NIST Special Publication
NIST SP 800-63A-4 2pd

Digital Identity Guidelines

Identity Proofing and Enrollment

Second Public Draft

David Temoshok
Christine Abruzzi
Yee-Yin Choong
James L. Fenton
Ryan Galluzzo
Connie LaSalle
Naomi Lefkovitz
Andrew Regenscheid
Ryan Galluzzo

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63a-4.2pd

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

NIST Special Publication
NIST SP 800-63A-4 2pd

Digital Identity Guidelines

Identity Proofing and Enrollment

Second Public Draft

David Temoshok
Ryan Galluzzo
Connie LaSalle
Naomi Lefkovitz
Ryan Galluzzo
Applied Cybersecurity Division
Information Technology Laboratory

Yee-Yin Choong
Information Access Division
Information Technology Laboratory

Andrew Regenscheid
Computer Security Division
Information Technology Laboratory

Christine Abruzzi
Cacapon Cyber Solutions

James L. Fenton
Altmode Networks

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63a-4.2pd

August 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

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

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 the National Institute of Standards and Technology, 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 https://csrc.nist.gov/publications.

Authority

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

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

NIST Technical Series Policies

Copyright, Fair Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History

Approved by the NIST Editorial Review Board on YYYY-MM-DD [will be added upon final publication]

How to Cite this NIST Technical Series Publication

Temoshok D, Abruzzi C, Choong YY, Fenton JL, Galluzzo R, LaSalle C, Lefkovitz N, Regenscheid A (2024) Digital Identity Guidelines: Identity Proofing and Enrollment. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63A-4 2pd. https://doi.org/10.6028/NIST.SP.800-63a-4.2pd

Author ORCID iDs

David Temoshok: 0000-0001-6195-0331
Christine Abruzzi: 0000-0001-8904-930X
Yee-Yin Choong: 0000-0002-3889-6047
James L. Fenton: 0000-0002-2344-4291
Ryan Galluzzo: 0000-0003-0304-4239
Connie LaSalle: 0000-0001-6031-7550
Naomi Lefkovitz: 0000-0003-3777-3106
Andrew Regenscheid: 0000-0002-3930-527X
Ryan Galluzzo: 0000-0003-0304-4239

Public Comment Period

August 21, 2024 - October 7, 2024

Submit Comments

mailto:dig-comments@nist.gov

Additional Information

Additional information about this publication is available at https://csrc.nist.gov/pubs/sp/800/63/a/4/2pd, including related content, potential updates, and document history.

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

Abstract

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. The guidelines are not intended to constrain the development or use of standards outside of this purpose. This publication supersedes NIST Special Publication (SP) 800-63A.

Keywords

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

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.

Note to Reviewers

In December 2022, NIST released the Initial Public Draft (IPD) of SP 800-63, Revision 4. Over the course of a 119-day public comment period, the authors received exceptional feedback from a broad community of interested entities and individuals. The input from nearly 4,000 specific comments has helped advance the improvement of these Digital Identity Guidelines in a manner that supports NIST's critical goals of providing foundational risk management processes and requirements that enable the implementation of secure, private, equitable, and accessible identity systems. Based on this initial wave of feedback, several substantive changes have been made across all of the volumes. These changes include but are not limited to the following:

1. Updated text and context setting for risk management. Specifically, the authors have modified the process defined in the IPD to include a context-setting step of defining and understanding the online service that the organization is offering and intending to potentially protect with identity systems.
2. Added recommended continuous evaluation metrics. The continuous improvement section introduced by the IPD has been expanded to include a set of recommended metrics for holistically evaluating identity solution performance. These are recommended due to the complexities of data streams and variances in solution deployments.
3. Expanded fraud requirements and recommendations. Programmatic fraud management requirements for credential service providers and relying parties now address issues and challenges that may result from the implementation of fraud checks.
4. Restructured the identity proofing controls. There is a new taxonomy and structure for the requirements at each assurance level based on the means of providing the proofing: Remote Unattended, Remote Attended (e.g., video session), Onsite Unattended (e.g., kiosk), and Onsite Attended (e.g., in-person).
5. Integrated syncable authenticators. In April 2024, NIST published interim guidance for syncable authenticators. This guidance has been integrated into SP 800-63B as normative text and is provided for public feedback as part of the Revision 4 volume set.
6. Added user-controlled wallets to the federation model. Digital wallets and credentials (called “attribute bundles” in SP 800-63C) are seeing increased attention and adoption. At their core, they function like a federated IdP, generating signed assertions about a subject. Specific requirements for this presentation and the emerging context are presented in SP 800-63C-4.

The rapid proliferation of online services over the past few years has heightened the need for reliable, equitable, secure, and privacy-protective digital identity solutions. Revision 4 of NIST Special Publication SP 800-63, *Digital Identity Guidelines*, intends to respond to the changing digital landscape that has emerged since the last major revision of this suite was published in 2017, including the real-world implications of online risks. The guidelines present the process and technical requirements for meeting digital identity management assurance levels for identity proofing, authentication, and federation, including requirements for security and privacy as well as considerations for fostering equity and the usability of digital identity solutions and technology.

Based on the feedback provided in response to the June 2020 Pre-Draft Call for Comments, research into real-world implementations of the guidelines, market innovation, and the current threat environment, this draft seeks to:

- Address comments received in response to the IPD of Revision 4 of SP 800-63

- Clarify the text to address the questions and issues raised in the public comments
- Update all four volumes of SP 800-63 based on current technology and market developments, the changing digital identity threat landscape, and organizational needs for digital identity solutions to address online security, privacy, usability, and equity

NIST is specifically interested in comments and recommendations on the following topics:

1. Identity Proofing and Enrollment
    - Is the updated structure of the requirements around defined types of proofing sufficiently clear? Are the types sufficiently described?
    - Are there additional fraud program requirements that need to be introduced as a common baseline for CSPs and other organizations?
    - Are the fraud requirements sufficiently described to allow for appropriate balancing of fraud, privacy, and usability trade-offs?
    - Are the added identity evidence validation and authenticity requirements and performance metrics realistic and achievable with existing technology capabilities?
2. General
    - What specific implementation guidance, reference architectures, metrics, or other supporting resources could enable more rapid adoption and implementation of this and future iterations of the Digital Identity Guidelines?
    - What applied research and measurement efforts would provide the greatest impacts on the identity market and advancement of these guidelines?

Reviewers are encouraged to comment and suggest changes to the text of all four draft volumes of the SP 800-63-4 suite. NIST requests that all comments be submitted by 11:59pm Eastern Time on October 7th, 2024. Please submit your comments to dig-comments@nist.gov. NIST will review all comments and make them available on the NIST Identity and Access Management website. Commenters are encouraged to use the comment template provided on the NIST Computer Security Resource Center website for responses to these notes to reviewers and for specific comments on the text of the four-volume suite.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: mailto:dig-comments@nist.gov.

Table of Contents

List of Tables

List of Figures

Preface

The purpose of this document, and associated companion volumes [SP800-63], [SP800-63B], and [SP800-63C], is to provide guidance to organizations for the processes and technologies for the management of digital identities at designated levels of assurance.

This document provides requirements for the identity proofing of individuals at each Identity Assurance Level (IAL) for the purposes of enrolling them into an identity service or providing them access to online resources. It applies to the identity proofing of individuals over a network or in person.

Acknowledgments

The authors would like to thank their fellow collaborators on the current revision of this special publication, Sarbari Gupta, Diana Proud-Madruga, and Justin P. Richer, as well as Kerrianne Buchanan and Greg Fiumara for their contributions and review. The authors would like to also acknowledge the past contributions of Donna F. Dodson, Elaine M. Newton, Ray A. Perlner, W. Timothy Polk, Emad A. Nabbus, Paul A. Grassi, Kristen Greene, Mary Theofanos, Jamie M. Danker, Adam Cooper, Alastair Treharne, Julian White, Tim Bouma, Kaitlin Boeckl, Joni Brennan, Ben Piccarreta, Ellen Nadeau, and Danna Gabel O'Rourke.

1. Introduction

This section is informative.

One of the challenges of providing online services is being able to associate a set of activities with a single, known individual. While there are situations where this is not necessary, there are other situations where it is important to reliably establish an association with a real-life subject. Examples of this include accessing government services and executing financial transactions. There are also situations where association with a real-life subject is required by regulations (e.g., the financial industry's 'Customer Identification Program' requirements) or to establish accountability for high-risk actions (e.g., changing the release rate of water from a dam).

This guidance defines identity proofing as the process of establishing, to some degree of assurance, a relationship between a subject accessing online services and a real-life person. This document provides guidance for Federal Agencies, third-party Credential Service Providers (CSP), and other organizations that provide or use identity proofing services.

1.1. Expected Outcomes of Identity Proofing

The expected outcomes of identity proofing include:

- **Identity resolution**: Determine that the claimed identity corresponds to a single, unique individual within the context of the population of users served by the CSP or online service.
- **Evidence validation**: Confirm that supplied evidence is genuine, authentic, and valid.
- **Attribute validation**: Confirm the accuracy of the core attributes. Core attributes are the minimum set required for identity proofing.
- **Identity verification**: Confirm that the claimant is the genuine owner of the presented evidence and attributes.
- **Identity enrollment**: Enroll the identity proofed applicant in the CSP's identity service as a subscriber.
- **Fraud mitigation**: Detect, respond to, and prevent access to benefits, services, data, or assets using a fraudulent identity.

Identity proofing services are expected to incorporate privacy-enhancing principles, such as data minimization, as well as employ good usability practices, to minimize the burden on applicants while still accomplishing the expected outcomes.

1.2. Identity Assurance Levels

Assurance (confidence) in a subscriber's identity is established using the processes associated with the defined Identity Assurance Levels (IAL). Each successive IAL builds on the requirements of lower IALs in order to achieve increased assurance.

No identity proofing: There is no requirement to link the applicant to a specific, real-life person. Any attributes provided in conjunction with the subject's activities are self-asserted or are treated as self-asserted. Evidence is not validated and attributes are neither validated nor verified.

IAL1: The identity proofing process supports the real-world existence of the claimed identity and provides some assurance that the applicant is associated with that identity. Core attributes are obtained from identity evidence or self-asserted by the applicant. All core attributes (see Sec. 2.2) are validated against authoritative or credible sources and steps are taken to link the attributes to the person undergoing the identity proofing process. Identity proofing is performed using remote or onsite processes, with or without the attendance of a CSP representative (proofing agent or trusted referee). Upon the successful completion of identity proofing, the applicant is enrolled into a subscriber account and any authenticators, including subscriber-provided authenticators, can then be bound to the account. IAL1 is designed to limit highly scalable attacks, provide protection against synthetic identities, and provide protections against attacks using compromised PII.

IAL2: IAL2 adds additional rigor to the identity proofing process by requiring the collection of additional evidence and a more rigorous process for validating the evidence and verifying the identity. In addition to those threats addressed by IAL1, IAL2 is designed to limit scaled and targeted attacks, provide protections against basic evidence falsification and evidence theft, and provide protections against basic social engineering tactics.

IAL3: IAL3 adds the requirement for a trained CSP representative (proofing agent) to interact directly with the applicant, as part of an on-site attended identity proofing session, and the collection of at least one biometric. The successful on-site identity proofing session concludes with the enrollment of the applicant into a subscriber account and the delivery of one or more authenticators associated (bound) to that account. IAL3 is designed to limit more sophisticated attacks, provide protections against advanced evidence falsification, theft, and repudiation, and provide protection against more advanced social engineering tactics.

1.3. Notations

This guideline uses the following typographical conventions in text:

- Specific terms in **CAPITALS** represent normative requirements. When these same terms are not in **CAPITALS**, the term does not represent a normative requirement.
  - 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, 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.

1.4. Document Structure

This document is organized as follows. Each section is labeled as either normative (i.e., mandatory for compliance) or informative (i.e., not mandatory).

- Section 1 provides an introduction to the document. This section is *informative*.
- Section 2 describes requirements for identity proofing. This section is *normative*.
- Section 3 describes general requirements for IALs. This section is *normative*.
- Section 4 describes requirements for specific IALs. This section is *normative*.
- Section 5 describes subscriber accounts. This section is *normative*.
- Section 6 provides security considerations. This section is *informative*.
- Section 7 provides privacy considerations. This section is *informative*.
- Section 8 provides usability considerations. This section is *informative*.
- Section 9 provides equity considerations. This section is *informative*.
- References contains a list of publications referred to from this document. This section is *informative*.
- Appendix A provides a non-exhaustive list of types of identity evidence, grouped by strength. This appendix is *informative*.

- Appendix B contains a selected list of abbreviations used in this document. This appendix is *informative*.
- Appendix C contains a glossary of selected terms used in this document. This appendix is *informative*.
- Appendix D contains a summarized list of changes in this document's history. This appendix is *informative*.

2. Identity Proofing Overview

This section is normative.

This section provides an overview of the identity proofing and enrollment process, as well as requirements to support the resolution, validation, and verification of the identity claimed by an applicant. It also provides guidelines on additional aspects of the identity proofing process. These requirements are intended to ensure that the claimed identity exists in the real world and that the applicant is the individual associated with that identity.

Additionally, these guidelines provide for multiple methods by which resolution, validation, and verification can be accomplished, as well as providing the multiple types of identity evidence that support the identity proofing process. CSPs and organizations **SHALL** provide options when implementing their identity proofing services and processes to promote access for applicants with different means, capabilities, and technology access. These options **SHOULD** include accepting multiple types and combinations of identity evidence; supporting multiple data validation sources; enabling multiple methods for verifying identity; providing multiple channels for engagement (e.g., onsite, remote); and offering assistance mechanisms for applicants (e.g., applicant references).

CSPs **SHALL** evaluate the risks associated with each identity proofing option offered (e.g., identity proofing types, validation sources, assistance mechanisms) and implement mitigating fraud controls, as appropriate. At a minimum, CSPs **SHALL** design each option such that, in aggregate, the options provide comparable assurance.

2.1. Identity Proofing and Enrollment

The objective of identity proofing is to ensure that, to a stated level of certainty, the applicant involved in the identity proofing process is who they claim to be. This document presents a three-step process for CSPs to identity proof applicants at designated assurance levels. The first step, identity resolution, consists of collecting appropriate identity evidence and attribute information to determine that the applicant is a unique identity in the population served by the CSP and is a real-life person. The second step, identity validation, validates the genuineness, accuracy, and validity of the evidence and attribute information collected in the first step. The third step, identity verification, confirms that the applicant presenting the identity evidence is the same individual to whom the validated evidence was issued and with whom the validated attributes are associated. In most cases, upon successfully identity proofing an applicant to the designated IAL, the CSP establishes a unique subscriber account for the applicant (now a subscriber in the identity service), which allows one or more authenticators to be bound to the proven identity in the account.

Identity proofing can be part of an organization's business processes that support the determination of suitability or entitlement to a benefit or service. While these guidelines

provide guidance for appropriate levels of identity assurance, suitability and eligibility determinations for benefits or services are distinct business process decisions from these identity proofing processes and are outside the scope of these guidelines.

2.1.1. Process Flow

This subsection is informative.

Figure 1 provides an illustrative example of the three-step identity proofing process.

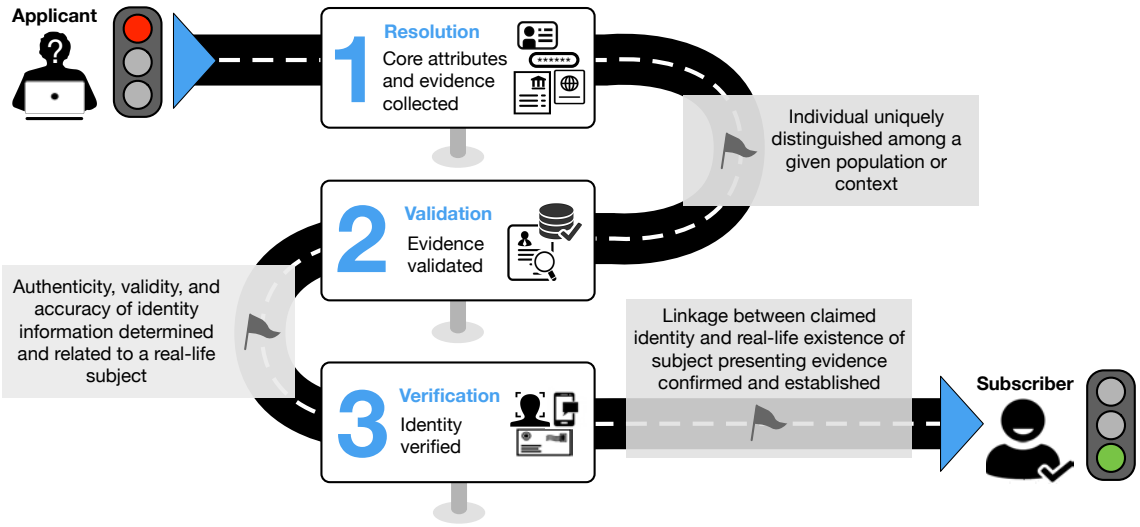

Fig. 1. Identity Proofing Process

The following steps present a common workflow example for IAL2 remote identity proofing, which is intended to illustrate the workflow steps for this example. These steps are not intended to represent a normative processing workflow model.

1. **Resolution**
   - The CSP captures one or more pieces of identity evidence, such as a driver's license, mobile driver's license, or passport.
   - The CSP collects any additional attributes, as needed, from the applicant to supplement those contained on the presented identity evidence.
2. **Validation**
   - The CSP confirms the presented evidence is authentic, accurate, and valid (e.g., not revoked).
   - The CSP validates the attributes obtained in step 1 by checking them against authoritative or credible validation sources.

3. **Verification**

    - The CSP employs one of the IAL2 Verifcation Pathways to confirm the applicant is the genuine owner of the presented identity evidence.

Enrollment

Upon the successful completion of the three identity proofing steps, a notification of proofing is sent to a validated address, and the applicant can be enrolled into a subscriber account with the CSP, as described in Section 5. A subscriber account includes at least one validated address (e.g., phone number, mailing address) that can be used to communicate with the subscriber about their account. Additionally, one or more authenticators are bound to the proven identity in the subscriber account.

2.1.2. Identity Proofing Roles

To support the delivery of identity proofing that meets the various needs of applicants and risk scenarios, different individuals would be expected to play different roles within the proofing process. To support the consistent implementation of these guidelines, the following identity proofing roles are defined:

1. **Proofing Agent** - An agent of the CSP who is trained to attend identity proofing sessions, either onsite or remotely, and make limited, risk-based decisions – such as visually inspecting identity evidence and making a determination that the evidence has not been altered.
2. **Trusted Referee** - An agent of the CSP who is trained to make risk-based decisions regarding an applicant's identity proofing case when that applicant is unable to meet expected requirements of a defined IAL proofing process. Unlike a Proofing Agent (although a trusted referee may also fulfill this role), the level of training is expected to be more substantial to include training to detect deception and signs of social engineering, in addition to the ability to support validation and verification through physical inspection of the evidence and visual comparison of the applicant to a reference facial image. Requirements for trusted referees are contained in Sec. 3.1.13.1. > **Note:** Trusted referees differ from proofing agents in that trusted referees receive additional training and resources to support exception handling scenarios, including when applicants do not possess the required identity evidence or the attributes on the evidence do not all match the claimed identity (e.g., due to a recent name or address change).
3. **Applicant Reference** - A representative of the applicant who can vouch for the identity of the applicant, specific attributes related to the applicant, or conditions relative to the context of the individual (e.g., emergency status, homelessness). This individual does not act on behalf of the applicant in the identity proofing

process but is a resource that can be called on to support claims of identity. Requirements for applicant references are contained in Sec. 3.1.13.3.

