html#binding) for instructions on binding authenticators to subscribers.

# 6. Derived Identity

*This section is normative.*

Derived identity (formerly known as derived credentials in previous versions of SP 800-63) is 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 that are bound to the existing, identity proofed record, or credential. Since it is beneficial to the individual and the CSP to minimize the number of times the identity proofing process is repeated, deriving identity is accomplished by proving possession and successful authentication of the primary authenticator that is bound to the original, proofed digital identity.

The definition of derived in this section does *not* infer that an authenticator is cryptographically tied to a primary authenticator, for example deriving a key from another key.

There are two specific use cases for deriving identity:

1. A *claimant* seeks to obtain a secondary authenticator, bound to a proofed identity record, for use only within the limits and authorizations of the primary authenticator. For example, this could be a derived PIV credential in federal use cases. *This section covers this use case.*
2. An *applicant* seeks to obtain an authenticator, bound to a proofed identity record, from a CSP that did not proof the individual or issue the original/primary authenticator and credential. For example, if an applicant wants to switch CSPs and/or have another authenticator at 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.*

For the first use case above, the management of authenticators issued by deriving identity is similar to that described in Section 6.1.2. Post-Enrollment Binding (https://pages.nist.gov/800-63-3/sp800-63b.html#post-enroll-bind); however, authenticators considered in this section are only issued to a subject that is authorized to have a primary authenticator. Once the primary authenticator has been revoked, it is possible that all authenticators bound to the identity will also be revoked.

> Note: In some cases, like the PIV smartcard, the authenticator *and* credential will be revoked. The individual will typically surrender their authenticator (i.e. the PIV), but since the credential has also been revoked, the PIV is unusable regardless of whether the individual surrenders it or not. In many consumer use cases, rendering the authenticator unusable is not a desirable outcome. The individual may provide their own authenticator(s), so the CSP will revoke the credential the authenticator is bound to, such that authentication is no longer possible with that CSP; but the authenticator will can be used by the individual at other CSPs.

The following requirements detail how a CSP determines the existence of an enrolled, proofed identity record (i.e. the credential) prior to issuance of a secondary authenticator. It also lists lifecycle management requirements to keep new authenticators in sync with the primary authenticator.

## 6.1. General Requirements

1. The IAL of the credential bound to the new authenticator SHALL be at or below the primary IAL. In most cases the IALs are expected to be the same in order to benefit from the reuse of the original identity proofing event(s).
2. Before issuance, the CSP SHALL verify the primary authenticator status. The CSP SHALL NOT issue an additional authenticator if status indicates any type of termination, disablement, revocation, or expiration.
3. Before issuance, the CSP SHALL verify that the primary authenticator is possessed and controlled by the claimant.
4. The new authenticator SHALL be valid only as long as the subscriber is authorized to hold the primary authenticator.
5. The CSP SHALL record the details of the primary authenticator used as the basis for derived authenticator issuance.
6. The CSP SHOULD set the expiration of the new authenticator to the expiration, if any, of the primary authenticator. There are instances where the new authenticator need not be directly tied to the expiration of the primary authenticator as the new authenticator can provide authentication services in its place, for example, while the expiring primary credential is being replaced.
7. The new authenticator type MAY be any type allowable at any AAL, regardless of the AAL of the primary authenticator or the IAL of the bound credential.

## 6.2. AAL2 Requirements

- The CSP SHOULD check the status of the primary authenticator weekly in order to keep all authenticators in sync.

## 6.3. AAL3 Requirements

1. The CSP SHOULD verify in-person that a claimant possesses, controls and can successfully authenticate using the primary authenticator(s).

2. The CSP SHOULD perform in-person issuance. This is important if the CSP needs to explicitly provision the authenticator to a trusted device and in-person is the only mechanism to ensure delivery and assurance.
3. The CSP SHOULD check the status of the primary authenticator daily in order to keep all authenticators in sync.
4. The CSP SHALL obtain and verify a copy of a biometric recorded when the primary authenticator was issued. An example of such a biometric is the signed biometric data object, however if the biometric reference is not available from the primary AAL3 authenticator, it may be obtained elsewhere, as long as its authenticity is assured.
5. The CSP SHALL compare a fresh biometric sample from the applicant to the reference biometric retained when the primary AAL3 authenticator was issued.
6. The CSP SHALL determine that the primary authenticator meets all AAL3 requirements.

# 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 (CSPs). This section focuses on addressing impersonation threats. Infrastructure threats are addressed by normal computer security controls (e.g., separation of duties, record keeping, independent audits) and are outside the scope of this document.

