Modified NIST Special Publication 800-63A (Kantara Initiative Service Assessment Criteria)

v0.05

Digital Identity Guidelines

Enrollment and Identity Proofing

Abstract

This document is a modification of NIST's SP 800-63A, published 2017-06-21, for the purposes of establishing discrete and uniquely identifiable/referenceable requirements, so as to create a set of Kantara Initiative Service Assessment Criteria which has sufficient clarity and quantification to make it fit for consistent interpretation and application for the purposes of applying a Kantara assessment of a service against NIST SP 800-63-3, in the generic context.

The modifications have been applied based on the following principles:

a) only NORMATIVE text has been retained (hence, only §4 & 5 have been retained);
b) within that, the essential objective has been to only retain text applicable to AAL2, expressed either generally (implicitly) or explicitly;
c) for structural or other reasons, other text may have been retained for the sake of context preservation;
d) accepting the consequences of the above modifications, all headings, section numbering and text has been preserved as originally identified in SP 800-63A, so as to facilitate back-reference to the original source text, when required;
e) where it has been considered that the original text is insufficiently clear or precise, or optimally-arranged, revisions or additions have been made, which in some cases has included moving text from one section to another;
f) Indexing has been reversed from the original NIST publication: this document employs the following structure (see this loist):
   a)
      1)
         i)
   so as to minimize the potential mis-interpretation of (e.g.) 4.2 1. and 4.2.1). In addition, bullets in tables have been indexed;
g) in executing the principles described above every effort has been made to make the modifications completely transparent.

The intention has been to make minimal changes to the structure and content of the text, such that it will be readily identified as being from the NIST SP 800-63 rev.3 publication.

Keywords

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

Acknowledgments

NIST's original authorship is hereby acknowledged, as is the organization's willingness to release Word copy to facilitate this modified work.

Copyright

Requirements Notation and Conventions

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

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

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

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

The term "UNLESS" is used to indicate an alternative course of action, to be applied if a preceding requirement or possible action cannot be satisfactorily executed to a (typically positive) conclusion.

CAVEAT

This document is intended solely to clarify the normative requirements of the original NIST publication in a Kantara Initiative-specific context. It is NOT intended as a substitute for that document, whose informative sections provide extensive tutorial and context-setting guidance and background information, which is essential understanding for implementors, users, and others.

Form of Presentation

In the following normative sections retained from the original publication, all annotations, notes and requirements identification are shown in italicized dark red text shown between square brackets *[such as this text]*.

The discrete requirements are prefixed with a unique reference, derived from the original SP800-63A clause number and a sequence number within that clause, in this version at decimal spacing (to permit future sequential insertion of criteria, should that be necessary).

Where it is determined that the original text requires replacement with a new criterion written with the purpose of clarifying the original requirement, the original requirement is indicated as deprecated by grey shading, with the replacement criterion following.

Source text which has been moved from its original placement is indicated by <WHAT?> and a ref to its new location is substituted at the original placement.

Where it is determined that the source text is in need of amendment, modifications have been applied using distinct font conventions, i.e. *inserted text dark red, thus*, ~~deleted text bright red, thus~~.

4 Identity Assurance Level Requirements

This section contains both normative and informative material.

[No requirements can be derived from this section – there is no content which is normatively-expressed.]

> *[*Note: The identity proofing process can be delivered by multiple service providers. It is possible, but not expected, that a single organization, process, technique, or technology will fulfill these process steps.
> *Therefore the Kantara notion of a 'Component Service' survives.]*

4.1 Process Flow

This section is informative. «pending errata will make this informative»

[No requirements can be derived from this section – there is no content which is normatively-expressed.]

4.2 General Requirements

This section is normative.

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

a) *[4.2#0010:* Identity proofing SHALL NOT be performed to determine suitability or entitlement to gain access to services or benefits.
The CSP's proofing policy SHALL NOT require evidence of membership or eligibility for the purposes of determine suitability or entitlement to gain access to services or benefits, although forms of evidence based on such attributes MAY be used for the sole purpose of verifying and establishing an identity.]

b) *[4.2#0020:* Collection of PII SHALL be limited to the minimum necessary to validate the unique existence of the claimed identity in a given context and to associate the claimed identity with the applicant providing identity evidence for appropriate identity resolution, validation, and verification. This MAY include attributes that correlate identity evidence to authoritative sources and to provide RPs with attributes used to make authorization decisions.*]*

c) *[4.2#0030:* The CSP SHALL provide explicit notice to the applicant at the time of collection regarding the purpose for collecting and maintaining a record of the attributes necessary for identity proofing, including whether such attributes are voluntary or mandatory to complete the identity proofing process, and the consequences for not providing the attributes by documenting and publishing a Privacy Policy.
NOTE – So long as a cross-reference is made, indicating the voluntary or mandatory attributes could be addressed by the CrP – see 4.2#0070.]

d) *[4.2#0040:* The CSP SHALL NOT use attributes collected and maintained in the identity proofing process for any purpose other than identity proofing, authentication, or attribute

Comment [RGW@Zygma1]: Note – indexing has been reversed from the original NIST publication: this version runs a) 1) i) to minimize the potential mis-interpretation of (e.g.) 4.2 1. and 4.2.1 – see? Also, bullets in tables have been indexed.