4. **Process Assistants** - An individual who provides support for the proofing process but does not support decision making or risk-based evaluation (e.g., translation, transcription, or accessibility support). Process assistants may be provided by the CSP or the applicant.

CSPs **SHALL** identify which of above roles are applicable to their identity service and **SHALL** provide training and support resources consistent with the requirements and expectations provided in Sec. 3.

2.1.3. Identity Proofing Types

The ability to provide resolution, validation, and verification as part of an identity proofing process is delivered through a combination of technologies, communication channels, and identity proofing roles to support the diverse users, communities, and relying parties CSPs serve. The types of proofing can be categorized based on two specific factors – whether they are attended and where they take place.

1. **Remote Unattended Identity Proofing** – Identity proofing conducted where the resolution, validation, and verification processes are completely automated and interaction with a proofing agent is not required. The location and devices used in the proofing process are not controlled by the CSP.
2. **Remote Attended Identity Proofing** – Identity proofing conducted where the applicant completes resolution, validation, and verification steps through a secure video session with a proofing agent. The location and devices used in the proofing process are not controlled by the CSP.
3. **Onsite Unattended Identity Proofing** - Identity proofing conducted where an individual interacts with a controlled workstation or kiosk, but interaction with a proofing agent is not required. The process is fully automated, but at a physical location and on devices approved by the CSP.
4. **Onsite Attended Identity Proofing** - Identity proofing conducted in a physical setting where the applicant completes the entire identity proofing process - to include resolution, validation, and verification – in the presence of a proofing agent. The proofing agent may be co-located with the user or interact with the user via a kiosk or device. The physical location and devices are all approved by the CSP.

Requirements at each assurance level are structured to allow CSPs to implement different combinations of proofing types to meet the requirements of different assurance levels (as appropriate). CSPs that offer IAL1 & IAL2 services **SHALL** provide a Remote Unattended identity proofing process and **SHALL** offer at-least one attended

identity proofing process option. CSPs that offer IAL1 & IAL2 services **SHOULD** support identity proofing processes that allow for the applicant to transition between proofing types in the event an applicant is unsuccessful with one type (e.g., allow an applicant who fails remote unattended to transition to remote attended).

2.2. Core Attributes

The identity proofing process involves the presentation and validation of the minimum attributes necessary to accomplish identity proofing - this includes what is needed to complete resolution, validation, and verification. While the necessary core attributes for a given use case will change based on the nature of the community being served, the following attributes **SHOULD** be collected by CSPs to support the proofing process:

- **First Name**: The applicant's given name.
- **Middle Name or Initial**: The applicant's middle name or initial if available.
- **Last Name**: The applicant's last name or family name as appropriate.
- **Government Identifier**: A unique identifier which is associated with the applicant in government records (e.g., SSN, TIN, Driver's License #).
- **Physical Address**: A physical address to which the applicant can receive communications related to the proofing process; or a **Digital Address**: A digital address (e.g., phone or email) to which the applicant can receive communications related to the proofing process.

Additional attributes may be added to these as required by the CSP and RP. The CSP and RP **SHALL** document all core attributes in trust agreements and practice statements. Following a privacy risk assessment, a CSP **MAY** request additional attributes that are not required to complete identity proofing, but that may support other RP business processes. See Sec. 3.1.3 for details on privacy requirements for requesting additional attributes.

2.3. Identity Resolution

The goal of identity resolution is to use the smallest possible set of attributes to uniquely and accurately distinguish an individual within a given population or context. This step involves comparing an applicant's collected attributes to those stored in records for users served by the CSP. While identity resolution is the starting point in the overall identity proofing process, to include the initial detection of potential fraud, it in no way represents a complete and successful identity proofing process.

2.4. Identity Validation and Identity Evidence Collection

The goal of identity validation is to collect the most appropriate identity evidence from the applicant and determine that it is genuine (not altered or forged), accurate (the pertinent data is correct, current, and related to the applicant), and valid.

> **Note:** This document uses the term "valid" rather than expired in recognition that evidence can remain a useful means to prove identity, even if it is expired or was issued outside a determined timeframe.

Identity evidence collection supports the identity validation process and consists of two steps: 1) the presentation of identity evidence by the identity proofing applicant to the CSP and 2) the determination by the CSP that the presented evidence meets the applicable strength requirements.

2.4.1. Evidence Strength Requirements

This section defines the requirements for identity evidence at each strength. The strength of a piece of identity evidence is determined by:

1. The issuing rigor,
2. The ability to provide confidence in validation, including accuracy and authenticity checks, and
3. The ability to provide confidence in the verification of the applicant presenting the evidence.

Appendix A of this document provides a non-exhaustive list of possible evidence types, grouped by strength.

2.4.1.1. Fair Evidence Requirements

To be considered FAIR, identity evidence **SHALL** meet *all* the following requirements:

1. The issuing source of the evidence confirmed the claimed identity through a process designed to enable it to form a belief that it knows the real-life identity of the person. For example, evidence issued by financial institutions that have customer identity verification obligations under the Customer Identification Program (CIP) Rule implementing Section 326 of the USA PATRIOT Act of 2001, or that have obligations to establish an Identity Theft Prevention Program under the Red Flags Rule and Guidelines, implemented under Sec. 114 of the Fair and Accurate Credit Transaction Act of 2003 (FACT Act).

1. It is likely that the evidence-issuing process would result in the delivery of the evidence to the person to whom it relates, such as delivery to a postal address.
2. The evidence contains the name of the claimed identity.
3. The evidence contains at least one reference number, a facial portrait, or sufficient attributes to uniquely identify the person to whom it relates.
4. The evidence contains physical (e.g., security printing, optically variable features, holograms) or digital security features that make it difficult to reproduce.
5. The information on the evidence is able to be validated by an authoritative or credible source.
6. The evidence is able to be verified through an approved method, as provided in Sec. 2.4.2.2.

2.4.1.2. Strong Evidence Requirements

In order to be considered STRONG, identity evidence **SHALL** meet *all* the following requirements:

1. The issuing source of the evidence confirmed the claimed identity by following written procedures designed to enable it to have high confidence that it knows the real-life identity of the subject. Additionally, these procedures are subject to recurring oversight by regulatory or publicly accountable institutions, such as states, the federal government, and some regulated industries. Such procedures would include, but not be limited to, identity proofing at IAL2 or above.
2. It is likely that the evidence-issuing process would result in the delivery of the evidence to the person to whom it relates, such as delivery to a postal address.
3. The evidence contains the name of the claimed identity.
4. The evidence contains a reference number or other attributes that uniquely identify the person to whom it relates.
5. The evidence contains a facial portrait or other biometric characteristic of the person to whom it relates.
6. The evidence includes physical security features or digital security features that make it difficult to copy or reproduce.
7. The information on the evidence is able to be validated by an authoritative or credible source.
8. The evidence is able to be validated through an approved method, as provided in Sec. 2.4.2.2.

2.4.1.3. Superior Evidence Requirements

In order to be considered SUPERIOR, identity evidence **SHALL** meet *all* the following requirements:

1. The issuing source of the evidence confirmed the claimed identity by following written procedures designed to enable it to have high confidence that the source knows the real-life identity of the subject. Additionally, these procedures are subject to recurring oversight by regulatory or publicly accountable institutions, such as states and the federal government, and some regulated industries. Such procedures would include, but not be limited to, identity proofing at IAL2 or above.
2. The identity evidence contains attributes and data objects that are cryptographically protected and can be validated through verification of a digital signature applied by the issuing source.
3. The issuing source had the subject participate in an attended enrollment and identity proofing process that confirmed their physical existence.
4. It is likely that the evidence-issuing process would result in the delivery of the evidence to the person to whom it relates, such as delivery to a postal address.
5. The evidence contains the name of the claimed identity.
6. The evidence contains at least one reference number that uniquely identifies the person to whom it relates.
7. The evidence contains a facial portrait or other biometric characteristic of the person to whom it relates.
8. If the evidence is physical, then evidence includes security features that make it difficult to copy or reproduce.
9. The evidence is able to be verified through an approved method, as provided in Sec. 2.4.2.2.

2.4.2. Identity Evidence and Attribute Validation

Identity evidence validation involves examining the presented evidence to confirm it is authentic (not forged or altered), accurate (the information on the evidence is correct), and valid (unexpired or within the CSP's defined timeframe for issuance or expiration). Attribute validation involves confirming the accuracy of the core attributes, whether obtained from presented evidence or self-asserted. The following subsections provide the acceptable methods for evidence and attribute validation.

2.4.2.1. Evidence Validation

The CSP **SHALL** validate the authenticity, accuracy, and validity of presented evidence by confirming:

- The evidence is in the correct format and includes complete information for the identity evidence type;
- The evidence is not counterfeit and that it has not been tampered with;
- Any security features; and
- The information on the evidence is accurate.

2.4.2.2. Evidence Validation Methods

Acceptable methods for validating presented evidence include:

- Visual and tactile inspection by trained personnel for onsite identity proofing;
- Visual inspection by trained personnel for remote identity proofing;
- Automated document validation processes using appropriate technologies; and
- Cryptographic verification of the source and integrity of digital evidence, or attribute data objects.

2.4.2.3. Attribute Validation

The CSP **SHALL** validate all core attributes, as described in Sec. 2.2, whether obtained from identity evidence or self-asserted by the applicant, with an authoritative or credible source, as in Sec. 2.4.2.4.

2.4.2.4. Validation Sources

The CSP **SHALL** use authoritative or credible sources that meet the following criteria.

An authoritative source is the issuing source of identity evidence or attributes, or has direct access to the information maintained by issuing sources, such as state DMVs for driver's license data and the Social Security Administration for Social Security Cards and Social Security Numbers. An authoritative source may also be one that provides or enables direct access to issuing sources of evidence or attributes, such as the American Association of Motor Vehicle Administrators' Driver's License Data Verification (DLDV) Service.

A credible source is an entity that can provide or validate the accuracy of identity evidence and attribute information. In addition to being subject to regulatory oversight (such as the Fair Credit Reporting Act (FCRA)), a credible source has access to attribute information that can be traced to an authoritative source, or maintains identity attribute information obtained from multiple sources that is correlated for accuracy, consistency, and currency. Examples of credible sources are credit bureaus that are subject to the FCRA.

2.5. Identity Verification

The goal of identity verification is to establish, to a specified level of confidence, the linkage between the claimed validated identity and the real-life applicant engaged in the identity proofing process. In other words, verification provides assurance that the applicant presenting the evidence is the rightful owner of that evidence.

2.5.1. Identity Verification Methods

The CSP **SHALL** verify the linkage of the claimed identity to the applicant engaged in the identity proofing process through one or more of the following methods. Section 4 provides acceptable verification methods at each IAL.

- **Confirmation Code Verification.** The individual is able to demonstrate control of a piece of identity evidence through the return of a confirmation code, consistent with the requirements specified in Sec. 3.1.8.
- **Authentication and Federation Protocols.** The individual is able to demonstrate control of a digital account (e.g., online bank account) or signed digital assertion (e.g., verifiable credentials) through the use of authentication or federation protocols. This may be done in person, through presentation of the credential to a device or reader, but can also be done during remote identity proofing sessions.
- **Micro Transaction.** An individual is able to demonstrate control of a piece of evidence by returning a value based on a micro transaction made between the CSP and the issuing source of the evidence (e.g., bank account).
- **Onsite-In-person (Attended) visual facial image comparison.** The proofing agent and applicant interact for the identity proofing event. The proofing agent performs a visual comparison of the facial portrait presented on identity evidence to the face of the applicant engaged in the identity proofing event.
- **Remote (Attended or Unattended) visual facial image comparison.** The proofing agent performs a visual comparison of the facial portrait presented on identity evidence, or stored by the issuing source, to the facial image of the applicant engaged in the identity proofing event. The proofing agent may interact directly with the applicant during some or all of the identity proofing event (attended) or may conduct the comparison at a later time (unattended) using a captured video or photograph and the uploaded copy of the evidence. If the comparison is performed at a later time, steps are taken to ensure the captured video or photograph was taken from the live applicant present during the identity proofing event.
- **Automated (Unattended) biometric comparison.** Automated biometric comparison, such as facial recognition or other fully automated algorithm-driven biometric comparison, **MAY** be performed for onsite or remote identity proofing events. The facial image or other biometric characteristic (e.g., fingerprints,

palm prints, iris and retina patterns, voiceprints, or vein patterns) on the identity evidence, or stored in authoritative records, is compared to the facial image in a photograph of the live applicant or other biometric live sample collected from the applicant during the identity proofing event.

Knowledge-based verification (KBV) or knowledge-based authentication **SHALL NOT** be used for identity verification.

3. Identity Proofing Requirements

This section is normative.

This section provides requirements for CSPs that operate identity proofing and enrollment services, including requirements for identity proofing at each of the IALs. This section also includes additional requirements for federal agencies regardless of whether they operate their own identity service or use an external CSP.

Sections 4.1, 4.2, and 4.3 provide the requirements and guidelines for identity proofing at a specific IAL. Section 4.4 includes a summarized list of these requirements by IAL in Table 1.

3.1. General Requirements

The requirements in this section apply to all CSPs performing identity proofing at any IAL.

3.1.1. Identity Service Documentation and Records

The CSP **SHALL** conduct its operations according to a practice statement that details all identity proofing processes as they are implemented to achieve the defined IAL. The practice statement **SHALL** include, at a minimum:

1. A complete service description including the particular steps the CSP follows to identity proof applicants at each offered assurance level;
2. The CSP's policy for providing notice to applicants about the types of identity proofing processes available, the evidence and attribute collection requirements for the specified IAL, the purpose of PII collection (per Sec. 3.1.3.2), and for the collection, use, and retention of biometrics (see Sec. 3.1.11);
3. The CSP's policy for ensuring the identity proofing process is concluded in a timely manner, once the applicant has met all of the requirements;
4. Types of identity evidence the CSP accepts to meet the evidence strength requirements;
5. The CSP's policy and process for validating and verifying identity evidence, including training and qualification requirements for personnel who have validation and verification responsibilities, as well as specific technologies the CSP employs for evidence validation and verification;
6. Alternative processes for the CSP to complete identity proofing for an individual applicant who does not possess the required identity evidence to complete the identity proofing process[1];

[1] Options include using a trusted referee, with or without an applicant representative.

7. The attributes that the CSP considers to be core attributes, and the authoritative and credible sources it uses for validating those attributes. Core attributes include the minimum set of attributes that the CSP needs to perform identity resolution as well as any additional attributes that the CSP collects and validates for the purposes of identity proofing, fraud mitigation, complying with laws or legal process, or conveying to relying parties (RPs) through attribute assertions;
8. The CSP's policy and process for addressing identity proofing errors;
9. The CSP's policy and process for identifying and remediating suspected or confirmed fraudulent accounts, including communicating with RPs and affected individuals;
10. The CSP's policy for managing and communicating service changes (e.g., changes in data sources, integrated vendors, or biometric algorithms) to RPs;
11. The CSP's policy for any conditions that would require re-verification of the user (e.g., account recovery, account abandonment, regulatory "recertification" requirements);
12. The CSP's policy for conducting privacy risk assessments, including the timing of its periodic reviews and specific conditions that will trigger an updated privacy risk assessment (see Sec. 3.1.3.1);
13. The CSP's policy for conducting assessments to determine potential equity impacts, including the timing of its periodic reviews and any specific conditions that will trigger an out-of-cycle review (see Sec. 3.1.4); and,
14. The CSP's policy for the collection, purpose, retention, protection, and deletion of all personal and sensitive data, including the treatment of all personal information if the CSP ceases operation or merges or transfers operations to another CSP.

> **Note:** 800-63C references the use of trust agreements to define requirements between an IdP, CSP, and RP in a federated relationship. CSP practice statements **MAY** be included directly in these agreements.

3.1.2. Fraud Management

A critical aspect of the identity proofing process is to mitigate fraudulent attempts to gain access to benefits, services, data, or assets protected by identity management systems. Resolution, Validation, and Verification processes in many instances can mitigate many attacks. However, with the constantly changing threat environment, the layering of additional checks and controls can provide increased confidence in proofed identities and additional protections against attacks intended to defeat other controls. The ability to identify, detect, and resolve instances of potential fraud is a critical functionality for CSPs and RPs alike.

3.1.2.1. CSP Fraud Management

1. CSPs **SHALL** establish and maintain a fraud management program that provides fraud identification, detection, investigation, reporting, and resolution capabilities. The specific capabilities and details of this program **SHALL** be documented within their CSP practice statement.
2. CSPs **SHALL** conduct a Privacy Risk Assessment of all fraud checks and fraud mitigation technologies prior to implementation.
3. The CSP **SHALL** establish a self-reporting mechanism and investigation capability for subjects who believe they have been the victim of fraud or an attempt to compromise their involvement in the identity proofing processes.
4. The CSP **SHALL** take measures to prevent unsuccessful applicants from inferring the accuracy of any self-asserted information with that confirmed by authoritative or credible sources. NOTE: This is often called “data washing” and can be prevented through a number of methods, depending on the interfaces deployed by a CSP. As such, these guidelines do not dictate specific mechanisms to prevent this practice.
5. CSPs **SHALL** implement the following fraud check for all identity proofing processes:

    - **Date of Death Check** – Confirm with a credible, authoritative, or issuing source that the applicant is not deceased. Such checks can aid in preventing synthetic identity fraud, the use of stolen identity information, and exploitation by a close associate or relative.

6. CSPs **SHOULD** implement - but are not limited to - the following fraud checks for their identity proofing processes based on their available identity proofing types, selected technologies, evidence, and user base:

    - **SIM Swap Detection** – Confirm that the phone number used in an identity proofing process has not been recently ported to a new user or device. Such checks can provide an indication that a phone or device was compromised by a targeted attack.
    - **Device or Account Tenure Check** – Evaluate the length of time a phone or other account has existed without substantial modifications or changes. Such checks can provide additional confidence in the reliability of a device or piece of evidence used in the identity proofing process.
    - **Transaction Analytics** – Evaluate anticipated transaction characteristics – such as IP Addresses, geolocations, and transaction velocities – to identify anomalous behaviors or activities that can indicate a higher risk or a potentially fraudulent event. Such checks can provide protections against scaled and automated attacks, as well as give indications of specific attack patterns being executed on identity systems.

- **Fraud Indicator Check** – Evaluate records, such as reported, confirmed, or historical fraud events to determine if there is an elevated risk related to a specific applicant, applicant's data, or device. Such checks can give an indication of identity theft or compromise. Where such information is collected, aggregated, or exchanged across commercial platforms and made available for use to RPs and other CSPs, users **SHALL** be made aware of this practice. This also applies to all websites that report user activity to Federal RPs.