The 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 |
| | Repudiation of enrollment | A subscriber denies enrollment, claiming that they did not enroll with the CSP. |
| | Social engineering | A malicious applicant manipulates an individual at the CSP responsible for performing some or all of the identity proofing in order to be enrolled as another individual. |
| Issuance | Disclosure | A key created by the CSP for a subscriber is copied by an attacker as it is transported from the CSP to the subscriber during authenticator issuance. |
| | Tampering | A new password created by the subscriber is modified by an attacker as it is being submitted to the CSP during the credential issuance phase. |
| | Unauthorized issuance | A person claiming to be the subscriber (but in reality is not the subscriber) is issued credentials for that subscriber. |
| | Social engineering | A malicious person manipulates an individual at the CSP responsible for issuance in order to obtain a credential bound to another, valid subscriber. |

## 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 to prove who carried out an impersonation. At each level, methods are employed to determine that a person with the claimed identity exists, that the applicant is the person who is 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 |
|---|---|---|
| Enrollment | Falsified identity proofing evidence | CSP validates physical security features of presented evidence. |
| | | CSP validates personal details in the evidence with the issuer or other authoritative source. |
| | Fraudulent use of another's identity | CSP verifies identity evidence or biometric of applicant against information on evidence or obtained from issuer or other authoritative source. |
| | | 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 in achieving a higher level of confidence in the identity of the applicant. |

| Activity | Threat/Attack | Mitigation Strategy |
|---|---|---|
| | Repudiation of enrollment | Have the applicant sign a form acknowledging participation in the enrollment activity. |
| | Social engineering | Duplicate records check. |
| Issuance | Disclosure | Issue the authenticator in person, physically mail it in a sealed envelope to a secure location, or use a protected session to send the authenticator electronically. |
| | Tampering | Issue credentials in person, physically mailing storage media in a sealed envelope, or through the use of a communication protocol that protects the integrity of the session data. |
| | | Establish a procedure that allows the Subscriber to authenticate the CSP as the source of any authenticator and credential data that he or she may receive. |
| | Unauthorized issuance/Social engineering | Establish procedures to ensure that the individual who receives the authenticator is the same individual who participated in the enrollment procedure. |
| | | Implement a dual-control issuance process that ensures two independent individuals shall cooperate in order to issue an authenticator. |

# 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 (3) permits only the collection of 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. Collection of unnecessary PII can create confusion as to why information is being collected if it is not being used for the identity proofing service and leads to concerns about invasiveness or overreach which can lead to loss of applicant trust. In addition, the retention of any PII 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 (2) does not permit the CSP to collect the SSN unless it is necessary for performing identity resolution because it cannot be accomplished by collection of another attribute or combination of attributes. Unnecessary use of the SSN may be particularly vulnerable to misuse and can place the applicant at risk of harm such as through identity theft. The SSN may serve to 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 though that evidence requirements at the higher IALs preclude the usage of the SSN or the Social Security Card as acceptable identity evidence.

The initial requirement in Executive Order (EO) 9397 for all federal agencies 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.

Prior to collecting the SSN for identity proofing, organizations should 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 should be demonstrated by an inability to alter systems, processes, or forms due to cost or unacceptable levels of risk. Operational necessity should not be justified by ease of use or unwillingness to change.

Federal agencies should 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 Memorandum M-07-16, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information,” May 22, 2007, which requires agencies to review their use of social security numbers in agency systems and programs to identify instances in which collection or use of the social security number is superfluous.

## 8.2. Notice and Consent

Section 4.2, requirement (4) requires the CSP to provide explicit notice at the time of collection to the applicant 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, as well as an assessment of privacy risks that may arise from the collection. There are various factors that should be considered, including the reliability of the assumptions Applicants may have about the collection, other information that may be collected from other sources and appended to the information collected from the Applicant, etc. However, an effective notice is never only a link that leads 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 (5) 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, or to comply with law or legal process unless the CSP provides clear notice and obtains consent from the subscriber for additional uses.