Comment [RGW@Zygma2]: This criterion expressing format has the following features:
i) encloses the original text and the proposed KI criterion in square braclets;
ii) where possible uses the original text, with clarifying modification if necessary (modifications are ~~redlined if deleted~~, green if added);
iii) where deemed necessary, the original text is shaded grey and replaced with alternative, more precise or more granular, text, *in dark red italics*;
iv) may break down an original paragraph into discrete clauses, where necessary;
v) introduces some KI-specific concepts already employed in existing criteria;
vi) includes some 'presumptive' requirements based on rumoured FICAM expectations;
vii) maintains a sequential numeric tag, initially incremented decimally with a prefix which relates to the second-level source clause.

Comment [ZYG_RGW3]: added to reinforce the fact that this requirement effectively makes §4.4.1.1 a repetition.

assertions, or to comply with law or legal process unless the CSP provides clear notice and obtains consent from the subscriber for additional uses. CSPs SHALL NOT make consent with these additional purposes a condition of the service.*]*

e) *[4.2#0050:* The CSP SHALL provide mechanisms for redress of applicant complaints or problems arising from the identity proofing. These mechanisms SHALL be easy for applicants to find and use.*]*
[4.2#0060: The CSP SHALL assess the mechanisms for their efficacy in achieving resolution of complaints or problems.*]*

f) *[4.2#0070:* The identity proofing and enrollment processes SHALL be performed according to an applicable written policy
The CSP's identity proofing and enrollment policy SHALL be documented and published in its Credential Policy (CrP) which SHALL adopt the structure of RFC3647.]
[4.2#0080: or *practice statement* that specifies the particular steps taken to verify identities. The *practice statement* SHALL include control information detailing how the CSP handles proofing errors that result in an applicant not being successfully enrolled. For example, the number of retries allowed, proofing alternatives (e.g., in-person if remote fails), or fraud counter-measures when anomalies are detected.
The CSP SHALL document in its Credentialling Practice Statement (CrPS) the practices which it implements to fulfil its CrP intentions. The CrPS SHALL reflect the structure of its CrP and SHALL include control information detailing how the CSP handles proofing errors that result in an applicant not being successfully enrolled.
*NOTE – "*the number of retries allowed, proofing alternatives, ...*" etc. are expressed as exemplars and therefore are not considered as explicit requirements with which conformance has to be demonstrated.]*

g) *[4.2#0090:* The CSP SHALL maintain a record, including audit logs, of all steps taken to verify the identity of the applicant and SHALL record the types of identity evidence presented in the proofing process.*]*
[4.2#0100: The CSP SHALL document both its risk management process and the outcomes of applying that process.]
[4.2#0110: The CSP SHALL conduct a risk management process, including assessments of privacy and security risks, at least annually and whenever there is a significant change to its CrP, to determine:

1) Any steps that it will take to verify the identity of the applicant beyond any mandatory requirements specified herein;
2) The PII, including any biometrics, images, scans, or other copies of the identity evidence that the CSP will maintain as a record of identity proofing (Note: Specific federal requirements may apply.); and
3) The schedule of retention for these records (Note: CSPs may be subject to specific retention policies in accordance with applicable laws, regulations, or policies, including any National Archives and Records Administration (NARA) records retention schedules that may apply).*]*

h) *[4.2#0110:* All PII collected as part of the enrollment process SHALL be protected to ensure confidentiality, integrity, and attribution of the information source. *]*

Comment [ZYG_RGW4]: This pre-empting a forthcoming FICAM requirement. It is otherwise not required (especially since it is also not an existing KI requirement).