7. CSPs **MAY** employ knowledge-based verification (KBV) as part of its fraud management program.
8. CSPs **SHOULD** consider the recency of fraud-related data when factoring it into fraud prevention capabilities and decisions.
9. For attended proofing processes, CSPs **SHALL** train proofing agents to detect indicators of fraud and **SHALL** provide proofing agents and trusted referees with tools to flag suspected fraudulent events for further treatment and investigation.
10. CSPs **SHALL** continuously monitor the performance of their fraud checks and fraud mitigation technologies to identify and remediate issues related to disparate performance across their platforms or between the demographic groups served by their identity service.
11. CSPs **SHALL** establish a technical or process-based mechanism to communicate suspected and confirmed fraudulent events to RPs.
12. CSPs **SHOULD** implement shared signaling, as described in NIST SP 800-63C-4, to communicate fraud events in real time to RPs.
13. CSPs **MAY** implement fraud mitigation measures as compensating controls. When this is done, these **SHALL** be documented as deviations from the normative guidance of these guidelines and **SHALL** be conveyed to all RPs through a Digital Identity Acceptance Statement prior to integration.

3.1.2.2. RP Fraud Management

1. RPs **SHALL** establish a point of contact with whom CSPs interact and communicate fraud data.
2. Pursuant to a privacy risk assessment, the RP **MAY** also request additional attributes beyond what a CSP provides as its core attributes to combat fraud or to support other business processes.
3. Pursuant to applicable laws and regulations, RPs **SHOULD** establish a mechanism to communicate the outcomes of fraud reports and investigations, including both positive and negative results, to CSPs and other partners in order to allow them to improve their own fraud identification, mitigation, and reporting capabilities.

4. RPs **SHOULD** establish a fraud management program consistent with their mission, regulatory environment, systems, applications, data, and resources.
5. RPs **SHALL** conduct a privacy risk assessment of any CSP fraud checks and mitigation technologies to identify potential privacy risks or unintended harms. Federal agency RPs **SHALL** implement this consistent with the requirements contained in Sec. 3.1.7.
6. RPs **SHALL** include any requirements for fraud checks and fraud mitigation technologies in trust agreements with their CSPs.
7. RPs **SHALL** conduct periodic reviews of their CSP's fraud management program, fraud checks, and fraud technologies to adjust thresholds, review investigations into fraud events, and make determinations about the effectiveness and efficacy of fraud controls.
8. RPs **SHALL** review all fraud mitigation measures that have been deployed as compensating or supplemental controls by CSPs for alignment to their internal risk tolerance and acceptance. The RP **SHALL** record the CSPs compensating controls in their own Digital Identity Acceptance Statement prior to integration.

3.1.2.3. Treatment of Fraud Check Failures

The effectiveness of fraud checks and mitigation technologies will vary based on numerous contributing factors including the data sources used, the technologies used, and – perhaps most importantly – the applicant population. It is therefore critical to have well-structured and documented processes for how to handle failures arising from the fraud management measures. The following requirements apply to handling these failures:

1. CSPs **SHALL** establish and document thresholds and actions related to each of the fraud checks they implement and provide these thresholds to RPs.
2. CSPs **SHALL** establish procedures for redress to allow applicants to resolve issues associated with fraud checks and mitigation technologies. See (see Sec. 3.6 of [SP800-63]) for a more information about redress.
3. The CSP **SHALL** offer trusted referee services to those who fail fraud checks in unattended remote processes. Trusted referees **SHALL** be provided with a summary of the results of the fraud failures to inform their risk-based decisioning processes.

3.1.3. General Privacy Requirements

The following privacy requirements apply to all CSPs providing identity services at any IAL.

3.1.3.1. Privacy Risk Assessment

1. The CSP **SHALL** conduct and document a privacy risk assessment for the processes used for identity proofing and enrollment.[2] At a minimum, the privacy risk assessment **SHALL** assess the risks associated with:
    a) Any processing of PII - including identity attributes, biometrics, images, video, scans, or copies of identity evidence - for the purposes of identity proofing, enrollment, or fraud management;
    b) Any additional steps that the CSP takes to verify the identity of an applicant beyond the mandatory requirements specified herein;
    c) Any processing of PII for purposes outside the scope of identity proofing and enrollment, except to comply with law or legal processes;
    d) The retention schedule for identity records and PII;
    e) Any non-PII that, when aggregated or processed by an algorithm (e.g., artificial intelligence or machine learning tools), could be used to identify a person; and,
    f) Any PII that is processed by a third-party service on behalf of the CSP.
2. Based on the results of its privacy risk assessment, the CSP **SHALL** document the measures it takes to maintain the disassociability, predictability, manageability, confidentiality, integrity, and availability of the PII it processes. [3] In determining such measures, the CSP **SHOULD** apply relevant guidance and standards, such as the *NIST Privacy Framework* [NIST-Privacy] and NIST Special Publication [SP800-53].
3. The CSP **SHALL** re-assess privacy risks and update its privacy risk assessment any time it makes changes to its identity service that affect the processing of PII.
4. The CSP **SHALL** review its privacy risk assessment periodically, as documented in its practice statement, to ensure that it accurately reflects the current risks associated with the processing of PII.

[2] For more information about privacy risk assessments, refer to the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf.

[3] [NISTIR8062] provides an overview of predictability and manageability including examples of how these objectives can be met.

5. The CSP **SHALL** make a summary of its privacy risk assessment available to any organizations that use its services. The summary **SHALL** be in sufficient detail to enable such organizations to do a due diligence investigation.
6. The CSP **SHALL** perform a privacy risk assessment for the processing of any personal information maintained in the subscriber account Sec. 5.

3.1.3.2. Additional Privacy Protective Measures

1. The processing of PII **SHALL** be limited to the minimum necessary to validate the existence of the claimed identity, associate the claimed identity with the applicant, mitigate fraud, and provide RPs with attributes that they may use to make authorization decisions.
2. The CSP **SHALL** provide privacy training to all personnel and any third-party service providers who have access to sensitive information associated with the CSP's identity service.
3. The CSP **MAY** collect the Social Security Number (SSN) as an attribute when necessary for identity resolution, in accordance with the privacy requirements in Sec. 3.1.3. If SSNs are collected, CSPs **SHOULD** implement privacy protective techniques (e.g., transmitting and accepting derived attribute values rather than full attribute values) to limit the proliferation and retention of SSN data. Knowledge of an SSN is not sufficient to act as evidence of identity nor is it considered an acceptable method of verifying possession of the Social Security Card when used as evidence. If the SSN is collected on behalf of a federal, state, or local government agency, the CSP **SHALL** provide notice to the applicant for the collection in accordance with applicable laws.
4. At the time of collection, the CSP **SHALL** provide explicit notice to the applicant regarding the purpose for collecting the PII and attributes necessary for identity proofing, enrollment, and fraud mitigation, including whether such PII and attributes are voluntary or mandatory to complete the identity proofing process, the specific attributes and other sensitive data that the CSP intends to store in the applicant's subsequent subscriber account, the consequences for not providing the attributes, and the details of any records retention requirement if one is in place.

3.1.4. General Equity Requirements

In support of the goal of improved equity, and as part of its overall risk assessment process, CSPs assess the elements of their identity services to identify processes and technologies that may result in inequitable access, treatment, or outcomes for members of one group as compared to others. Where risks to equity are identified, CSPs proactively employ mitigations that will reduce or eliminate these discrepancies between demographic groups. Sec. 9 of this document provides a non-exhaustive list of

identity proofing processes and technologies that may be subject to inequitable access or outcomes, as well as possible mitigations.

Executive order [EO13985], *Advancing Racial Equity and Support for Underserved Communities Through the Federal Government*, requires each federal agency to assess whether, and to what extent, its programs and policies perpetuate systemic barriers to opportunities and benefits for people of color and other underserved groups. Additionally, executive order [EO13988], *Preventing and Combating Discrimination on the Basis of Gender Identity or Sexual Orientation*, sets policy that all persons are be treated with respect, regardless of gender identity or sexual orientation, and requires agencies to enforce this prohibition on sex discrimination.

CSPs **SHOULD** review the methods of assessment, data collection, and redress outlined in OMB Report, *A Vision for Equitable Data: Recommendations from the Equitable Data Working Group* [EO13985-vision] for the development of its equity assessment policy and practices.

The following requirements apply to all CSPs providing identity services at any IAL:

1. The CSP **SHALL** assess the elements of its identity proofing process(es) to identify processes or technologies that can result in inequitable access, treatment, or outcomes for members of one group as compared to others.
2. Based on the results of its assessment, the CSP **SHALL** document the measures it takes to mitigate the possibility of inequitable access, treatment, or outcomes.
3. The CSP **SHALL** re-assess the risks to equitable access, treatment, or outcomes periodically and any time the CSP makes changes to its identity service that affect the processes or technologies.
4. The CSP **SHALL NOT** make applicant participation in these risk assessments mandatory.
5. The CSP **SHALL** make the results of its equity assessment, including any associated mitigations, publicly available.

3.1.5. General Security Requirements

1. Each online transaction within the identity proofing process, including transactions that involve third parties, **SHALL** occur over an authenticated protected channel.
2. The CSP **SHALL** implement a means to prevent automated attacks on the identity proofing process. Acceptable means include, but are not limited to: bot detection, mitigation, and management solutions; behavioral analytics[4]; web application firewall settings; and network traffic analysis.

[4] Behavioral analytics in this context are used to determine if an interaction is indicative of an automated attack and not an effort to identify or authenticate a specific user based on a captured reference template for that user.

3. All PII collected as part of the identity proofing process **SHALL** be protected to maintain the confidentiality and integrity of the information, including the encryption of data at rest and the exchange of information using authenticated protected channels.
4. The CSP **SHALL** assess the risks associated with operating its identity service, according to the NIST *Risk Management Framework* [NIST-RMF] or equivalent risk management guidelines. At a minimum, the CSP **SHALL** apply appropriate controls consistent with [SP800-53] moderate baseline, regardless of IAL.
5. The CSP **SHOULD** assess risks associated with its use of third-party services and apply appropriate controls, as provided in the [SP800-161] *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*.

3.1.6. Redress Requirements

1. The CSP **SHALL** provide mechanisms for the redress of applicant complaints and for problems arising from the identity proofing process, including but not limited to: proofing failures, delays, and difficulties.
2. These mechanisms **SHALL** be easy for applicants to find and use.
3. The CSP **SHALL** assess the mechanisms for their efficacy in achieving a resolution of complaints or problems.

See Sec. 3.6 of [SP800-63] for more information about redress.

3.1.7. Additional Requirements for Federal Agencies

The following requirements apply to federal agencies, regardless of whether they operate their own identity service or use an external CSP as part of their identity service:

1. The agency **SHALL** consult with their Senior Agency Official for Privacy (SAOP) to conduct an analysis determining whether the collection of PII, including biometrics, to conduct identity proofing triggers Privacy Act requirements.
2. The agency **SHALL** consult with their SAOP to conduct an analysis determining whether the collection of PII, including biometrics, to conduct identity proofing triggers E-Government Act of 2002 [E-Gov] requirements.
3. The agency **SHALL** publish a System of Records Notice (SORN) to cover such collection, as applicable.[5]
4. The agency **SHALL** publish a Privacy Impact Assessment (PIA) to cover such collection, as applicable.

[5] For more information about SORNs, see OPM's *System of Records Notice (SORN) Guide* (https://www.opm.gov/information-management/privacy-policy/privacy-references/sornguide.pdf).

5. The agency **SHALL** consult with the senior official, office, or governance body responsible for diversity, equity, inclusion, and accessibility (DEIA) for their agency to determine how the identity proofing service can meet the needs of all served populations.
6. The agency **SHOULD** consult with public affairs and communications professionals within their organization to determine if a communications or public awareness strategy should be developed to accompany the roll-out of any new process, or an update to an existing process, including requirements associated with identity proofing. This may include materials detailing information about how to use the technology associated with the service, a Frequently Asked Questions (FAQs) page, prerequisites to participate in the identity proofing process (such as required evidence), webinars or other live or pre-recorded information sessions, or other media to support adoption of the identity service and provide applicants with a mechanism to communicate questions, issues, and feedback.
7. If the agency uses a third-party CSP, the agency SHALL conduct its own privacy risk assessment as part of its PIA process, using the CSP's privacy risk assessment as input to the agency's assessment.
8. If the agency uses a third-party CSP, the agency **SHALL** incorporate the CSP's assessment of equity risks into its own assessment of equity risks.

3.1.8. Requirements for Confirmation Codes

This section includes requirements for CSPs that support the use of confirmation codes.

Confirmation codes are used to confirm that an applicant has access to a postal address, email address, or phone number, for the purposes of future communications. They are also used as an identity verification option at IALs 1 and 2, as described in Sec. 2.5.1.

Confirmation codes used for these purposes **SHALL** include at least 6 decimal digits (or equivalent) from an approved random bit generator (see Sec. 3.2.12 of [SP800-63B]). The confirmation code may be presented as numeric or alphanumeric (e.g., Base64) for manual entry; a secure (e.g., https) link containing a representation of the confirmation code; or a machine-readable optical label, such as a QR code, containing the confirmation code.

Confirmation codes **SHALL** be valid for at most:

- 21 days, when sent to a validated postal address within the contiguous United States;
- 30 days, when sent to a validated postal address outside the contiguous United States;
- 10 minutes, when sent to a validated telephone number (SMS or voice); or

- 24 hours, when sent to a validated email address.

Upon its use, the CSP **SHALL** invalidate the confirmation code.

3.1.9. Requirements for Continuation Codes

This section includes requirements for CSPs that support the use of continuation codes.

Continuation codes are used to re-establish an applicant's linkage to an incomplete identity proofing or enrollment process. CSPs **MAY** use continuation codes when an applicant is unable to complete all the steps necessary to be successfully identity proofed and enrolled into the CSP's identity service in a single session, or when switching between different identity proofing types (such as from remote unattended to remote attended). Continuation codes are intended to be maintained offline (e.g., printed or written down) and stored in a secure location by the applicant for use in re-establishing linkage to a previous, incomplete session.

In order to facilitate the authentication of the applicant to a subsequent session, the CSP **SHALL** first bind an authenticator to a record or account established for the applicant prior to the cessation of the initial session. Continuation codes **SHALL** include at least 64 bits from an approved random bit generator (see Sec. 3.2.12 of [SP800-63B]). The continuation code **MAY** be presented as numeric or alphanumeric (e.g., Base64) for manual entry, or as a machine-readable optical label, such as a QR code containing the continuation code.

Verification of continuation codes **SHALL** be subject to throttling requirements, as provided in Sec. 3.2.2 of [SP800-63B]. Continuation codes **SHALL** be stored in hashed form, using a FIPS-approved or NIST recommended one-way function. Upon its use, the CSP **SHALL** invalidate the continuation code.

3.1.10. Requirements for Notifications of Identity Proofing

Notifications of proofing are sent to the applicant's validated address notifying them that they have been successfully identity proofed and provide information about the identity proofing event and subsequent enrollment, including how the recipient can repudiate they were the subject of the identity proofing.

The following requirements apply to CSPs and RPs that send notifications of proofing at any IAL.

Notifications of proofing:

1. **SHALL** be sent to a validated postal address, email address, or phone number.
2. **SHALL** include details about the identity proofing event, including the name of the identity service and the date the identity proofing was completed.

3. **SHALL** provide clear instructions, including contact information, on actions for the recipient to take in the case that they repudiate the identity proofing event.
4. **SHALL** provide additional information, such as how the organization or CSP protects the security and privacy of the information it collects and any responsibilities that the recipient has as a subscriber of the identity service.
5. **SHOULD** provide instructions on how to access their subscriber account or information about how the subscriber can update the information contained in that account.

In the event a subscriber repudiates having been identity proofed by the identity service, the CSP or RP **SHALL** respond in accordance to its fraud management program (Sec. 3.1.2).

3.1.11. Requirements for the Use of Biometrics

Biometrics is the automated recognition of individuals based on their biological and behavioral characteristics such as, but not limited to, fingerprints, voice patterns, or facial features (biological characteristics), and keystroke patterns, angle of holding a smart phone, screen pressure, typing speed, mouse movements, or gait (behavioral characteristics). As used in these guidelines, biometric data refers to any analog or digital representation of biological and behavioral characteristics at any stage of their capture, storage, or processing. This includes live biometric samples from applicants (e.g., facial images, fingerprint), as well as biometric references obtained from evidence (e.g., facial image on a driver's license, fingerprint minutiae template on identification cards). As applied to the identity proofing process, CSPs can use biometrics to verify that an individual is the rightful subject of identity evidence, to bind an individual to a new piece of identity evidence or credential, or for the purposes of fraud detection.

The following requirements apply to CSPs that employ biometrics as part of their identity proofing process:

1. CSPs **SHALL** provide clear, publicly available information about all uses of biometrics, what biometric data is collected, how it is stored, how it is protected, and information on how to remove biometric information consistent with applicable laws and regulations.
2. CSPs **SHALL** collect an explicit biometric consent from all applicants before collecting biometric information.
3. CSPs **SHALL** store a record of subscriber's consent for biometric use and associate it with subscriber's account.
4. CSPs **SHALL** have a documented, and publicly available, deletion process and default retention period for all biometric information.

5. CSPs **SHALL** support the deletion of all of a subscriber's biometric information upon the subscriber's request at any time, except where otherwise restricted by regulation, law, or statute.
6. CSPs **SHALL** have their biometric algorithms periodically tested by independent entities (e.g., accredited laboratories or research institutions) for their performance characteristics, including performance across demographic groups. At a minimum, the CSP **SHALL** have an algorithm retested after it has been updated.
7. CSPs **SHALL** assess the performance and demographic impacts of employed biometric technologies in conditions that are substantially similar to the operational environment and user base of the system. The user base is defined by both the demographic characteristics of the expected users as well as the devices they are expected to use. When such assessments include real-world users, participation by users **SHALL** be voluntary.
8. CSPs **SHALL** meet the following minimum performance thresholds for biometric usage in verification scenarios:
   - False match rate: 1:10,000 or better; and
   - False non-match rate: 1:100 or better
9. CSPs **MAY** use 1:N matching in support of resolution or fraud detection, pursuant to a privacy risk assessment. In 1:N scenarios, CSPs **SHALL** meet a minimum performance threshold for false positive identifications of 1:1,000. This applies to, and **SHALL** be tested for, each demographic group. Tests demonstrating this requirement **SHALL** employ a gallery no smaller than 90% of the current or intended operational size (N).
10. CSPs that make use of 1:N biometric matching for either resolution or fraud prevention purposes **SHALL NOT** decline a user's enrollment without a manual review by a trained proofing agent or trusted referee to confirm the automated matching results and confirm the results are not a false positive identification (for example, twins submitting for different accounts with the same CSP).
11. CSPs **SHALL** employ biometric technologies that provide similar performance characteristics for applicants of different demographic groups (age, race, sex, etc.). If significant performance differences across demographic groups are discovered, CSPs **SHALL** act expeditiously to provide redress options to affected individuals and to close performance gaps.
12. All biometric performance tests **SHALL** be conformant to ISO/IEC 19795-1:2021 and ISO/IEC 19795-10:2024, including demographics testing.
13. CSPs **SHALL** make performance and operational test results publicly available.

The following requirements apply to CSPs who collect biometric characteristics from applicants:

1. CSP **SHALL** collect biometrics in such a way that provides reasonable assurance that the biometric is collected from the applicant, and not another subject.
2. When collecting and comparing biometrics remotely, the CSP **SHALL** implement presentation attack detection (PAD) capabilities, which meet IAPAR performance metric <0.15, to confirm the genuine presence of a live human being and to mitigate spoofing and impersonation attempts.
3. When collecting biometrics onsite, the CSP **SHALL** have the operator view the biometric source (e.g., fingers, face) for the presence of non-natural materials and perform such inspections as part of the proofing process. All biometric presentation attack detection tests **SHALL** be conformant to ISO/IEC 30107-3:2023

3.1.12. Requirements for Evidence Validation Processes (Authenticity Checks)

Evidence validation can be conducted by remote optical capture and inspection (often called document authentication or doc auth) or conducted by visual inspection of a trained proofing agent or trusted referee. CSPs may employ either or both processes for evaluating the authenticity of identity evidence.