Care should be taken to ensure that use of attributes collected and maintained in the identity proofing process are limited to its original purpose for collection. If use of such information does not fall within uses related to identity proofing, authentication, authorization or attribute assertions, or to comply with law or legal process, the CSP must provide notice and obtain consent from the subscriber. Agencies should consult their Senior Agency Official for Privacy (SAOP) if there are questions about whether proposed agency uses fall within the scope of these uses. This notice should follow the

same principles as described in Section 8.2 *Effective Notice* 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 (6) requires the CSP to provide effective mechanisms for redress of 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 maintaining a system of records to follow procedures to enable applicants to access and, if the records are incorrect, amend their records. Any Privacy Act Statement should include a reference to the applicable system of records notice(s) (SORN), which provides 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 clear to users the availability of alternative methods for completing the process, (e.g., in person at a customer service center, if available), in the event an applicant is unable to establish his/her 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 as to 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

Sections 4.2, requirement (8) and (11) 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 (13) 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 as advise the agency on compliance requirements such as whether or not the collection of PII to conduct identity proofing triggers the Privacy Act of 1974 or the E-Government Act of 2002 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 so as to advise appropriately on what compliance 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.*

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 key elements necessary 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; since 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, conducting it 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.

The goal of this section is to raise implementers’ awareness of usability considerations associated with enrollment and identity proofing (for usability considerations for typical authenticator usage and intermittent events, see 800-63-3B).

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.

- Minimize the number of steps at every step of the process required for enrollment and make each step as clear and easy as possible for users, in order to avoid user frustration.
- Clearly communicate how and where to acquire technical assistance. For example, provide users helpful information, such as a link to online self-service feature, chat sessions, and a phone number for help desk support. Ideally, sufficient information is provided to enable users to answer their own enrollment preparation questions without outside intervention.
- Clearly explain to users who is collecting and who is retaining information they’re providing as well as the path their data will take.
- Ensure all information presented to the user 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 usability evaluation for each step with representative users, realistic goals and tasks, and appropriate contexts of use.

Usability considerations specifically for each step are detailed below.

## 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 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., documentation required) in a usable format in an appropriate timeframe. This includes making users aware of exactly what identity evidence will be required, conveyed from the users’ perspective, not the implementers’ perspectives. 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 type of IAL is required for access to a particular system.

In order 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, in case 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 her or his 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 regarding setting up an enrollment session appointment and 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 (for example, a raised seal on a birth certificate or an original authenticator for obtaining a derived authenticator). 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 that users 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 and 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.
    - 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.
- 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 and what, if any, information will be retained for future follow-up sessions (and for how long), and what identity evidence they will need to bring to complete a future session.
    - If enrollment is unsuccessful, provide users with clear instructions for alternative enrollment session types, for example, offering in-person proofing if users failed remote proofing.
- If users receive the authenticator during the enrollment session, provide users information on the use and maintenance of the authenticator. For example, 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.
- 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 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 800-63B, Sections 10.1 through 10.3 (sp800-63b.html#usabilitycommon). 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.

# 10. References

*This section is informative.*

[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 (https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual).

[Canadian Guideline on Identity Assurance] available at: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=30678&section=HTML (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=30678&section=HTML).

[COPPA] Children's Online Privacy Protection Act of 1998 ("COPPA"), 15 U.S.C. 6501-6505, 16 CFR Part 312

[OMB 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://www.whitehouse.gov/omb/memoranda/m03-22.html (https://www.whitehouse.gov/omb/memoranda/m03-22.html).

[M-04-04] OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies* (December 16, 2003), available at: https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf (https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf).

[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 (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).

[FBCACP] X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), Version 2.27 (December 2, 2013), available at: https://www.idmanagement.gov/IDM/servlet/fileField?entityId=ka0t0000000TN7cAAG&field=File__Body__s (https://www.idmanagement.gov/IDM/servlet/fileField?entityId=ka0t0000000TN7cAAG&field=File__Body__s).

[FBCASUP] FBCA Supplementary Antecedent, In-Person Definition (July 16, 2009), available at: https://www.idmanagement.gov/IDM/servlet/fileField?entityId=ka0t0000000TNPgAAO&field=File__Body__s (https://www.idmanagement.gov/IDM/servlet/fileField?entityId=ka0t0000000TNPgAAO&field=File__Body__s).

[A-130] OMB Circular A-130, *Managing Federal Information as a Strategic Resource* (July 28, 2016), available at: https://www.whitehouse.gov/omb/circulars_default (https://www.whitehouse.gov/omb/circulars_default).

[ISO 9241-11] International Organization for Standardization, *Ergonomic requirements for office work with visual display terminals (VDTs) – Part 11: Guidance on Usability*, ISO 9241-11:1998, ISO: Geneva, Switzerland, 1998.

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

[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 (https://www.ssa.gov/foia/html/EO9397.htm).

[SP 800-53] NIST Special Publication 800-53, Revision 4, *Recommended Security and Privacy Controls for Federal Information Systems and Organizations*, August 2013 and Errata as of January 2015.