i) *[4.2#0120:* The entire proofing transaction, including transactions that involve a third party, SHALL occur over an authenticated protected channel. *]*

j) *[4.2#0130:* The CSP SHOULD obtain additional confidence in identity proofing using fraud mitigation measures (e.g., inspecting geolocation, examining the device characteristics of the applicant, evaluating behavioral characteristics, checking vital statistic repositories such as the Death Master File [DMF], so long as any additional mitigations do not substitute for the mandatory requirements contained herein. *]*
[4.2#0140: In the event the CSP uses fraud mitigation measures, the CSP SHALL conduct a privacy risk assessment for these mitigation measures. Such assessments SHALL include any privacy risk mitigations (e.g., risk acceptance or transfer, limited retention, use limitations, notice) or other technological mitigations (e.g., cryptography), and be documented per requirement 4.2(7) above.
Note –requirement 4.2#0140 is enforceable only if the preceding clause is invoked.]

k) *[4.2#0150:* In the event a CSP ceases to conduct identity proofing and enrollment processes, the CSP SHALL be responsible for fully disposing of or destroying any sensitive data including PII, or its protection from unauthorized access for the duration of retention. *]*

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

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

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

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

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

[Note – this clause has no bearing in the context of a Kantara assessment – this is an internal agency responsibility applicable outside the scope of the service per se*, as the introductory qualifier states.]*

m) *[4.2#0160:* The CSP SHOULD NOT collect the Social Security Number (SSN) UNLESS it is necessary for performing identity resolution, and identity resolution cannot be accomplished by collection of another attribute or combination of attributes. *]*

4.3 Identity Assurance Level 1

This section is normative.
[No treatment is given to this section.]

A CSP that supports only IAL1 NEED~~CSPSHALLM~~ NOT validate and verify attributes.

a) The CSP MAY request zero or more self-asserted attributes from the applicant to support their service offering.

b) An IAL2 or IAL3 CSP SHOULD support RPs that only require IAL1, if the user consents.

4.4 Identity Assurance Level 2

This section is normative.

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

[4.4#0010: A CSP SHALL proof according to the requirements in Section 4.4.1 or Section 4.4.2. A CSP SHOULD implement identity proofing in accordance Section 4.4.1 Depending on the population the CSP serves, the CSP MAY implement identity proofing in accordance with Section 4.4.2.
A CSP SHALL preferentially proof according to the requirements in Section 4.4.1. If the applicant fails that proofing process the CSP MAY additionally proof according to the requirements in Section 4.4.2.] *«this text potentially in pending errata»*

4.4.1 IAL2 Conventional Proofing Requirements

The following sections provide requirements for IAL2 resolution, evidence collection, validation, verification, and presence. They also explore biometric collection and security controls.

4.4.1.1 Resolution Requirements

*[*Collection of PII SHALL be limited to the minimum necessary to resolve to a unique identity in a given context. This MAY include the collection of attributes that assist in data queries. See Section 5.1 for general resolution requirements.
Editor's notes – 1) This is re-stating a previous requirement - see 4.2#0020: 2) §5.1 has no explicitly normative requirements]

4.4.1.2 Evidence Collection Requirements

[4.4#0010: The CSP SHALL collect the following from the applicant:

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

Comment [RGW@Zygma5]: If the point is to establish minima, no need to express a highter-level requirement.

[4.4#0020: The CSP SHALL document its justification, for each form of evidence it recognises in fulfilling its CrP and these criteria, of how the strength of the evidence it collects satisfies the qualities identified in Table 4-1, taking into account the following:

a) The CSP MAY employ appropriate matching algorithms to account for differences in personal information and other relevant proofing data across multiple forms of identity evidence, issuing sources, and authoritative sources. Matching algorithms and rules used SHOULD be available publicly or, at minimum, to the relevant community of interest;
b) The CSP MAY use Knowledge-based verification (KBV) - sometimes referred to as knowledge-based authentication or questions (KBA / KBQ) - to resolve to a unique, claimed identity.*]*

Table 4-2 Strengths of Identity Evidence

Comment [RGW@Zygma6]: Moved here since not relevant anywhere else

Strength	Qualities of Identity Evidence
[Editor's note: Only those strengths applicable to IAL2 have been retained, hence 'e)' is the initial entry.]	
Fair	e) ~~T~~It can be demonstrated or otherwise reasonably expected that the issuing source of the evidence*:* f) confirmed the claimed identity through an identity proofing process. g) The issuing process for the evidence means that it can reasonably be assumed to have been delivered into the possession of the person to whom it relates. h) The evidence: 1) Contains at least one reference number that uniquely identifies the person to whom it relates, **OR** 2) Contains a photograph or biometric template (any modality) of the person to whom it relates, **OR** 3) Can have ownership confirmed through KBV. *e) It can be demonstrated or otherwise reasonably expected that the issuing source of the evidence:* *1) confirmed the claimed identity through an identity proofing process.* *2) delivered the evidence into the possession of the person to whom it relates.* *f) The evidence:* *1) Contains at least one reference number that uniquely identifies the person to whom it relates, **OR*** *2) Contains a photograph or biometric template (any modality) of the person to whom it relates, **OR*** *3) Can have ownership confirmed through KBV.* g) Where the evidence includes digital information, that information is protected using cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the claimed issuing source to be confirmed. h) Where the evidence includes physical security features, it requires proprietary knowledge to be able to reproduce it.