The following requirements apply to CSPs that employ optical capture and inspection for the purposes of determining document authenticity:

1. Automated evidence validation technology **SHALL** meet the following performance measures:
   - Document false acceptance rate (DFAR) of .10 or less. [6]
   - Document false rejection rate (DFRR) of .10 or less. [7]
2. If a Machine Readable Zone (MRZ) or barcode is present on the evidence, the optical capture and inspection **SHALL** compare the MRZ data to the printed data on the evidence for consistency.
3. CSPs **SHALL** implement live capture of documents during the validation process. CSPs **SHOULD** deploy technology controls to prevent the injection of document images, for example using document presence checks (also called document

[6] For the purposes of this document, the DFAR is the proportion of processed, fraudulent documents that the document validation system determined to be valid divided by the number of processed fraudulent documents. DFAR is defined as the number of fraudulent documents processed that were deemed valid by a document validation system divided by the number of processed fraudulent documents.

[7] For the purposes of this document, DFRR is the proportion of processed, genuine documents which the document validation system determined to be invalid. DFRR is defined as the number of genuine documents processed that were deemed invalid by a document validation system divided by the number of processed genuine documents.

liveness) or inspecting device characteristics to determine the presence of a virtual camera or device emulator.

4. CSPs **SHALL** assess the performance of employed optical capture and inspection technologies in conditions that are substantially similar to the operational environment and user base of the system. These tests **SHALL** account for all available identity evidence types that the CSPs allow to be validated using optical capture and inspection technology. Where subscribers' documents, PII, or images are used as part of the testing, it **SHALL** be on a voluntary basis and with subscriber notification and consent.
5. CSPs **SHOULD** have their evidence validation technology periodically tested by independent entities (e.g., accredited laboratories or research institutions) for their performance characteristics.
6. CSPs **SHALL** make the results of their testing available publicly.

> **Note:** These requirements apply to technologies that capture and validate images of physical identity evidence. They do not apply to validation techniques that rely on PKI or other cryptographic technologies that are embedded in the evidence themselves.

The following requirements apply to CSPs that employ visual inspection of evidence by trained proofing agents or trusted referees for the purposes of determining document authenticity:

1. Proofing agents and trusted referees **SHALL** be trained and provided resources to visually inspect all forms of evidence supported by the CSP. This training **SHALL** include:
   - Authentic layouts and topography of evidence types
   - Physical security features (e.g., raised letters, holographic features, microprinting)
   - Techniques for assessing features (e.g., tools to be used, where tactile inspection is needed, manipulation to view specific features)
   - Common indications of tampering (e.g., damage to the lamination, image modification)
2. When the setting allows for it (e.g., onsite attended proofing events), proofing agents and trusted referees **SHALL** be provided with specialized tools and equipment to support the visual inspection of evidence (e.g., magnifiers, ultraviolet lights, barcode readers).

3. Proofing agents and trusted referees who conduct visual inspection via remote means **SHALL** be provided with devices and internet connections that support sufficiently high-quality imagery to be able to effectively inspect presented evidence. In these instances, the visual validation **SHOULD** be supported by automated document validation technologies that provide additional confidence in the authenticity of the evidence (e.g., submitting and validating evidence in advance of an attended remote session)
4. Proofing agents and trusted referees **SHALL** be reviewed regarding their ability to visually inspect evidence on an ongoing basis, and be assessed and certified with at least annual evaluations.

> **Note:** Due to the potential number and permutations of identity evidence, these guidelines do not attempt to provide a comprehensive list of security features. CSPs need to provide evidence validation training specific to the types of identity evidence they accept.

3.1.13. Exception and Error Handling

Throughout the identity proofing process there are many points where errors or failures may occur. Such exceptions to a standard identity proofing workflow include: process failures, such as when a user does not possess the required evidence; technical failures, such as when an integrated service is not available; and failures due to user error, such as when an applicant is unable to capture a clear image of their identity evidence when using remote validation tools.

In order to increase the accessibility, usability, and equity of their identity proofing services, CSPs **SHALL** document their operational processes for dealing with errors and handling exceptions. These documented processes **SHALL** include providing trusted referees to support those applicants who are otherwise unable to meet the requirements of IALs 1 and 2. Additionally, CSPs **SHOULD** support the use of applicant references who can vouch for an applicant's attributes, conditions, or identity.

3.1.13.1. Trusted Referees Requirements

To increase accessibility and promote equal access to online government services, CSPs provide trusted referees. Trusted referees are used to facilitate the identity proofing and enrollment of individuals who are otherwise unable to meet the requirements for identity proofing to a specific IAL. A non-exhaustive list of examples of such individuals and demographic groups includes: individuals who do not possess and cannot obtain the required identity evidence; persons with disabilities; older individuals; persons experiencing homelessness; individuals with little or no access to online services or computing devices; persons without a bank account or with limited credit history;

victims of identity theft; individuals displaced or affected by natural disasters; and children under 18. The following requirements apply to the use of trusted referees:

1. The CSP **SHALL** provide notification to the public of the availability of trusted referee services and how such services are obtained.
2. The CSP **SHALL** establish written policies and procedures for the use of trusted referees as part of its practice statement, as specified in Sec. 3.1.1.
3. The CSP **SHALL** train and certify its trusted referees to make risk-based decisions that allow applicants to be successfully identity proofed based on their unique circumstances. At a minimum such training **SHALL** include:
   (a) Document identification and validation, such as common templates, security features, layouts, and topography.
   (b) Indicators of fraudulent documents, such as damage, tampering, modification, and material types
   (c) Facial and image comparisons to conduct verification of applicants against presented documents
   (d) Indicators of social engineering - such as distress, confusion, or coercion - exhibited by an applicant
   (e) Annual recertification of the trusted referee's capabilities
4. The CSP **SHALL** establish a record of any identity proofing session that involves a trusted referee, to include: what evidence was presented; which processes were completed (e.g., validation or verification); and, the reason(s) why a trusted referee was used (e.g., automated process failure, applicant request, established exception policy).
5. The CSP **MAY** offer trusted referee services for either onsite-attended or remote-attended sessions. These sessions **SHALL** be consistent with the requirements of these proofing types based on the IAL of the proofing event.

3.1.13.2. Trusted Referee Uses

Trusted referees offer a critical path for those who are unable to complete identity proofing by other means. However, given the number of possible failures that may occur within the proofing process, it is essential for CSPs to define the uses for which a trusted referee can be applied within their own service offerings. The following requirements apply to defining the integration of trusted referees into the identity proofing process:

1. CSPs **SHALL** document which types of exceptions and failures are eligible for the use of a trusted referee.
2. CSPs **SHALL** offer trusted referee services for failures of automated verification processes (e.g., biometric comparisons).

3. CSPs **SHOULD** offer trusted referee services for failures in completing automated validation processes, such as in cases of mismatched core attributes or the absence of the applicant in a record source.
   (a) CSPs **SHALL** provide a policy for additional evidence types that may be used to corroborate core attributes or changes in core attributes.
   (b) Trusted referees **SHALL** review additional evidence types for authenticity to the greatest degree allowed by the evidence.
   (c) If no authoritative or credible records are available to support validation, the trusted referee **MAY** compare the attributes on additional pieces of evidence with the strongest piece of evidence available to corroborate the consistency of core attributes.
   (d) If there is a partial mismatch of core attributes to authoritative records, the trusted referee **SHALL** review evidence that supports the legitimacy of the asserted attribute value (e.g., recent move or change of name).

3.1.13.3. Applicant Reference Requirements

Applicant references are individuals who participate in the identity proofing of an applicant in order to vouch for the applicant's identity, attributes, or circumstances related to the applicant's ability to complete identity proofing. Applicant representatives are not agents of the CSP, but instead are representatives of the applicant who have sufficient knowledge to aide in the completion of identity proofing when other forms of evidence, validation, and verification are not available.

The following requirements apply to the use of applicant references at IAL1 or IAL2:

1. The CSP **SHALL** provide notification to the public of the allowability of applicant references and any requirements for the relationship between the reference and an applicant.
2. The CSP **SHALL** establish written policies and procedures for the use of applicant references as part of its practice statement, as specified in Sec. 3.1.1.
3. The CSP **SHALL** identity proof an applicant reference to the same or higher IAL intended for the applicant. The CSP **SHALL** include the information collected, recorded, and retained for identity proofing the applicant references in its privacy risk assessment for identity proofing applicants, as required in section Sec. 3.1.3.
4. The CSP **SHALL** record the use of an applicant reference in the subscriber account as well as maintain a record of the applicant reference and their relationship to the applicant.
5. The RP **SHALL** conduct a risk assessment to determine the applicability, business requirements, and potential risks associated with excluding or including applicant references for proofing events.

3.1.13.4. Uses of Applicant References

Applicant references may take several different actions to support an applicant in the identity proofing process. CSPs and RPs **SHALL** establish all acceptable uses for applicant references in their Trust Agreements. These **MAY** include the following:

1. The applicant reference **MAY** vouch for one or more claimed core attributes relative to the applicant as part of evidence and attribute validation process.
2. The applicant reference **MAY** vouch for a specific condition or status of an applicant relative to the identity proofing process (e.g., homelessness, disaster scenarios) > **Note:** This information is intended to support risk determinations relative to the identity proofing event. Use of applicant reference statements relative to eligibility for status or benefits is outside the scope of these guidelines.
3. The applicant reference **MAY** vouch for the identity of the applicant in the absence of sufficient identity evidence.

In all instances, the CSP **SHALL** establish a record of the role the applicant reference played in the process and document these actions sufficient to support any applicable legal and regulatory requirements. This **MAY** include:

1. Capturing and recording the statements and assertions made by the applicant reference;
2. Capturing an electronic, digital signature, or physical signature of the applicant reference; or,
3. Capturing consent and acknowledgement relative to the legal and liability impacts of the applicant reference's statements.

CSPs **SHALL** make available to the applicant reference clear and understandable information relative to the legal and liability impacts that may result from their participation as an applicant reference.

3.1.13.5. Establishing Applicant Reference Relationships

In many cases, there will be business, legal, or fraud prevention reasons to confirm the relationship between the applicant and an applicant reference. Where such steps are deemed necessary by a risk assessment, the following requirements **SHALL** apply:

1. The CSP and RP **SHALL** establish requirements for applicant reference relationship confirmation processes and document this in any Trust Agreements.
2. The CSP **SHALL** make a list of acceptable evidence of relationship available to the applicant reference prior to initiating the relationship confirmation process
3. The CSP **SHALL** request evidence of the applicant's relationship (e.g., notarized power of attorney, a professional certification)

4. Upon successfully identity proofing an applicant, the CSP **SHALL** record the evidence used to confirm the applicant reference's relationship to the applicant in the subscriber account.

3.1.13.6. Requirements for Interacting with Minors

The following requirements apply to all CSPs providing identity proofing services to minors at any IAL.

1. The CSP **SHALL** establish written policy and procedures as part of its practice statement for identity proofing minors who may not be able to meet the evidence requirements for a given IAL.
2. When interacting with persons under the age of 13, the CSP **SHALL** ensure compliance with the Children's Online Privacy Protection Act of 1998 [COPPA], or other laws and regulations dealing with the protection of minors, as applicable.
3. CSPs **SHALL** support the use of applicant references when interacting with individuals under the age of 18.

3.2. Elevating Subscriber IALs

CSPs **SHOULD** allow subscribers to elevate identity assurance levels related to their subscriber accounts to support higher assurance transactions with RPs. For CSPs supporting these functions the following apply:

1. CSPs **SHALL** document their approved approaches for elevating assurance levels in their practice statements.
2. CSPs **SHALL** require subscribers to authenticate at the highest AAL available on their account prior to initiating the upgrade process.
3. CSPs **SHALL** collect, validate, and verify additional evidence, as mandated to achieve the higher IAL.
4. CSPs **SHOULD** avoid collecting, validating, and verifying previously processed evidence, though they **MAY** do so based on the age of the account, indicators of fraud, or if evidence has become invalidated since the original proofing event.

4. Identity Assurance Level Requirements

This section is normative.

4.1. Identity Assurance Level 1 Requirements

Identity proofing processes at IAL1 allow for a range of acceptable techniques in order to detect the fraudulent claims to identities by malicious actors, while facilitating user adoption, minimizing the rejection of legitimate users, and reducing application departures. The use of biometric matching, such as the automated comparison of a facial portrait to supplied evidence, at IAL1 is optional, providing pathways to proofing and enrollment where such collection may not be viable.

4.1.1. Proofing Types

1. IAL1 Identity Proofing **MAY** be delivered through any proofing type, as described in Sec. 2.1.3.
2. CSPs **SHALL** offer Unattended Remote identity proofing as an option.
3. CSPs **SHALL** offer at least one method of Attended (Remote or Onsite) identity proofing as an option.
4. CSPs MAY combine proofing types and their stated requirements to create hybrid processes. For example, a CSP might leverage remote unattended identity proofing validation processes in advance of a remote attended session where verification will take place. Where such steps are combined, CSPs SHALL document their processes in alignment of requirements of each proofing type that is applied.

4.1.2. Evidence Collection

For each identity proofing type, the CSP **SHALL** collect the following:

1. One piece of FAIR evidence or better (i.e., STRONG, SUPERIOR) evidence

For onsite attended identity proofing at IAL1, organizations **SHOULD** prioritize the use of evidence (FAIR or STRONG) that contains a facial portrait, which can be used for verification purposes. While forms of evidence that do not contain a facial portrait **MAY** be used for such sessions, the associated verification requirements (e.g., returning a confirmation code) may result in additional burden on applicants.

4.1.3. Attribute Collection

The CSP **SHALL** collect all Core Attributes. Validated evidence is the preferred source of identity attributes. If the presented identity evidence does not provide all the attributes that the CSP considers core attributes, it **MAY** collect attributes that are self-asserted by the applicant.

4.1.4. Evidence Validation

Each piece of evidence presented **SHALL** be validated using one of the following techniques:

1. Confirming the authenticity of digital evidence through interrogation of digital security features (e.g., signatures on assertions or data).
2. Confirming the authenticity of physical evidence using automated scanning technology able to detect physical security features.
3. Confirming the integrity of physical security features of presented evidence through visual inspection by a proofing agent using real-time or asynchronous processes (e.g., offline manual review).
4. Confirming the integrity of physical security features through physical and tactile inspection of security features by a proofing agent at an onsite location.

4.1.5. Attribute Validation

1. The CSP **SHALL** validate all core attributes and the government identifier against an authoritative or credible source to determine accuracy.
2. CSPs **SHOULD** correlate the data on evidence, self-asserted, and as presented by credible and authoritative sources for consistency.
3. CSPs **SHOULD** validate the reference numbers of presented identity evidence if available.

4.1.6. Verification Requirements

The CSP **SHALL** verify the applicant's ownership of one piece of evidence using one of the following processes:

1. Confirming the applicant's ability to return a confirmation code delivered to a validated address associated with the evidence;
2. Confirming the applicant's ability to return a micro-transaction value delivered to a validated financial or similar account;
3. Confirming the applicant's ability to successfully complete an authentication and federation protocol equivalent to AAL2/FAL2, or higher, to access an account related to the identity evidence;
4. Comparing the applicant's facial image to a facial portrait on evidence via an automated comparison.
5. Visually comparing the applicant's facial image to a facial portrait on evidence, or in records associated with the evidence, during either an onsite attended session (in-person with a proofing agent), a remote attended session (live video with a proofing agent), or an asynchronous process (i.e., visual comparison made by a proofing agent at a different time).

6. Comparing a stored biometric on identity evidence, or in authoritative records related to the evidence, to a sample provided by the applicant.

4.1.7. Remote Attended Requirements

1. All video sessions **SHALL** take place using a service that allows for the exchange of information over an authenticated protected channel.
2. During the video session, the applicant **SHALL** remain in view of the proofing agent during each step of the proofing process.
3. The video quality **SHALL** be sufficient to support the necessary steps in the validation and verification processes, such as inspecting evidence and making visual comparisons of the user to the evidence.
4. The proofing agent **SHALL** be trained to identify signs of manipulation, coercion, or social engineering occurring during the recorded session.
5. CSPs **MAY** record and maintain video sessions for fraud prevention and prosecution purposes pursuant to a privacy risk assessment, as defined in Sec. 3.1.3.1. If the CSP records session, the following further requirements apply:
   (a) The CSP **SHALL** notify the applicant of the recording prior to initiating a recorded session.
   (b) The CSP **SHALL** gain consent from the applicant to prior to initiating a recorded session.
   (c) The CSP **SHALL** publish their retention schedule and deletion processes for all video records.
6. The CSP **SHOULD** introduce challenges and response features into their video sessions that are randomized or periodically changed to deter deep fakes and pre-recorded materials from being used to defeat the proofing process. These MAY be shifting questions, changes to the orders of sessions, or physical cues that would be hard for attackers to predict.
7. The CSP **SHALL** provide proofing agents with a method or mechanism to flag events for potential fraud.

4.1.8. Onsite Attended Requirements

1. The CSP **SHALL** provide a physical setting in which onsite identity proofing sessions are conducted.
2. The CSP **SHALL** ensure all information systems and technology leveraged by proofing agents and trusted referees are protected consistent with FISMA Moderate or comparable levels of controls.

3. CSP proofing agents **SHALL** be trained to identify signs of manipulation, coercion, or social engineering occurring during the onsite session.
4. CSPs **MAY** record and maintain video sessions for fraud prevention and prosecution purposes pursuant to a privacy risk assessment, as defined in Sec. 3.1.3.1. If the CSP records session, the following further requirements apply:
   (a) The CSP **SHALL** notify the applicant of the recording prior to initiating a recorded session.
   (b) The CSP **SHALL** gain consent from the applicant prior to initiating a recorded session.
   (c) The CSP **SHALL** publish their retention schedule and deletion processes for all video records.
5. The CSP **SHALL** provide proofing agents with a method or mechanism to safely flag events for potential fraud.

4.1.9. Onsite Unattended Requirements (Devices & Kiosks)

1. All devices **SHALL** be safeguarded from tampering through either observation by CSP representatives or through physical and digital tamper prevention features.
2. All devices **SHALL** be protected by appropriate baseline security features comparable to FISMA Moderate controls – including Malware Protection, Admin Specific Access Controls, and Software Update processes.
3. All devices **SHALL** be inspected periodically by trained technicians to deter tampering, modification, or damage.

4.1.10. Initial Authenticator Binding

Upon the successful completion of the identity proofing process, a unique subscriber account is established and maintained for the applicant (now subscriber) in the CSP's identity system. One or more authenticators can be associated (bound) to the subscriber's account, either at the time of identity proofing or at a later time. See Sec. 5 for more information about subscriber accounts.

1. The CSP **SHALL** provide the ability for the applicant to bind an authenticator using one of the following methods:
   (a) The remote enrollment of a subscriber-provided authenticator, consistent with the requirements for the authenticator type as defined in Sec. 4.1.3 of [SP800-63B].
   (b) Distribution of a physical authenticator to a validated address of record.
   (c) Distribution or onsite enrollment of an authenticator.

2. Where authenticators are bound outside of a single protected session with the user, the CSP **SHALL** confirm the presence of the intended subscriber through one of the following methods:
   (a) Return of an confirmation code, or
   (b) Comparison against a biometric collected at the time of proofing.

4.1.11. Notification of Proofing

Upon the successful completion of identity proofing at IAL1, the CSP **SHALL** send a notification of proofing to a validated address for the applicant, as specified in Sec. 3.1.10.

4.2. Identity Assurance Level 2 Requirements

IAL2 identity proofing includes additional evidence, validation, and verification requirements in order to provide increased mitigation against impersonation attacks and other identity proofing errors relative to IAL1. IAL2 can be achieved through a number of different types of proofing (e.g., remote unattended, remote attended, etc.) and identity verification at IAL2 can be accomplished with or without the use of biometrics. To provide clear options to achieving IAL2, this section presents three different pathways to achieving alignment with IAL2 outcomes and requirements: IAL2 Verification - Non-Biometric Pathway; IAL2 Verification - Biometric Pathway; and IAL2 Verification - Digital Evidence Pathway. These different options do not imply different security or assurance outcomes; instead they present requirements in a manner that allows for clear selection of non-biometric methods that can be used to achieve IAL2.

4.2.1. Proofing Types

1. Identity proofing at IAL2 **MAY** be delivered through any proofing type, as described in Sec. 2.1.3.
2. CSPs **SHALL** offer Unattended Remote identity proofing as an option.
3. CSPs **SHALL** offer at least one method of Attended (Remote or Onsite) identity proofing as an option.
4. CSPs **MAY** combine elements of different proofing types to create hybrid processes. For example, a CSP might leverage remote unattended identity proofing validation processes in advance of a remote attended session where verification will take place. If a CSP employs a hybrid process, it **SHALL** document how the process satisfies the requirements associated with the associated proofing types.

4.2.2. Evidence Collection

For all types of proofing the CSP **SHALL** collect:

1. One piece of FAIR Evidence and one piece of STRONG; or
2. One piece of SUPERIOR.

4.2.3. Attribute Collection

Same as IAL1

4.2.4. Evidence Validation

1. Each piece of FAIR or STRONG evidence presented **SHALL** be validated using one of the following techniques.
   (a) Confirming the authenticity of digital evidence through interrogation of digital security features (e.g., signatures on assertions or data).
   (b) Confirming the authenticity of physical evidence using automated scanning technology able to detect physical security features.
   (c) Confirming the integrity of physical security features of presented evidence through visual inspection by a proofing agent using real-time or asynchronous processes (e.g., offline manual review).
   (d) Confirming the integrity of physical security features through physical and tactile inspection of security features by a proofing agent at an onsite location.
2. Each Piece of SUPERIOR evidence **SHALL** be validated through cryptographic verification of the evidence contents and the issuing source, including digital signature verification and the validation of any trust chain back to a trust anchor. SUPERIOR evidence unable to be validated using cryptographic verification **SHALL** be considered STRONG evidence and validated consistent with the requirements above.

4.2.5. Attribute Validation

1. The CSP **SHALL** validate all core attributes by either:
   (a) Comparing the government identifier and core attributes against an authoritative or credible source to determine accuracy; or
   (b) Validating the accuracy of digitally signed attributes contained on SUPERIOR evidence through the public key of the issuing source.
2. CSPs **SHOULD** correlate the attributes collected from evidence, self-assertion, and as presented by credible and authoritative sources for consistency.
3. CSPs **SHOULD** validate the reference numbers of presented identity evidence if available.

4.2.6. Verification Requirements

Verification pathways **SHOULD** be implemented consistent with relevant policy and be responsive to the use cases, populations, and threat environment of the online service being protected. CSPs **SHOULD** deploy more than one pathway to IAL2 verification and **MAY** combine pathways in order to achieve desired outcomes.

4.2.6.1. IAL2 Verification - Non-Biometric Pathway

The IAL2 Non-Biometric Pathway provides verification methods that do not use automated comparison of biometric samples provided by the applicant. Non-biometric processes will often still include biometric data being collected and verified - for example, through a visual comparison performed by a proofing agent and images contained on identity evidence - but comparisons are not done through automated means. Additional verification methods that may not require the use of automated biometric comparison are also included in the IAL2 Verification - Digital Evidence Pathway requirements specified in Sec. 4.2.6.2.

1. The CSP **SHALL** verify the applicant's ownership of all presented identity evidence.
2. Approved non-biometric methods for verifying FAIR evidence at IAL2 include:
   (a) Confirming the applicant's ability to return a confirmation code delivered to a validated address associated with the evidence (e.g., postal address, email address, phone number)
   (b) Visually comparing the applicant's facial image to a facial portrait on evidence, or in records associated with the evidence, during either an onsite attended session (in-person with a proofing agent), a remote attended session (live video with a proofing agent), or an asynchronous process (i.e., visual comparison made by a proofing agent at a different time)
3. Approved non-biometric methods for verifying STRONG and SUPERIOR evidence at IAL2 include:
   (a) Confirming the applicant's ability to return a confirmation code delivered to a physical address (i.e., postal address) that was obtained from the evidence and was validated with an authoritative source
   (b) Visually comparing the applicant's facial image to a facial portrait on evidence, or in records associated with the evidence, during either an onsite attended session (in-person with a proofing agent), a remote attended session (live video with a proofing agent), or an asynchronous process (i.e., visual comparison made by a proofing agent at a different time)

4.2.6.2. IAL2 Verification - Digital Evidence Pathway

The IAL2 Digital Evidence Pathway provides a means of allowing individuals to make use of digital forms of evidence, such as digital credentials (sometimes referred to as *digital identity documents*) or digital accounts as part of the verification process. This pathway achieves verification by confirming the individual's ability to access evidence through digital means.

1. The CSP **SHALL** verify the applicant's ownership of all pieces of presented identity evidence.
2. Approved digital evidence verification methods for FAIR evidence at IAL2 include:
   (a) Confirming the applicant's ability to return a micro-transaction value delivered to a validated account (e.g., a checking account)
   (b) Confirming the applicant's ability to return a confirmation code delivered to a validated digital address associated with the digital evidence (e.g., MNO/Phone account)
   (c) Confirming the applicant's ability to successfully complete an authentication and federation protocol equivalent to AAL2/FAL2 to access an account related to the identity evidence
3. Approved digital evidence verification methods for STRONG evidence at IAL2 include:
   (a) Confirming the applicant's ability to successfully complete an authentication and federation protocol equivalent to AAL2/FAL2, or higher, to access an account related to the identity evidence
4. Approved digital evidence verification methods for SUPERIOR evidence at IAL2 include:
   (a) Confirming the applicant's ability to successfully complete an authentication and federation protocol equivalent to AAL3/FAL2, or higher, to access an account related to the identity evidence

4.2.6.3. IAL2 Verification - Biometric Pathway

The IAL2 Biometric Pathway provides verification methods that support automated comparison of biometric samples provided by the applicant.

1. The CSP **SHALL** verify the applicant's ownership of all pieces of presented identity evidence.
2. Approved biometric methods for verifying FAIR evidence at IAL2 include:
   (a) Comparing the applicant's facial image to a facial portrait on evidence via an automated comparison

3. Approved methods for verifying STRONG and SUPERIOR evidence for use in the IAL2 Biometric Pathway include:
   (a) Comparing the applicant's facial image to a facial portrait on evidence via an automated comparison
   (b) Comparing, via automated means, a non-facial portrait biometric stored on identity evidence, or in-records associated with the evidence, to a live sample provided by the applicant

4.2.7. Remote Attended Requirements

Same as IAL1.

4.2.8. Onsite Attended Requirements

Same as IAL1.

4.2.9. Onsite Unattended Requirements (Devices & Kiosks)

Same as IAL1.

4.2.10. Notification of Proofing

Same as IAL1.

4.2.11. Initial Authenticator Binding

Same as IAL 1.

4.3. Identity Assurance Level 3

IAL3 adds additional rigor to the steps required at IAL2 and is subject to additional and specific processes (including the use of biometric information comparison, collection, and retention) to further protect the identity and RP from impersonation and other forms of identity fraud. In addition, identity proofing at IAL3 must be attended by a CSP proofing agent, as described in Sec. 2.1.2.

4.3.1. Proofing Types

IAL 3 Identity Proofing **SHALL** only be delivered as Onsite Attended. The Proofing Agent **MAY** be collocated or attend the proofing session remotely via a CSP controlled kiosk or device.

4.3.2. Evidence Collection

1. For all types of IAL 3 identity proofing the CSP **SHALL** collect either:
   (a) One piece of STRONG and one piece of FAIR (or better), or
   (b) One piece of SUPERIOR

4.3.3. Attribute Requirements

1. The CSP **SHALL** collect all core attributes. Validated evidence is the preferred source of identity attributes. If the presented identity evidence does not provide all the attributes that the CSP considers core attributes, it **MAY** collect attributes that are self-asserted by the applicant.
2. The CSP **SHALL** collect and retain a biometric sample from the applicant during the identity proofing process to support account recovery, non-repudiation, and establish a high level of confidence that the same participant is present in the proofing and issuance processes (if done separately). CSPs **MAY** choose to periodically re-enroll user biometrics based on the modalities they use and the likelihood that subscriber accounts will persist long enough to warrant such a refresh.

4.3.4. Evidence Validation

1. Each piece of FAIR or STRONG evidence presented **SHALL** be validated using one of the following techniques.
   (a) Confirming the authenticity of digital evidence through interrogation of digital security features (e.g., signatures on assertions or data).
   (b) Confirming the authenticity of physical evidence using automated scanning technology able to detect physical security features.
   (c) Confirming the integrity of physical security features of presented evidence through physical inspection by a proofing agent using real-time or asynchronous processes (e.g., offline manual review).
   (d) Confirming the integrity of physical security features through physical and tactile inspection of security features by a proofing agent at an onsite location.
2. Each Piece of SUPERIOR evidence **SHALL** be validated through cryptographic verification of the evidence contents and the issuing source, including digital signature verification and the validation of any trust chain back to a trust anchor.

4.3.5. Attribute Validation

1. The CSP **SHALL** validate all core attributes by either:
   (a) Comparing the core attributes against an authoritative or credible source to determine accuracy; or
   (b) Validating the accuracy of digitally signed attributes contained on SUPERIOR evidence through the public key of the issuing source.
2. CSPs **SHOULD** correlate the attributes collected from evidence, self-assertion, and as presented by credible and authoritative sources for consistency.
3. CSPs **SHOULD** validate the reference numbers of presented identity evidence if available.

4.3.6. Verification Requirements

1. The CSP **SHALL** verify the applicants ownership of the strongest piece of evidence (STRONG or SUPERIOR) by one of the following methods:
   (a) Confirming the applicant's ability to successfully authenticate to a physical device or application (for example a mobile driver's license) and comparing a digitally protected and transmitted facial portrait to the applicant.
   (b) Comparing the applicant's facial image to the facial portrait on evidence via an automated comparison.
   (c) Visually comparing the applicant's facial image to the facial portrait on evidence, either during an onsite attended session or a remote attended session (live video).
   (d) Comparing a stored biometric on identity evidence, or in authoritative records associated with the evidence, to a sample provided by the applicant.

4.3.7. Onsite Attended Requirements (Locally Attended)

1. The CSP **SHALL** provide a secure, physical setting in which onsite identity proofing sessions are conducted.
2. The CSP **SHALL** provide sensors and capture devices for the collection of biometrics from the applicant.
3. The CSP **SHALL** have the proofing agent view the source of the collected biometric for the presence of any non-natural materials.
4. The CSP **SHALL** have the proofing agent collect the biometric samples in such a way that ensures the sample was collected from the applicant and no other source.

5. The CSP **SHALL** ensure all information systems and technology leveraged by proofing agents and trusted referees are protected consistent with FISMA Moderate or comparable levels of controls to include physical controls for the proofing facility.
6. CSP proofing agents **SHALL** be trained to identify signs of manipulation, coercion, or social engineering occurring during the onsite session.
7. CSPs **MAY** record and maintain video sessions for fraud prevention and prosecution purposes pursuant to a privacy risk assessment, as defined in Sec. 3.1.3.1. If the CSP records session, the following further requirements apply:
   (a) The CSP **SHALL** notify the applicant of the recording prior to initiating a recorded session.
   (b) The CSP **SHALL** gain consent from the applicant to prior to initiating a recorded session.
   (c) The CSP **SHALL** publish their retention schedule and deletion processes for all video records.
8. The CSP **SHALL** provide proofing agents with a method or mechanism to safely flag events for potential fraud.

4.3.8. Onsite Attended Requirements (Remotely Attended - Formerly Supervised Remote Identity Proofing)

1. The CSP **MAY** offer a remote means of interacting with a proofing agent whereby the agent and the applicant do not have to be at the same facility. In this scenario, the following requirements apply:
   (a) The CSP **SHALL** monitor the entire identity proofing session through a high-resolution video transmission with the applicant.
   (b) The CSP **SHALL** have a live proofing agent participate remotely with the applicant for the evidence collection, evidence validation, and verification steps of the identity proofing process. Data entry of attributes for resolution and enrollment **MAY** be done without the presence of a live proofing agent.
   (c) The CSP **SHALL** require all actions taken by the applicant during the evidence collection, evidence validation, and verification steps to be clearly visible to the remote proofing agent.
   (d) The CSP **SHALL** require that all digital validation and verification of evidence (e.g., via chip or wireless technologies) be performed by integrated scanners and sensors (e.g., embedded fingerprint reader).

(e) All devices used to support interaction between the proofing agent and the applicant **SHALL** be safeguarded from tampering through observation by CSP representatives or monitoring devices (e.g., cameras) and through physical and digital tamper prevention features.

(f) All devices used to support interaction between the proofing agent and the applicant **SHALL** be protected by appropriate baseline security features comparable to FISMA Moderate controls, including malware protection, admin-specific access controls, and software update processes.

(g) All devices used to support interaction between the proofing agent and the applicant **SHALL** be inspected periodically by trained technicians to deter tampering, modification, or damage.

4.3.9. Notification of Proofing

Same as IAL1.

4.3.10. Initial Authenticator Binding

1. The CSP **SHALL** distribute or enroll the applicant's initial authenticator during an onsite attended interaction with a proofing agent.
2. If the CSP distributes or enrolls the initial authenticator outside of a single, protected session with the user, the CSP **SHALL** compare a biometric sample collected from the applicant to the one collected at the time of proofing, prior to issuance of the authenticator.
3. The CSP **MAY** request that the applicant bring the identity evidence used during the proofing process to the issuance event to further strengthen the process of binding the authenticators to the applicant.

4.4. Summary of Requirements

Table 1 summarizes the requirements for each of the identity assurance levels:

Table 1. IAL Requirements Summary

Process	**IAL1**	**IAL2**	**IAL3**
Proofing Types	Remote Unattended Remote Attended Onsite Unattended Onsite Attended	Same as IAL1	Onsite Attended
Evidence Collection	*Unattended:* –1 FAIR or –1 STRONG *Attended:* –1 FAIR w/ image or –1 STRONG	*For all proofing types:* –1 FAIR and 1 STRONG or –1 SUPERIOR	–1 STRONG + 1 FAIR or –1 SUPERIOR
Attribute Collection	All Core Attributes	All Core Attributes	All Core Attributes + Biometric Sample
Evidence Validation	*Physical Evidence:* –automated doc auth. –visual inspection *Digital Evidence:* –interrogation of digital security features	*Physical Evidence:* –automated doc. auth. –visual inspection –physical/tactile inspection *Digital Evidence:* –interrogation of digital security features *SUPERIOR Evidence:* –Dig. sig. verification	*Physical Evidence:* –automated doc. auth. –physical inspection –physical/tactile inspection *Digital Evidence:* –interrogation of digital security features *SUPERIOR Evidence:* –Dig. sig. verification
Attribute Validation	Confirmation of core attributes against authoritative or credible sources.	Confirmation of core attributes against authoritative or credible sources. Confirmation of digitally signed attributes through signature verification.	Confirmation of core attributes against authoritative or credible sources. Confirmation of digitally signed attributes through digital signature verification.
Verification	Verify applicant's ownership of either the FAIR evidence or the STRONG evidence per 4.1.6	Verify applicant's ownership of all presented evidence using methods provided in 4.2.6	Verify applicant's ownership of all presented evidence using methods provided in 4.3.6

5. Subscriber Accounts

This section is normative.

5.1. Subscriber Accounts

The CSP **SHALL** establish and maintain a unique subscriber account for each active subscriber in the CSP identity system from the time of enrollment to the time of account closure. The CSP establishes a subscriber account to record each subscriber as a unique identity within its identity service and to maintain a record of all authenticators associated with that account.

The CSP **SHALL** assign a unique identifier to each subscriber account. The identifier **SHOULD** be randomly generated by the CSP system and of sufficient length and entropy to ensure uniqueness within its user population and to support federation with RPs, where applicable. The identifier **MAY** be used as a subject identifier in the generation of assertions, consistent with [SP800-63C].

At a minimum, the CSP **SHALL** include the following information in each subscriber account:

- The unique identifier associated with the subscriber account
- Any subject identifiers established for the subscriber, including any RP specific subject identifiers
- A record of the identity proofing steps completed for the subscriber, including:
  - The type and issuer of identity evidence
  - The type of proofing (Remote Unattended, Remote Attended, Onsite Attended, Onsite Unattended)
  - The validation and verification methods used
  - The use of a trusted referee or other exception handling process
  - The use of an applicant reference, including a unique identifier for the applicant reference
- Maximum IAL successfully achieved for the identity proofing of the subscriber
- Records of any applicant consent agreements related to the collection and processing of information about the applicant, including biometrics, throughout the subscriber account lifecycle
- All authenticators currently bound to the subscriber account, whether registered at enrollment or subsequent to enrollment
- Attributes that were validated during the identity proofing process or in subsequent transactions to support RP access

5.2. Subscriber Account Access

The CSP **SHALL** provide the capability for subscribers to authenticate and access information in their subscriber account.

For subscriber accounts that contain PII, this capability **SHALL** be accomplished through AAL2 or AAL3 authentication processes using authenticators registered to the subscriber account.

5.3. Subscriber Account Maintenance and Updates

The CSP **SHALL** provide the capability for a subscriber to request the CSP to update information contained in their subscriber account. The CSP **MAY** provide a mechanism for subscribers to update any non-core attributes directly.

The CSP **SHALL** validate any changes to core attribute information maintained in the subscriber account.

The CSP **SHALL** provide notice to the subscriber of any updates made to information in the subscriber account.

The CSP **SHALL** provide the capability for the subscriber to report any unauthorized access or potential compromise to information in their subscriber account.

5.4. Subscriber Account Suspension or Termination

The CSP **SHALL** promptly suspend or terminate the subscriber account when one of the following occurs:

- The subscriber elects to terminate their subscriber account with the CSP.
- The CSP determines that the subscriber account has been compromised.
- The CSP determines that the subscriber has violated the policies or rules for participation in the CSP identity service.
- The CSP determines that the subscriber account is inactive in accordance with the policies or rules established by the CSP.
- The CSP receives notification of a subscriber's death from an authoritative source.
- The CSP receives a legal instrument from a court to terminate a subscriber's account.
- The CSP ceases identity system and services operations.

The CSP **SHALL** provide notification to the subscriber that their subscriber account has been suspended or terminated. Such notices **SHALL** include information about why the account was suspended or terminated, reactivation or renewal options, and any options for redress if the subscriber thinks the account was suspended or terminated in error.