Strength	Qualities of Identity Evidence
	i) The issued evidence is unexpired.
Strong	j) ~~T~~It can be demonstrated or otherwise reasonably expected that the issuing source of the evidence: 1) confirmed the claimed identity through written procedures designed to enable it to form a reasonable belief that it knows the real-life identity of the person. Such procedures shall be subject to recurring oversight by regulatory or publicly-accountable institutions. For example, the Customer Identification Program guidelines established in response to the USA PATRIOT Act of 2001 or the Red Flags Rule, under Section 114 of the Fair and Accurate Credit Transaction Act of 2003 (FACT Act). 2) ~~The issuing process for the evidence ensured that it was~~ delivered the evidence into the possession of the subject to whom it relates. k) The issued evidence contains at least one reference number that uniquely identifies the person to whom it relates. l) The full name on the issued evidence must be the name that the person was officially known by at the time of issuance. Not permitted are pseudonyms, aliases, an initial for surname, or initials for all given names. m) The: 1) Issued evidence contains a photograph or biometric template (of any modality) of the person to whom it relates, **OR** 2) Applicant proves possession of an AAL2 authenticator bound to an IAL2 identity, at a minimum. n) Where the issued evidence includes digital information, that information is protected using cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the claimed issuing source to be confirmed. o) Where the issued evidence contains physical security features, it requires proprietary knowledge and proprietary technologies to be able to reproduce it. p) The evidence is unexpired.
Superior	q) ~~T~~It can be demonstrated or otherwise reasonably expected that the issuing source of the evidence: 1) confirmed the claimed identity by following written procedures designed to enable it to have high confidence that the source knows the real-life identity of the subject. Such procedures shall be subject to recurring oversight by regulatory or publicly accountable institutions. 2) ~~The issuing source~~ visually identified the applicant and performed further checks to confirm the existence of that person. 3) ~~The issuing process for the evidence ensured that it was~~ delivered the evidence into the possession of the person to whom it relates. r) The evidence contains at least one reference number that uniquely identifies the person to whom it relates.

Strength	Qualities of Identity Evidence
	s) The full name on the evidence must be the name that the person was officially known by at the time of issuance. Not permitted are pseudonyms, aliases, an initial for surname, or initials for all given names. t) The evidence contains a photograph of the person to whom it relates. u) The evidence contains a biometric template (of any modality) of the person to whom it relates. v) The evidence includes digital information, the information is protected using cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the issuing source to be confirmed. w) The evidence includes physical security features that require proprietary knowledge and proprietary technologies to be able to reproduce it. x) The evidence is unexpired.

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

4.4.1.3 Validation Requirements

The CSP SHALL validate identity evidence as follows:

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

[4.4#0030: The CSP SHALL document its justification, for each form of evidence it recognises in fulfilling its CrP and these criteria, of how it validates each piece evidence it collects against the qualities identified in Table 4-2]

Table 4-3 Validating Identity Evidence

Strength	Method(s) Performed by the CSP
Fair	c) Attributes contained in the evidence have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s), **OR** d) The evidence has been confirmed as genuine using appropriate technologies, confirming the integrity of physical security features and that the evidence is not fraudulent or inappropriately modified, **OR** e) The evidence has been confirmed as genuine by trained personnel, **OR** f) The evidence has been confirmed as genuine by confirmation of the integrity of cryptographic security features.

Strength	Method(s) Performed by the CSP
Strong	g) The evidence has been confirmed as genuine: 1) using appropriate technologies, confirming the integrity of physical security features and that the evidence is not fraudulent or inappropriately modified, **OR** 2) by trained personnel and appropriate technologies, confirming the integrity of the physical security features and that the evidence is not fraudulent or inappropriately modified, **OR** 3) by confirmation of the integrity of cryptographic security features. h) All personal details and evidence details have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s).
Superior	i) The evidence has been confirmed as genuine by trained personnel and appropriate technologies including the integrity of any physical and cryptographic security features. j) All personal details and evidence details from the evidence have been confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s).