1988 The CSP **SHALL** delete any personal or sensitive information from the subscriber account
1989 records following account termination in accordance with the record retention and
1990 disposal requirements, as documented in its practices statement Sec. 3.1.1.

6. Threats and Security Considerations

This section is informative.

Effective protection of identity proofing processes requires the layering of security controls and processes throughout a transaction with a given applicant. To achieve this, it is necessary to understand where and how threats can arise and compromise enrollments. There are three general categories of threats to the identity proofing process:

- **Impersonation**: where an attacker attempts to pose as another, legitimate, individual (e.g., identity theft)
- **False or Fraudulent Representation**: where an attacker may create a false identity or false claims about an identity (e.g., synthetic identity fraud)
- **Infrastructure**: where attackers may seek to compromise confidentiality, availability, and integrity of the infrastructure, data, software, or people supporting the CSP's identity proofing process (e.g., distributed denial of service, insider threats)

This section focuses on impersonation and false or fraudulent representation threats, as infrastructure threats are addressed by traditional computer security controls (e.g., intrusion protection, record keeping, independent audits) and are outside the scope of this document. For more information on security controls, see [SP800-53], *Recommended Security and Privacy Controls for Federal Information Systems and Organizations*.

Table 2. Identity Proofing and Enrollment Threats

Attack/Threat	Description	Example
Automated Enrollment Attempts	Attackers leverage scripts and automated processes to rapidly generate large volumes of enrollments	Bots leverage stolen data to submit benefits claims.
Evidence Falsification	Attacker creates or modifies evidence in order to claim an identity	A fake driver's license is used as evidence.
Synthetic Identity fraud	Attacker fabricates evidence of identity that is not associated with a real person	Opening a credit card in a fake name to create a credit file.
Fraudulent Use of Identity (Identity Theft)	Attacker fraudulently uses another individual's identity or identity evidence	An individual uses a stolen passport.
Social Engineering	Attacker convinces a legitimate applicant to provide identity evidence or complete the identity proofing process under false pretenses	An individual submits their identity evidence to an attacker posing as a potential employer.
False Claims	Attacker associates false attributes or information with a legitimate identity	An individual falsely claims residence in a state in order to obtain a benefit that is available only to state residents.
Video or Image Injection Attack	Attacker creates a fake video feed of an individual associated with a real person	A deepfake video is used to impersonate an individual portrayed on a stolen driver's license.

6.1. Threat Mitigation Strategies

Threats to the enrollment and identity proofing process are summarized in Table 2. Related mechanisms that assist in mitigating the threats identified above are summarized in Table 3. These mitigations should not be considered comprehensive but a summary of mitigations detailed more thoroughly at each Identity Assurance Level and applied based on the risk assessment processes detailed in Sec. 3 of [SP800-63].

Table 3. Identity Proofing and Enrollment Threat Mitigation Strategies

Threat/Attack	Mitigation Strategies	Normative Reference(s)
Automated Enrollment Attempts	Web Application Firewall (WAF) controls and bot detection technology. Out-of-band engagement (e.g., confirmation codes). Biometric verification and liveness detection mechanisms. Traffic and network analysis capabilities to identify indications or malicious traffic.	3.1.5, 3.1.8, 3.1.11
Evidence Falsification	Validation of core attributes with authoritative or credible sources. Validation of physical or digital security features of the presented evidence.	4.1.4 & 4.1.5 (IAL1), 4.2.4 & 4.2.5 (IAL2), 4.3.4 & 4.3.5 (IAL3)
Synthetic Identity Fraud	Collection of identity evidence. Validation of core attributes with authoritative or credible sources. Biometric comparison of the applicant to validated identity evidence or biometric data. Checks against vital statistics repositories (e.g., Death Master File).	3.1.2.1, 4.1.2, 4.1.5, & 4.1.6 (IAL1), 4.2.2, 4.2.5, & 4.2.6 (IAL2), 4.3.2, 4.3.5, & 4.3.6 (IAL3)
Fraudulent Use of Identity (Identity Theft)	Biometric comparison of the applicant to validated identity evidence or biometric data. Presentation attack detection measures to confirm the genuine presence of applicant. Out-of-band engagement (e.g., confirmation codes) and notice of proofing. Checks against vital statistics repositories (e.g., Death Master File). Fraud, transaction, and behavioral analysis capabilities to identify indicators of potentially malicious account establishment.	3.1.2.1, 3.1.8, 3.1.10, 3.1.11, 4.1.6 (IAL1), 4.2.6 (IAL2), 4.3.6 (IAL3)
Social Engineering	Training of trusted referees to identify indications of coercion or distress. Out-of-band engagement and notice of proofing to validated address. Provide information and communication to end users on common threats and schemes. Offer onsite in-person attended identity proofing option.	2.1.3, 3.1.8, 3.1.110, 3.1.13.1, 8.4
False Claims	Geographic restrictions on traffic. Validation of core attributes with authoritative or credible sources.	3.1.2.1, 4.1.5 (IAL1), 4.2.5 (IAL2), 4.3.5 (IAL3)
Video or Image Injection Attack	Use of a combination of active and passive PAD. Use of authenticated protected channels for communications between devices and servers running matching. Authentication of biometric sensors where feasible. Monitoring and analysis of incoming video and image files to detect signs of injection.	3.1.8

6.2. Collaboration with Adjacent Programs

Identity proofing services typically serve as the front door for critical business or service functions. Accordingly, these services should not operate in a vacuum. A close coordination of identity proofing and CSP functions with cybersecurity teams, threat intelligence teams, and program integrity teams can enable a more complete protection of business capabilities while constantly improving identity proofing capabilities. For example, payment fraud data collected by program integrity teams could provide indicators of compromised subscriber accounts and potential weaknesses in identity proofing implementations. Similarly, threat intelligence teams may receive indications of new tactics, techniques, and procedures that may impact identity proofing processes. CSPs and RPs should seek to establish consistent mechanisms for the exchange of information between critical security and fraud stakeholders. Where the CSP is external, this may be complicated, but should be addressed through contractual and legal mechanisms, to include technical and interoperability considerations. All data collected, transmitted, or shared should be minimized and subject to a detailed privacy and legal assessment.

7. Privacy Considerations

This section is informative.

These privacy considerations provide additional information in implementing the requirements set forth in Sec. 3.1.3 and are intended to guide CSPs and RPs in designing identity systems that prioritize protecting their users' privacy.

7.1. Collection and Data Minimization

These guidelines permit the collection and processing of only the PII necessary to validate the claimed identity, associate the claimed identity to the applicant, mitigate fraud, and to provide RPs with attributes they may use to make authorization decisions. Collecting unnecessary PII can create confusion regarding why information that is not being used for the identity proofing service is being collected. This leads to invasiveness or overreach concerns, which can lead to a loss of applicant trust. Further, PII retention can become vulnerable to unauthorized access or use. Data minimization reduces the amount of PII vulnerable to unauthorized access or use, and encourages trust in the identity proofing process.

7.1.1. Social Security Numbers

These guidelines permit the CSP collection of the SSN as an attribute for use in identity resolution. However, over-reliance on the SSN can contribute to misuse and place the applicant at risk of harm, such as through identity theft. Nonetheless, the SSN may facilitate identity resolution for CSPs, in particular federal agencies that use the SSN to correlate an applicant to agency records. This document recognizes the role of the SSN as an attribute and makes appropriate allowance for its use. Knowledge of the SSN is not sufficient to serve as identity evidence.

Where possible, CSPs and agencies should consider mechanisms to limit the proliferation and exposure of SSNs during the identity proofing process. This is particularly pertinent where the SSN is communicated to third party providers during attribute validation processes. To the extent possible, privacy protective techniques and technologies should be applied to reduce the risk of an individual's SSN being exposed, stored, or maintained by third party systems. Examples of this could be the use of attribute claims (e.g., yes/no responses from a validator) to confirm the validity of a SSN without requiring it to be unnecessarily transmitted by the third party. As with all attributes in the identity proofing process, the value and risk of each attribute being processed is subject to a privacy risk assessment and federal agencies may address further in its associated PIA and SORN documentation. The SSN should only be collected where it is necessary to support identity resolution associated with the applications assurance and risk levels.

7.2. Notice and Consent

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

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

In addition, RPs should provide additional guidance to applicants for available choices for the selection of CSPs, identity document requirements, related privacy notices, and alternative means of accessing services.

7.3. Use Limitation

The guidelines require CSPs to use measures to maintain the objectives of predictability (enabling reliable assumptions by individuals, owners, and operators about PII and its processing by an information system) and manageability (providing the capability for the granular administration of PII, including alteration, deletion, and selective disclosure) commensurate with privacy risks that can arise from the processing of attributes for purposes other than identity proofing, authentication, authorization, or attribute assertion, related fraud mitigation, or to comply with law or legal process. A framework for managing these risks and supporting privacy risk management principles can be found in [NISTIR8062].

CSPs may have various business purposes for processing attributes, including providing non-identity services to subscribers. However, processing attributes for other purposes than those disclosed to a subject can create additional privacy risks. CSPs can determine appropriate measures commensurate with the privacy risk arising from the additional processing. For example, absent applicable law, regulation, or policy, it may not be necessary to obtain consent when processing attributes to provide non-identity services requested by subscribers, although notices may help the subscribers maintain reliable assumptions about the processing (predictability). Other processing of attributes may carry different privacy risks which may call for obtaining consent or allowing subscribers more control over the use or disclosure of specific attributes (manageability). Subscriber consent needs to be meaningful; therefore, when CSPs do use consent measures, they cannot make acceptance by the subscriber of additional uses a condition of providing the identity service.

Federal agencies should consult their SAOP if there are questions about whether the proposed processing falls outside the scope of the permitted processing or the appropriate privacy risk mitigation measures.

7.4. Redress

The guidelines require the CSP to provide effective mechanisms for redressing applicant complaints or problems arising from the identity proofing, and make the mechanisms easy for applicants to find and access.

The Privacy Act requires federal CSPs that maintain a system of records to follow procedures to enable applicants to access and, if incorrect, amend their records. Any Privacy Act Statement should include a reference to the applicable SORN(s) (see Sec. 3.1.3), which provide the applicant with instructions on how to make a request for access or correction. Non-federal CSPs should have comparable procedures, including contact information for any third parties if they are the source of the information.

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

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

7.5. Privacy Risk Assessment

The guidelines require the CSP to conduct a privacy risk assessment. In conducting a privacy risk assessment, CSPs should consider:

1. The likelihood that an 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 on the applicant should a problem occur. CSPs should be able to justify any response they take to identified privacy risks, including accepting the risk, mitigating the risk, and sharing the risk. Applicant consent is considered to be 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 this shared risk.

7.6. Agency-Specific Privacy Compliance

The guidelines cover specific compliance obligations for federal CSPs. It is critical to involve an agency's SAOP in the earliest stages of identity service development to assess and mitigate privacy risks and advise the agency on compliance requirements, such as whether or not the PII collection to conduct identity proofing triggers the Privacy Act of 1974 [PrivacyAct] or the E-Government Act of 2002 [E-Gov] requirement to conduct a Privacy Impact Assessment. For example, with respect to identity proofing, it is likely that the Privacy Act requirements will be triggered and require coverage by either a new or existing Privacy Act system of records notice (SORN) 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 identity lifecycle or includes the identity proofing process as part of a larger, programmatic PIA that discusses the program or benefit to which the agency is establishing online access.

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

8. Usability Considerations

This section is informative.

In order to align with the standard terminology of user-centered design and usability, the term "user" is used throughout this section to refer to the human party. In most cases, the user in question will be the subject (in the role of applicant, claimant, or subscriber) as described elsewhere in these guidelines.

This section is intended to raise implementers' awareness of the usability considerations associated with identity proofing and enrollment (for usability considerations for typical authenticator usage and intermittent events, see Sec. 8 of [SP800-63B].

[ISO/IEC9241-11] defines usability as the "extent to which a system, product, or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use." This definition focuses on users, goals, and context of use as the necessary elements for achieving effectiveness, efficiency, and satisfaction. A holistic approach considering these key elements is necessary to achieve usability.

The overarching goal of usability for identity proofing and enrollment 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 the amount of information to track). To achieve this goal, organizations have to first familiarize themselves with their users.

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

Usability cannot be achieved in a piecemeal manner. Performing a usability evaluation on the enrollment and identity proofing process is critical. It is important to conduct a usability evaluation with representative users, realistic goals and tasks, and appropriate contexts of use. The enrollment and identity proofing process should be designed and implemented so that it is easy for users to do the right thing, hard for them to do the wrong thing, and easy for them to recover when the wrong thing happens. [ISO/IEC9241-11], [ISO16982], and [ISO25060] provide guidance on how to evaluate the overall usability of an identity service and additional considerations for increasing usability.

From the user's perspective, the three main steps of identity proofing and enrollment 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.

Guidelines and considerations are described from the users' perspective.

Section 508 of the Rehabilitation Act of 1973 [Section508] was enacted to eliminate barriers in information technology and require federal agencies to make electronic and information technology accessible to people with disabilities. While these guidelines do not directly assert requirements from Section 508, identity service providers are expected to comply with Section 508 provisions. Beyond compliance with Section 508, Federal Agencies and their service providers are generally expected to design services and systems with the experiences of people with disabilities in mind to ensure that accessibility is prioritized throughout identity system lifecycles.

8.1. General User Considerations During Identity Proofing and Enrollment

This sub-section provides usability considerations that are applicable across all steps of the enrollment process. Usability considerations specific to each step are detailed in Sec. 8.2, Sec. 8.3, and Sec. 8.4.

- To avoid user frustration, streamline the process required for enrollment to make each step as clear and easy as possible.
- Clearly communicate how and where to acquire technical assistance. For example, provide helpful information such as a link to an online self-service portal, chat sessions, and a phone number for help desk support. Ideally, sufficient information should be provided to enable users to answer their own enrollment preparation questions without outside intervention.
- Clearly explain what personal data is being collected and whether collecting the data is optional or not. Additionally, provide information indicating with whom the data will be shared, where it will be stored, and how it will be protected.
- Ensure that all information presented is usable.
  - Follow good information design practice for all user-facing materials (e.g., data collection notices and fillable forms).
  - Write materials in plain language and avoid technical jargon. If appropriate, tailor that language to the literacy level of the intended population. 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 the 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 confirmation codes. Use a minimum font size of 12 points, as long as the text fits the display.

- Perform a usability evaluation for each step with representative users. Establish realistic goals and tasks, and appropriate contexts of use for the usability evaluation.

8.2. Pre-Enrollment Preparation

This section describes an effective approach to facilitate sufficient pre-enrollment preparation so users can avoid challenging, frustrating enrollment sessions. Ensuring that users are as prepared as possible for their enrollment sessions is critical to the overall success and usability of the identity proofing and enrollment process.

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

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

- Information about the entire process, such as what to expect in each step.
  - Clear explanations of the expected timeframes to allow users to plan accordingly.
- Explanation of the need for — and benefits of — identity proofing to allow users to understand the value proposition.
- Identity evidence requirements for the intended IAL and a list of acceptable evidence documents, with information about how they will be validated.
- If there is an enrollment fee and, if so, the amount and acceptable forms of payment. Offering a variety of acceptable forms of payment allows users to choose their preferred payment operation.
- Information on whether the user’s enrollment session will be in-person or in-person over remote channels, and whether a user can choose. Only provide information relevant to the allowable session option(s).

  - Information on the location(s), whether a user can choose their preferred location, and necessary logistical information for in-person or in-person over remote channels session. Note that users may be reluctant to bring identity evidence to certain public places (a supermarket versus a bank), as it increases exposure to loss or theft.
  - Information on the technical requirements (e.g., requirements for internet access) for remote sessions.
  - An option to set an appointment for in-person or in-person over remote channels identity proofing sessions to minimize wait times. If walk-ins are allowed, make it clear to users that their wait times may be greater without an appointment.
    * Provide clear instructions for setting up an enrollment session appointment, reminders, and how to reschedule existing appointments.
    * Offer appointment reminders and allow users to specify their preferred appointment reminder method(s) (e.g., postal mail, voicemail, email, text message). Users need information such as the date, time, and location, and a description of the required identity evidence.
- Information on the allowed and required identity evidence and attributes, whether each piece is voluntary or mandatory, and the consequences for not providing the complete set of identity evidence. Users need to know the specific combinations of identity evidence, including requirements specific to a piece of identity evidence (e.g., a raised seal on a birth certificate). This is especially important due to potential difficulties procuring the necessary identity evidence.
  - Where possible, implement tools to make it easier to obtain the necessary identity evidence.
  - Inform users of any special requirements for minors or people with unique needs. For example, provide users with the information on whether applicant reference and/or trusted referee processes are available and the information necessary to use those processes (see Sec. 3.1.13).
  - If forms are required:
    * Provide fillable forms before and at the enrollment session. Do not require users to have access to a printer.
    * Minimize the amount of information that users must enter on a form, as users are easily frustrated and more error-prone with longer forms. Where possible, pre-populate forms.

8.3. Identity Proofing and Enrollment

Usability considerations specific to identity proofing and enrollment include:

- At the start of the identity proofing session, remind users of the procedure. Do not expect them to remember the procedures described during 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.
- Depending on the identity proofing method (e.g., Remote or Onsite Unattended), provide a separate video window that provides a step-by-step tutorial of the identity proofing process. When these types of tutorials or examples are provided, service providers should provide a range of support options to cover a broad set of users. Alternatives to a video window include verbal or written instructions.
- Provide options for the user to reschedule the time or type of their identity proofing appointment, if needed.
- Provide a checklist with the allowed and required identity evidence to ensure that 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 or use exception processing through a trusted referee or, as appropriate, applicant references for identity proofing exception processing. This also would apply to international users where the types of identity evidence and access to data, services, and validation sources may not be easily or readily available to achieve IAL identity proofing requirements. Trusted referees and applicant references are intended to provide capabilities for alternative identity proofing workflows and risk-based decisions for such types of users needing exception processing.
- 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 if 1) users will receive an authenticator immediately at the end of a successful enrollment session; 2) if they will have to schedule a follow-up appointment to pick up an authenticator in person; or 3) or if users will receive the authenticator in the mail and, if so, 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 collected and processed by the CSP. (See Sec. 3.1 and Sec. 7 for detailed requirements on notices). CSPs should be aware that seeking consent from users for the use of their attributes for purposes other than identity proofing, authentication, authorization, or attribute assertions, may make them uncomfortable. If users do not perceive how they benefit by the additional collection or uses, they may be unwilling or hesitant to provide consent or continue the process. It is recommended, then, that CSPs provide users with a thorough explanation of how they might benefit from the additional processing of their personal information, and steps the CSP takes to mitigate the risks associated with such processing. Additionally, CSPs should provide users with the ability to opt out of the additional processing.

- If a confirmation code is issued:
  - Notify users in advance that they will receive a confirmation 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, or email).
  - When a confirmation code is delivered to a user, remind the users which service they are enrolling in and 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 Sec. 3.1.8.
  - If issuing a machine-readable optical label, such as a QR Code (see Sec. 3.1.8), provide users with information on how to obtain QR code scanning capabilities (e.g., acceptable QR code applications).
  - Inform users that they will be required to repeat the enrollment process if enrollment codes expire or are lost before use.
  - Provide users with alternative options, as not all users are able to access and use technology equitably. For example, users may not have the technology needed for this approach to be feasible.
- At the end of the enrollment session:
  - If enrollment is successful, send subscribers a notification of proofing confirming successful identity proofing and enrollment (see Sec. 3.1.8) and directions on next steps they need to take (e.g., when and where to pick up their authenticator, when it will arrive in the mail).
  - If enrollment is partially complete (due to users not having the complete set of identity evidence, users choosing to stop the process, or session timeouts), communicate to users:
    * what information will be destroyed;
    * what, if any, information will be retained for future follow-up sessions;

2380 * how long the information will be retained; and
2381 * what identity evidence they will need to bring to a future session.
2382 - If enrollment is not successful, provide users with clear instructions for
2383 alternative identity proofing and enrollment options, for example, in-person
2384 proofing for users who cannot complete remote proofing.

2385 • If users receive the authenticator during the enrollment session, provide users
2386 with instructions on the use and maintenance of the authenticator. For example,
2387 information could include instructions for use (especially if there are different
2388 requirements for first-time use or initialization), information on authenticator
2389 expiration, how to protect the authenticator, and what to do if the authenticator
2390 is lost or stolen.

2391 • For both in-person and remote identity proofing, additional usability
2392 considerations apply:

2393 - At the start of the enrollment session, operators or attendants need to
2394 explain their role to users (e.g., whether operators or attendants will walk
2395 users through the enrollment session or observe silently and only interact as
2396 needed).

2397 - At the start of the enrollment session, inform users that they must not depart
2398 during the session, and that their actions must be visible throughout the
2399 session.

2400 - When biometrics are collected during the enrollment session, provide users
2401 with clear instructions on how to complete the collection process. The
2402 instructions are best given just prior to the process. Verbal instructions with
2403 guidance from a live operator are the most effective (e.g., instructing users
2404 where the biometric sensor is, when to start, how to interact with the sensor,
2405 and when the biometric collection is completed).

2406 • Since remote identity proofing is conducted online, follow general web usability
2407 principles. For example:

2408 - Design the user interface to walk users through the enrollment process.
2409 - Reduce users' memory load.
2410 - Make the interface consistent.
2411 - Clearly label sequential steps.
2412 - Make the starting point clear.
2413 - Design to support multiple platforms and device sizes.
2414 - Make the navigation consistent, easy to find, and easy to follow.

8.4. Post-Enrollment

Post-enrollment refers to the step immediately following enrollment but prior to the first use of an authenticator (for usability considerations for typical authenticator usage and intermittent events, see [SP800-63B], Sec. 10. 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.
- Provide information to users about how to protect themselves from common threats to their identity accounts and associated authenticators, such as social engineering and phishing attacks.

9. Equity Considerations

This section is informative.

This section is intended to provide guidance to CSPs and RPs for assessing the risks associated with inequitable access, treatment, or outcomes for individuals using its identity services, as required in Sec. 3.1.4. It provides a non-exhaustive list of potential areas in the identity proofing process that may be subject to inequities, as well as possible mitigations that can be applied. CSPs and RPs can use this section as a starting point for considering where the risks for inequitable access, treatment, or outcomes exist within its identity service. It is not intended that the below guidance be considered a definitive, all-inclusive list of associated equity risks to identity services.

In assessing equity risks, CSPs and RPs start by considering the overall user population served by its online service. Additionally, CSPs and RPs further identify groups of users within the population whose shared characteristic(s) can cause them to be subject to inequitable access, treatment, or outcomes when using that service. CSPs and RPs are encouraged to assess the effectiveness of any mitigations by evaluating their impacts on the affected user group(s). The usability considerations provided in Sec. 8 should also be considered when applying equity risk mitigations to help improve the overall usability and equity for all persons using an identity service.

Pursuant to Executive Order 13985 [EO13985], *Advancing Racial Equity and Support for Underserved Communities Through the Federal Government*, OMB published its *Study to Identify Methods to Assess Equity: Report to the President* [OMB-Equity] which identified "the best methods, consistent with applicable law, to assist agencies in assessing equity with respect to race, ethnicity, religion, income, geography, gender identity, sexual orientation, and disability." CSPs and RPs are encouraged to consult this study when determining which approaches and methods they will use to assess the equity of their identity services.

It is intended that remote identity proofing can broaden usability and accessibility for enrollment into online identity services. The following subsections present considerations for some identity proofing processes that may create risks of inequitable treatment for some groups and individuals and present the use of trusted referees to help to mitigate such risks associated with remote identity proofing. However, it is important that the use of trusted referees do not create additional risks of exclusion among groups who may lack internet access or who do not have easy access to smartphones or computing devices. Providing in-person options for trusted referees can help ensure that those impacted by the digital divide are still able to access services offered by the CSP or RP.

Additionally, CSPs and RPs should assess whether implementing these considerations could introduce delays to the identity proofing process and employ appropriate

methods, such as online scheduling tools or additional staffing for peak demand times, to mitigate these delays.

It is also intended that the considerations and mitigations provided in this section will be proactively employed and result in a more equitable identity proofing experience for the population served by the identity service. CSPs are expected to continuously monitor the performance of their service and to make remedial updates, as appropriate. This includes policies and processes for redressing user reports of inequitable access, treatment, or outcomes of the service.

9.1. Identity Resolution and Equity

Identity resolution involves collecting the minimum set of attributes to be able to distinguish the claimed identity as a single, unique individual within the population served by the identity service. Attributes are obtained from the presented identity evidence, applicant self-assertion, and/or back-end attribute providers.

This section provides a set of possible problems and mitigations with the inequitable access, treatment, or outcomes associated with the identity resolution process:

Description: The identity service design requires an applicant to enter their name using a Western name format (e.g., first name, last name, optional middle name).

Possible mitigations include:

1. Analyzing possible name configurations and determining how all names can be accurately accommodated using the name fields
2. Providing easy-to-find and use guidance to users on how to enter all names using the name fields
3. Accepting reasonable name variations (for example, to allow for differences in name order, multiple surnames, etc.)
4. Providing the option for applicants to switch to an attended (onsite or remote) workflow option

Description: The identity service cannot accommodate applicants whose name, gender, or other attributes have changed and are not consistently reflected on the presented identity evidence or match what is in the attribute verifier's records.

Possible mitigations include:

1. Providing trusted referees (Sec. 3.1.13.1) who can make risk-based decisions based on the specific applicant circumstances
2. Allowing for the use of applicant references (Sec. 3.1.13.3) who can vouch for the differences in attributes

3. Providing an easily accessible list of acceptable evidence in support of the updated attribute, such as a marriage certificate
4. Accepting reasonable name variations (for example, to allow for differences in name order, multiple surnames, hyphenation, or recent name changes)

9.2. Identity Validation and Equity

Identity evidence and core attribute validation involves confirming the genuineness, currency, and accuracy of the presented identity evidence and the accuracy of any additional attributes. These outcomes are accomplished by comparison of the evidence and attributes against data held by authoritative or credible sources. When considered together with the identity resolution phase, the result of successful validation phase is the confirmation, to some level of confidence, that the claimed identity exists in the real world.

This section provides a set of possible problems and mitigations with the inequitable access, treatment, or outcomes associated with the evidence and attribute validation process:

Description: Certain user groups do not possess the necessary minimum evidence to meet the requirements of a given IAL.

Possible mitigations include:

1. Providing trusted referees (Sec. 3.1.13.1) who can make risk-based decisions based on the specific applicant circumstances
2. Allowing for the use of applicant references (Sec. 3.1.13.3), such as the parent of a minor child, who can vouch for the applicant
3. Ensuring that the selected IAL is not higher than necessary to be commensurate with the risk of the digital service offering
4. RPs offering a limited set of functionality or options for users identity proofed at lower IALs

Description: Records held by authoritative and credible sources are insufficient to support the validation of core attributes or presented evidence for applicants belonging to certain user groups, such as those who self-exclude themselves from programs and services due to fears of surveillance or other concerns that might result in a record of their association.

Possible mitigations include:

1. Providing trusted referees (Sec. 3.1.13.1) who can make risk-based decisions based on the specific applicant circumstances

2. Allowing the use of applicant references (Sec. 3.1.13.3) who can vouch for the difference in attributes
3. Employing multiple authoritative or credible sources

Description: Records held by authoritative and credible sources may include inaccurate or false information about persons who are the victims of identity fraud.

Possible mitigations include:

1. Providing trusted referees (Sec. 3.1.13.1) who can make risk-based decisions based on the specific applicant circumstances
2. Allowing the use of applicant references (Sec. 3.1.13.3) who can vouch for the difference in attributes
3. Employing multiple authoritative or credible sources

9.3. Identity Verification and Equity

Identity verification involves proving the binding between the applicant undergoing the identity proofing process and the validated, real-world identity established through the identity resolution and validation steps. It most often involves collecting a picture (facial image capture) of the applicant taken during the identity proofing event and comparing it to a photograph contained on a presented and validated piece of identity evidence.

This section provides a set of possible problems and mitigations with the inequitable treatment or outcomes associated with the identity verification phase:

Description: Facial image capture technologies lack the ability to capture certain skin tones or facial features of sufficient quality to perform a comparison.

Possible mitigations include:

1. Employing robust image capture technologies, with high performing algorithms, which have been demonstrated to accommodate different skin tones, facial features, and lighting situations
2. Conducting operational testing of image capture technologies to determine if they function equitably across ethnicity, race, sex assigned at birth, and other demographic factors and upgrading, as needed, to correct for inequities
3. Providing guidance to the applicant about how to improve the lighting or conditions for image capture
4. Providing risk-based alternative processes, such as Trusted Referees (Sec. 3.1.13.1), that compensate for residual bias and technological limitations
5. Providing the option for applicants to use CSP-controlled kiosks, which employ state-of-the-art facial and biometric capture technologies

6. Providing the option for applicants to switch to an attended workflow option

Description: For biometric comparison involving facial images, facial coverings worn for religious purposes may impede the ability to capture a facial image of an applicant. For biometric comparison involving other biometric characteristics, demographic factors may impede the ability to capture a usable biometric sample, such as age affecting the capability to collect a usable fingerprint.

Possible mitigations include:

1. Providing trusted referees (Sec. 3.1.13.1) who can make risk-based decisions based on the specific applicant circumstances.
2. Providing alternative ways to accomplish identity verification, such as an in-person proofing.
3. Offering alternative biometric collection and comparison capabilities.

Description: When using 1:1 facial image comparison technologies, biased facial comparison algorithms may result in false non-matches.

Possible mitigations include:

1. Using algorithms that are independently tested for consistent performance across demographic groups and image types
2. Supporting alternative processes to compensate for residual bias and technological limitations
3. Conducting ongoing quality monitoring and operational testing to identify performance variances across demographic groups and implementing corrective actions as needed (e.g., updated algorithms, machine learning, etc.)

Description: When employing visual facial image comparison performed by agents of the CSP (proofing agents or trusted referees), human biases and inconsistencies in making facial comparisons may result in false non-matches.

Possible mitigations include:

1. Defining policy and procedures aimed at reducing/eliminating the inequitable treatment of applicants by CSP agents
2. Rigorously training and certifying CSP agents
3. Conducting ongoing quality monitoring and taking corrective actions when biases, inequitable treatments, or outcomes are identified

9.4. User Experience and Equity

The Usability Considerations section of this document (Sec. 8) provides CSPs with guidance on how to provide applicants with a smooth, positive identity proofing experience. In addition to the specific considerations provided in Sec. 8, this section provides CSPs with additional considerations when considering the equity of their user experience.

Description: Lack of access to the needed technology (e.g. connected mobile device or computer), or difficulties in using the required technologies, unduly burdens some user groups.

Possible mitigations include:

1. Allowing the use of process assistants who assist applicants, who are otherwise able to meet the identity proofing requirements, in the use of the required technologies and activities
2. Allowing the use of publicly-available devices (e.g., computers or tablets) and providing online help resources for completing the identity proofing process on a non-applicant-owned computer or device
3. Providing in-person proofing options
4. Employing technologies, such as auto capture, that simplify the uploading of identity evidence and facial images

Description: The remote or in-person identity proofing process presents challenges for persons with disabilities.

Possible mitigations for remote identity proofing include:

1. Providing trusted referees (Sec. 3.1.13.1) who are trained to communicate and assist people with a variety of needs or disabilities (e.g., fluent in sign language)
2. Allowing for the use of applicant references (Sec. 3.1.13.3)
3. Supporting the use of accessibility and other technologies, such as audible instructions, screen readers and voice recognition technologies
4. Allowing the use of process assistants to assist applicants, who are otherwise able to meet the identity proofing requirements, in the use of the required technologies and activities

Possible mitigations for in-person identity proofing include:

1. Providing trained operators who are trained to communicate and assist people with a variety of needs or disabilities (e.g., fluent in sign language)
2. Choosing equipment and workstations that can be adjusted to different heights and angles
3. Selecting locations that are convenient and comply with ADA accessibility guidelines

References

This section is informative.

[A-130] Office of Management and Budget (2016) Managing Information as a Strategic Resource. (The White House, Washington, DC), OMB Circular A-130, July 28, 2016. Available at https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

[COPPA] Children's Online Privacy Protection Act of 1998, Pub. L. 105-277 Title XIII, 112 Stat. 2681-728. Available at https://www.govinfo.gov/app/details/PLAW-105publ277

[EO13985] Biden J (2021) Advancing Racial Equity and Support for Underserved Communities Through the Federal Government. (The White House, Washington, DC), Executive Order 13985, January 25, 2021. https://www.federalregister.gov/documents/2021/01/25/2021-01753/advancing-racial-equity-and-support-for-underserved-communities-through-the-federal-government

[EO13988] Biden J (2021) Preventing and Combating Discrimination on the Basis of Gender Identity or Sexual Orientation. (The White House, Washington, DC), Executive Order 13988, January 20, 2021. https://www.federalregister.gov/documents/2021/01/25/2021-01761/preventing-and-combating-discrimination-on-the-basis-of-gender-identity-or-sexual-orientation

[EO13985-vision] Office of Management and Budget (2022) A Vision for Equitable Data: Recommendations from the Equitable Data Working Group. (The White House, Washington, DC), OMB Report Pursuant to Executive Order 13985, April 22, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/04/eo13985-vision-for-equitable-data.pdf

[E-Gov] E-Government Act of 2002, Pub. L. 107-347, 116 Stat. 2899. https://www.govinfo.gov/app/details/PLAW-107publ347

[ISO/IEC9241-11] International Standards Organization (2018) *ISO/IEC 9241-11 Ergonomics of human-system interaction – Part 11: Usability: Definitions and concepts* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/63500.html

[ISO16982] International Standards Organization (2002) *ISO/TR 16982:2002 Ergonomics of human-system interaction Usability methods supporting human-centred design* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/31176.html

[ISO25060] International Standards Organization (2023) *ISO/TR 25060:2023 Systems and software engineering Systems and software Quality Requirements and Evaluation (SQuaRE) General framework for Common Industry Format (CIF) for usability-related information* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/83763.html

[NISTIR8062] Brooks SW, Garcia ME, Lefkovitz NB, Lightman S, Nadeau EM (2017) An Introduction to Privacy Engineering and Risk Management in Federal Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8062. https://doi.org/10.6028/NIST.IR.8062

[NIST-Privacy] National Institute of Standards and Technology (2020) NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) 10. https://doi.org/10.6028/NIST.CSWP.10

[NIST-RMF] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[OMB-Equity] Office of Management and Budget (July 20th, 2021). Study to Identify Methods to Assess Equity: Report to the President. https://www.whitehouse.gov/wp-content/uploads/2021/08/OMB-Report-on-E013985-Implementation_508-Compliant-Secure-v1.1.pdf

[PrivacyAct] Privacy Act of 1974, Pub. L. 93-579, 5 U.S.C. § 552a, 88 Stat. 1896 (1974). https://www.govinfo.gov/content/pkg/USCODE-2020-title5/pdf/USCODE-2020-title5-partI-chap5-subchapII-sec552a.pdf

[Section508] General Services Administration (2022) *IT Accessibility Laws and Policies*. Available at https://www.section508.gov/manage/laws-and-policies/

[RFC5280] Cooper D, Santesson S, Farrell S, Boeyen S, Housley R, Polk W (2008) Internet X.509 Public Key Infrastructure Certification and Certificate Revocation List (CRL) Profile. (Internet Engineering Task Force (IETF)), IETF Request for Comments (RFC) 5280. https://doi.org/10.17487/RFC5280

[SP800-53] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53 Rev. 5, Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[SP800-63] Temoshok D, Proud-Madruga D, Choong YY, Galluzzo R, Gupta S, LaSalle C, Lefkovitz N, Regenscheid A (2024) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-4 2pd. https://doi.org/10.6028/NIST.SP.800-63-4.2pd

[SP800-63B] Temoshok D, Fenton JL, Choong YY, Lefkovitz N, Regenscheid A, Galluzzo R, Richer JP (2024) Digital Identity Guidelines: Authentication and Authenticator Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63B-4 ipd. https://doi.org/10.6028/NIST.SP.800-63b-4.2pd

[SP800-63C] Temoshok D, Richer JP, Choong YY, Fenton JL, Lefkovitz N, Regenscheid A, Galluzzo R (2024) Digital Identity Guidelines: Federation and Assertions. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63C-4 2pd. https://doi.org/10.6028/NIST.SP.800-63c-4.2pd

[SP800-161] Boyen H, Smith A, Bartol N, Winkler K, Holbrook A (2022) Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD) NIST Special Publication (SP) 800-161r1. https://doi.org/10.6028/NIST.SP.800-161r1

Appendix A. Identity Evidence Examples by Strength

This appendix is informative.

This appendix provides a non-exhaustive list of types of identity evidence, grouped by strength.

A.1. Fair Evidence Examples

Table 4. Fair Evidence Examples

Evidence	Proofing	Validation	Verification
Financial Account	KYC/CIP requirements	Confirm signature on assertion is from intended origin.	*Demonstrated possession via an AAL2 authentication event and FAL 2 federated assertion. *User input of a micro deposit event of sufficient entropy.
Phone Account	Established and documented account opening practices.	*Confirm presence of user account with MNO. *Confirm signature on assertion is from intended origin.	*Demonstrated possession through enrollment code. *Demonstrated possession via and AAL2 authentication event and FAL2 federated assertion.
Student ID Card	Student registration and enrollment practices.	*Confirm signature on assertion is from intended origin; or *Confirm physical security features and evaluate for tampering.	*Demonstrated possession via and AAL2 authentication event and FAL2 federated assertion. *Physical comparison to image on the ID. *Biometric Comparison to image on the ID.

Corporate ID Card	Onboarding and background screening practices.	*Confirm signature on assertion is from intended origin; or *Confirm physical security features and evaluate for tampering.	*Demonstrated possession via and AAL2 authentication event and FAL2 federated assertion. *Physical comparison to image on the ID. *Biometric Comparison to image on the ID.
Veteran Health ID card	VA identity verification, issuance and eligibility process	*Confirm signature on assertion is from intended origin; or *Confirm physical security features and evaluate for tampering	*Demonstrated possession via and AAL2 authentication event and FAL2 federated assertion. *Physical comparison to image on the ID. *Biometric Comparison to image on the ID.
Credit or Debit Card	KYC/CIP Account Opening Practices.	*Confirm physical security features, physical signature.	*Demonstrated ability to authenticate to the card using a PIN or other activation factor (if available). *Physical inspection of the card. Must be presented with other evidence containing a photo.
Snap Card	State defined eligibility and enrollment requirements.	Confirm physical security features, physical signature	*Visual inspection of the card. Must be presented with other evidence containing a photo (if there is no image on the card).
Social Security Card	SSN application process.	*Confirm physical security features, inspect for tampering.	*Visual inspection of the card. Must be presented with other evidence containing a photo.

A.2. Strong Evidence Examples

Table 5. Strong Evidence Examples

Evidence	Proofing	Validation	Verification
Driver's License or State ID	State issuance processes, REAL ID Act	Confirm physical security features through inspection.	*Physical comparison of image on ID. *Biometric Comparison of the image on the ID. *Biometric comparison to issuing source records.
Permanent Resident Card (issued prior to May 11, 2010)	DHS issuance and eligibility process	*Confirm physical security features through inspection.	*Physical comparison of image on ID. *Biometric Comparison of the image on the ID. *Biometric comparison to issuing source records.
U.S. Uniformed Services Privilege and Identification Card	DoD issuance and eligibility processes	*Confirm physical security features through inspection.	*Visual comparison of image on ID. *Biometric Comparison of the image on the ID. *Biometric comparison to issuing source records.
Native American Tribal Photo Identification Card	Local issuance and eligibility processes	*Confirm physical security features through inspection.	*Visual comparison of image on ID. *Biometric Comparison of the image on the ID. *Biometric comparison to issuing source records.
Veteran Health ID Card (VHIC)	VA identity verification, issuance and eligibility process	*Confirm physical security features and evaluate for tampering	*Visual comparison to image on the ID. *Biometric Comparison to image on the ID.

A.3. Superior Evidence Examples

Table 6. Superior Evidence Examples

Evidence	Proofing	Validation	Verification
Personal Identity Verification (PIV) Card	FIPS 201-3 identity verification and issuance processes	Validation of stored PKI Certificate, CRL check if available	*Authentication consistent with multi-factor cryptographic authenticators per NIST SP 800-63B. *Biometric comparison to image stored on ID or biometric stored on ID. *Visual comparison of image on ID.
Personal Identity Verification-Interoperable (PIV-I) Card	FIPS 201-3 identity verification and issuance processes	Validation of stored PKI Certificate, CRL check if available	*Authentication consistent with multi-factor cryptographic authenticators per NIST SP 800-63B. *Biometric comparison to image stored on ID or biometric stored on ID. *Visual comparison of image on ID.
Common Access Card (CAC)	DoD identity verification and issuance process	Validation of stored PKI Certificate, CRL check if available	*Authentication consistent with multi-factor cryptographic authenticators per NIST SP 800-63B. *Biometric comparison to image stored on ID or biometric stored on ID. *Visual comparison of image on ID.
US Passport	State Department passport issuance process	Validation of stored PKI certificate, CRL check if available.	*Visual comparison of image on ID on stored in ID. *Biometric comparison to image on ID or stored in ID. *Biometric comparison to issuing source records.

International e-Passports Passports	ICAO compliant and/or State Department approved	Validation of stored PKI certificate, CRL check if available.	*Visual comparison of image on ID on stored in ID. *Biometric comparison to image on ID or stored in ID. *Biometric comparison to issuing source records.
Mobile Driver's License (MDL)	State Issuance processes, AAMVA guidance, and Real ID Act	Validation of Mobile Security Object, revocation check if available	*Authentication consistent with multi-factor cryptographic authenticators per NIST SP 800-63B.
Digital Permanent Resident Card (Verifiable Credential)	DHS issuance and eligibility process	Validation of stored verifiable credential, revocation check if available	*Authentication consistent with multi-factor cryptographic authenticators per NIST SP 800-63B.
European Digital Identity Wallet (EUDI Wallet) Personal Identification (PID) Element	EC defined identity verification and issuance process; qualified issuer certified	Validation of stored verifiable credential or Mobile Security Object, revocation check if available	*Authentication consistent with multi-factor cryptographic authenticators per NIST SP 800-63B.

Appendix B. List of Symbols, Abbreviations, and Acronyms

1:1 Comparison
One-to-One Comparison

AAL
Authentication Assurance Level

CSP
Credential Service Provider

DNS
Domain Name System

FACT Act
Fair and Accurate Credit Transaction Act of 2003

FAL
Federation Assurance Level

FEDRAMP
Federal Risk and Authorization Management Program

FMR
False Match Rate

FNMR
False Non-Match Rate

IAL
Identity Assurance Level

IdP
Identity Provider

KBA
Knowledge-Based Authentication

KBV
Knowledge-Based Verification

MFA
Multi-Factor Authentication

NARA
National Archives and Records Administration

PAD
Presentation Attack Detection

PIA
Privacy Impact Assessment

PII
Personally Identifiable Information

PKI
Public Key Infrastructure

RMF
Risk Management Framework

RP
Relying Party

SMS
Short Message Service

SORN
System of Records Notice

Appendix C. Glossary

This section is informative.

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

applicant
A *subject* undergoing the processes of *identity proofing* and *enrollment*.

applicant reference
A representative of the *applicant* who can vouch for the identity of the applicant, specific *attributes* related to the applicant, or conditions relative to the context of the individual (e.g., emergency status, homelessness).

approved cryptography
An encryption algorithm, *hash function*, random bit generator, or similar technique that is *Federal Information Processing Standard* (FIPS)-approved or NIST-recommended. Approved algorithms and techniques are either specified or adopted in a FIPS or NIST recommendation.

assertion
A statement from an *IdP* to an *RP* that contains information about an authentication event for a subscriber. Assertions can also contain identity *attributes* for the subscriber.

attribute
A quality or characteristic ascribed to someone or something. An identity attribute is an attribute about the identity of a subscriber.

attribute validation
The process or act of confirming that a set of attributes are accurate and associated with a real-life identity. See *validation*.

authenticate
See *authentication*.

authentication
The process by which a *claimant* proves possession and control of one or more *authenticators* bound to a *subscriber account* to demonstrate that they are the subscriber associated with that account.

Authentication Assurance Level (AAL)
A category that describes the strength of the authentication process.

authenticator
Something that the subscriber possesses and controls (e.g., a *cryptographic module* or *password*) and that is used to *authenticate* a *claimant's* identity. See *authenticator type* and *multi-factor authenticator*.

authenticity
The property that data originated from its purported source.

authoritative source
An entity that has access to or verified copies of accurate information from an *issuing source* such that a *CSP* has high confidence that the source can confirm the validity of the identity attributes or 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 identity proofing *validation* phase.

authorize
A decision to grant access, typically automated by evaluating a *subject*'s *attributes*.

biometric reference
One or more stored *biometric samples*, templates, or models attributed to an individual and used as the object of biometric comparison in a database, such as a facial image stored digitally on a passport, fingerprint minutiae template on a National ID card or Gaussian Mixture Model for speaker recognition.

biometric sample
An analog or digital representation of biometric characteristics prior to biometric feature extraction, such as a record that contains a fingerprint image.

biometrics
Automated recognition of individuals based on their biological or behavioral characteristics. Biological characteristics include but are not limited to fingerprints, palm prints, facial features, iris and retina patterns, voiceprints, and vein patterns. Behavioral characteristics include but are not limited to keystrokes, angle of holding a smart phone, screen pressure, typing speed, mouse or mobile phone movements, and gyroscope position.

claimant
A *subject* whose identity is to be verified using one or more *authentication protocols*.

claimed address
The physical location asserted by a *subject* where they can be reached. It includes the individual's residential street address and may also include their mailing address.

claimed identity
An *applicant's* declaration of unvalidated and unverified personal *attributes*.

core attributes
The set of identity *attributes* that the *CSP* has determined and documented to be required for *identity proofing*.

credential service provider (CSP)
A trusted entity whose functions include *identity proofing applicants* to the identity service and registering *authenticators* to *subscriber accounts*. A CSP may be an independent third party.

credible source
An entity that can provide or validate the accuracy of *identity evidence* and *attribute* information. A credible source has access to attribute information that was validated through an *identity proofing* process or that can be traced to an *authoritative source*, or it maintains identity attribute information obtained from multiple sources that is checked for data correlation for accuracy, consistency, and currency.

digital identity
An *attribute* or set of attributes that uniquely describes a *subject* within a given context.

digital signature
An *asymmetric key* operation in which 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* support but not confidentiality or *replay attack* protection.

disassociability
Enabling the *processing* of PII or events without association to individuals or devices beyond the operational requirements of the system. [NISTIR8062]

electronic authentication (e-authentication)
See *digital authentication*.

enrollment
The process through which a *CSP*/*IdP* provides a successfully identity-proofed *applicant* with a *subscriber account* and binds *authenticators* to grant persistent access.

entropy
The amount of uncertainty that an attacker faces to determine the value of a secret. Entropy is usually stated in bits. A value with *n* bits of entropy has the same degree of uncertainty as a uniformly distributed *n*-bit random value.

equity
The consistent and systematic fair, just, and impartial treatment of all individuals, including individuals who belong to underserved communities that have been denied such treatment, such as Black, Latino, and Indigenous and Native American persons, Asian Americans and Pacific Islanders, and other persons of color; members of religious minorities; lesbian, gay, bisexual, transgender, and queer (LGBTQ+) persons; persons with disabilities; persons who live in rural areas; and persons otherwise adversely affected by persistent poverty or inequality. [EO13985]

Federal Information Processing Standard (FIPS)
Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves the standards and guidelines that the National Institute of Standards and Technology (NIST) develops for federal computer systems. NIST issues these standards and guidelines as Federal Information Processing Standards (FIPS) for government-wide use. NIST develops FIPS when there are compelling federal government requirements, such as for security and interoperability, and there are no acceptable industry standards or solutions. See background information for more details.

FIPS documents are available online on the FIPS home page: https://www.nist.gov/itl/fips.cfm

federation
A process that allows for the conveyance of identity and authentication information across a set of *networked* systems.

Federation Assurance Level (FAL)
A category that describes the process used in a *federation transaction* to communicate authentication events and subscriber *attributes* to an *RP*.

hash function
A function that maps a bit string of arbitrary length to a fixed-length bit string. Approved hash functions satisfy the following properties:

1. One-way — It is computationally infeasible to find any input that maps to any pre-specified output.
2. Collision-resistant — It is computationally infeasible to find any two distinct inputs that map to the same output.

identifier
A data object that is associated with a single, unique entity (e.g., individual, device, or session) within a given context and is never assigned to any other entity within that context.

identity
See *digital identity*

Identity Assurance Level (IAL)
A category that conveys the degree of confidence that the *subject*'s *claimed identity* is their real identity.

identity evidence
Information or documentation that supports the real-world existence of the *claimed identity*. Identity evidence may be physical (e.g., a driver's license) or digital (e.g., a mobile driver's license or digital *assertion*). Evidence must support both *validation* (i.e., confirming *authenticity* and accuracy) and *verification* (i.e., confirming that the *applicant* is the true owner of the evidence).

identity proofing
The processes used to collect, validate, and verify information about a *subject* in order to establish assurance in the subject's *claimed identity*.

identity provider (IdP)
The party in a *federation transaction* that creates an *assertion* for the subscriber and transmits the assertion to the *RP*.

identity resolution
The process of collecting information about an *applicant* to uniquely distinguish an individual within the context of the population that the *CSP* serves.

identity verification
See *verification*

injection attack
An attack in which an attacker supplies untrusted input to a program. In the context of federation, the attacker presents an untrusted *assertion* or *assertion reference* to the *RP* in order to create an *authenticated session* with the RP.

issuing source
An authority responsible for the generation of data, digital evidence (i.e., *assertions*), or physical documents that can be used as *identity evidence*.

knowledge-based verification (KBV)
A process of validating knowledge of personal or private information associated with an individual for the purpose of verifying the *claimed identity* of an *applicant*. KBV does not include collecting personal *attributes* for the purposes of *identity resolution*.

legal person
An individual, organization, or company with legal rights.

manageability
Providing the capability for the granular administration of *personally identifiable information*, including alteration, deletion, and selective disclosure. [NISTIR8062]

natural person
A real-life human being, not synthetic or artificial.

network
An open communications medium, typically the Internet, used to transport messages between the *claimant* and other parties. Unless otherwise stated, no assumptions are made about the network's security; it is assumed to be open and subject to active (e.g., impersonation, *session* hijacking) and passive (e.g., eavesdropping) attacks at any point between the parties (e.g., claimant, *verifier*, *CSP*, *RP*).

non-repudiation
The capability to protect against an individual falsely denying having performed a particular transaction.

offline attack
An attack in which the attacker obtains some data (typically by eavesdropping on an authentication transaction or by penetrating a system and stealing security files) that the attacker is able to analyze in a system of their own choosing.

one-to-one (1:1) comparison
The process in which a *biometric sample* from an individual is compared to a *biometric reference* to produce a comparison score.

online attack
An attack against an *authentication protocol* in which the attacker either assumes the role of a *claimant* with a genuine *verifier* or actively alters the authentication channel.

online service
A service that is accessed remotely via a *network*, typically the internet.

personal information
See *personally identifiable information*.

personally identifiable information (PII)
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. [A-130]

personally identifiable information processing
An operation or set of operations performed upon *personally identifiable information* that can include the collection, retention, logging, generation, transformation, use, disclosure, transfer, or disposal of personally identifiable information.

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 parties' policies and practices and can become legally binding.

predictability
Enabling reliable assumptions by individuals, owners, and operators about PII and its *processing* by an information system. [NISTIR8062]

private key
In *asymmetric key* cryptography, the private key (i.e., a secret key) is a mathematical key used to create *digital signatures* and, depending on the algorithm, decrypt messages or files that are encrypted with the corresponding *public key*. In *symmetric key* cryptography, the same private key is used for both encryption and decryption.

processing
Operation or set of operations performed upon PII that can include, but is not limited to, the collection, retention, logging, generation, transformation, use, disclosure, transfer, and disposal of PII. [NISTIR8062]

presentation attack
Presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system.

presentation attack detection (PAD)
Automated determination of a *presentation attack*. A subset of presentation attack determination methods, referred to as *liveness detection*, involves the measurement and analysis of anatomical characteristics or voluntary or involuntary reactions, to determine if a *biometric sample* is being captured from a living *subject* that is present at the point of capture.

process assistant
An individual who provides support for the proofing process but does not support decision-making or risk-based evaluation (e.g., translation, transcription, or accessibility support).

proofing agent
An agent of the *CSP* who is trained to attend *identity proofing sessions* and can make limited risk-based decisions – such as physically inspecting *identity evidence* and making physical comparisons of the *applicant* to identity evidence.

Privacy Impact Assessment (PIA)
A method of analyzing how *personally identifiable information* (PII) is collected, used, shared, and maintained. PIAs are used to identify and mitigate privacy risks throughout the development lifecycle of a program or system. They also help ensure that handling information conforms to legal, regulatory, and policy requirements regarding privacy.

pseudonym
A name other than a legal name.

pseudonymity
The use of a *pseudonym* to identify a *subject*.

pseudonymous identifier
A meaningless but unique *identifier* that does not allow the *RP* to infer anything regarding the subscriber but that does permit the RP to associate multiple interactions with a single subscriber.

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

public key certificate
A digital document issued and digitally signed by the *private key* of a certificate authority that binds an *identifier* to a subscriber's *public key*. The certificate indicates that the subscriber identified in the certificate has sole control of and access to the private key. See also [RFC5280].

public key infrastructure (PKI)
A set of policies, processes, server platforms, software, and workstations used to administer certificates and public-_private key_ pairs, including the ability to issue, maintain, and revoke *public key certificates*.

registration
See *enrollment*.

relying party (RP)
An entity that relies upon a *verifier*'s *assertion* of a subscriber's identity, typically to process a transaction or grant access to information or a system.

remote
A process or transaction that is conducted through connected devices over a *network*, rather than in person.

resolution
See *identity resolution*.

risk assessment
The process of identifying, estimating, and prioritizing risks to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, and other organizations that result from the operation of a system. A risk assessment is part of *risk management*, incorporates threat and vulnerability analyses, and considers mitigations provided by security *controls* that are planned or in-place. It is synonymous with "risk analysis."

risk management
The program and supporting processes that manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, and other organizations and includes (i) establishing the context for risk-related activities, (ii) assessing risk, (iii) responding to risk once determined, and (iv) monitoring risk over time.

RP subscriber account
An account established and managed by the *RP* in a federated system based on the RP's view of the *subscriber account* from the *IdP*. An RP subscriber account is associated with one or more *federated identifiers* and allows the subscriber to access the account through a *federation transaction* with the IdP.

Senior Agency Official for Privacy (SAOP)
Person responsible for ensuring that an agency complies with privacy requirements and manages privacy risks. The SAOP is also responsible for ensuring that the agency considers the privacy impacts of all agency actions and policies that involve PII.

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.

subject
A person, organization, device, hardware, *network*, software, or service. In these guidelines, a subject is a *natural person*.

subscriber
An individual enrolled in the *CSP* identity service.

subscriber account
An account established by the *CSP* containing information and *authenticators* registered for each subscriber enrolled in the CSP identity service.

supplemental controls
Controls that may be added, in addition to those specified in the organization's tailored assurance level, in order to address specific threats or attacks.

synthetic identity fraud
The use of a combination of *personally identifiable information* (PII) to fabricate a person or entity in order to commit a dishonest act for personal or financial gain.

system of record (SOR)
An SOR is a collection of records that contain information about individuals and are under the control of an agency. The records can be retrieved by the individual's name or by an identifying number, symbol, or other *identifier*.

System of Record Notice (SORN)
A notice that federal agencies publish in the Federal Register to describe their systems of records.

transaction
See *digital transaction*

trust agreement
A set of conditions under which a *CSP*, *IdP*, and *RP* are allowed to participate in a *federation transaction* for the purposes of establishing an authentication *session* between the subscriber and the RP.

trusted referee
An agent of the *CSP* who is trained to make risk-based decisions regarding an *applicant's identity proofing* case when that applicant is unable to meet the expected requirements of a defined IAL proofing process.

usability
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. [ISO/IEC9241-11]

validation
The process or act of checking and confirming that the evidence and *attributes* supplied by an *applicant* are authentic, accurate and associated with a real-life identity. Specifically, evidence validation is the process or act of checking that the presented evidence is authentic, current, and issued from an acceptable source. See also *attribute validation*.

verification
The process or act of confirming that the *applicant* undergoing *identity proofing* holds the claimed real-life identity represented by the validated identity *attributes* and associated evidence. Synonymous with "identity verification."

verifier
An entity that verifies the *claimant's* identity by verifying the claimant's possession and control of one or more *authenticators* using an *authentication protocol*. To do this, the verifier needs to confirm the binding of the authenticators with the *subscriber account* and check that the subscriber account is

Appendix D. Change Log

This appendix is informative.

This appendix provides a high-level overview of the changes to SP 800-63A since its initial release.

- Reorganizes the sections to introduce general identity proofing requirements before providing specific requirements
- Separates global requirements from IAL-specific requirements to facilitate the design of identity services, regardless of assurance level
- Provides requirements for lower-risk applications, through an updated IAL1
- Introduces fraud mitigation guidance and requirements
- Adds requirements for CSP-specific privacy and equity risk assessments and considerations for integrating the results into agency assessment processes
- Introduces the concept of core attributes
- Decouples the collection of identity attributes from the collection of identity evidence
- Adjusts evidence collection requirements for IALs 1 and 2
- Expands acceptable evidence and attribute validation sources to include credible sources
- Provides non-biometric options for identity verification at IALs 1 and 2
- Adds new guidance and requirements for subscriber accounts
- Adds new guidance and requirements for the consideration of equity risks associated with identity proofing processes
- Introduces exception handling concepts and requirements, including requirements for the use of trusted referees and applicant references