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

[4.4#0030: The CSP SHALL document its policies, guidelines, and requirements for the ~~T~~training requirements for personnel validating evidence ~~SHALL be based on the policies, guidelines, or requirements of the CSP or RP~~. *]*

Comment [RGW@Zygma7]: KI only assess the CSP, therefore we can only put this onus on the CSP. The source text is a clear 'or', so there is no explicit requirement to accommodate the RP.
The CSP may choose, in its policies or through contract, to meet RP requirements. The assessment would cover that, however it was defined.

4.4.1.4 Verification Requirements

[4.4#0040: The CSP SHALL verify identity evidence as follows:

a) At a minimum, verifying the applicant's binding to identity evidence ~~must be verified~~ by a process that is able to achieve a strength of STRONG;
b) ~~The CSP SHALL adhere to~~ the requirements in Section 5.3.2 shall be adhered to if KBV is used to verify an identity {from §5.3.1}
c) Knowledge-based verification (KBV) SHALL NOT be used for in-person (physical or supervised remote) identity verification.*]*

[4.4#0050: The CSP SHALL document its justification, for each form of evidence it recognises in fulfilling its CrP and these criteria, of how it verifies each piece evidence it collects against the STRONG qualities identified in Table 4-3]

Table 4-4 Verifying Identity Evidence

Strength	Identity Verification Methods
Strong	d) The applicant's ownership of the claimed identity has been confirmed

Strength	Identity Verification Methods
	by: 1) physical comparison, using appropriate technologies, to a photograph, to the strongest piece of identity evidence provided to support the claimed identity. Physical comparison performed remotely SHALL adhere to all requirements as specified in SP 800-63B, Section 5.2.3, **OR** 2) biometric comparison, using appropriate technologies, of the applicant to the strongest piece of identity evidence provided to support the claimed identity. Biometric comparison performed remotely SHALL adhere to all requirements as specified in SP 800-63B, Section 5.2.3.
Superior	e) The applicant's ownership of the claimed identity has been confirmed by biometric comparison of the applicant to the strongest piece of identity evidence provided to support the claimed identity, using appropriate technologies. Biometric comparison performed remotely SHALL adhere to all requirements as specified in SP 800-63B, Section 5.2.3.

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

4.4.1.5 Presence Requirements

[4.4#0060: The CSP SHALL support at least one of in-person or remote identity proofing.*]* The CSP SHOULD offer both in-person and remote proofing.

4.4.1.6 Address Confirmation

[4.4#0070: The CSP SHALL confirm address by:

a) ~~Valid records to confirm address SHALL be~~relying only upon issuing source(s) or authoritative source(s).

b) ~~The CSP SHALL confirm address of record.~~ The CSP SHOULD confirm address of record through validation of the address contained on any supplied, valid piece of identity evidence. The CSP MAY confirm address of record by validating information supplied by the applicant that is not contained on any supplied piece of identity evidence.

c) ~~Self-asserted address data that has not been confirmed in records SHALL~~ NOT ~~be~~ using~~ed~~ a self-asserted address data that has not been confirmed in records~~for confirmation~~.

d) If the CSP performs in-person proofing (physical or supervised remote):

1) The CSP SHOULD send a notification of proofing to a confirmed address of record.
2) The CSP MAY provide an enrollment code directly to the subscriber if binding to an authenticator will occur at a later time.
3) The enrollment code SHALL be valid for a maximum of 7 days.

e) If the CSP performs remote proofing (unsupervised):

1) The CSP SHALL send an enrollment code to a confirmed address of record for the applicant.

2) The applicant SHALL present a valid enrollment code to complete the identity proofing process.
3) The CSP SHOULD send the enrollment code to the postal address that has been validated in records. The CSP MAY send the enrollment code to a mobile telephone (SMS or voice), landline telephone, or email if it has been validated in records.
4) If the enrollment code is also intended to be an authentication factor, it SHALL be reset upon first use.
~~5) Enrollment codes sent to a postal address of record SHALL be valid for a maximum of 10 days but MAY be made valid up to 30 days via an exception process to accommodate addresses outside the contiguous United States. Enrollment codes sent by telephone SHALL be valid for a maximum of 10 minutes. Enrollment codes sent via email SHALL be valid for a maximum of 24 hours.~~
6) SHALL have the following maximum validities:
    i) 10 days, when sent to a postal address of record within the contiguous United States;
    ii) 30 days, when sent to a postal address of record outside the contiguous United States;
    iii) 10 minutes, when sent to a telephone number of record (SMS or voice);
    iv) 24 hours, when sent ~~via~~to an email address of record.
7) The CSP SHALL ensure the enrollment code and notification of proofing are sent to different addresses of record. For example, if the CSP sends an enrollment code to a phone number validated in records, a proofing notification will be sent to the postal address validated in records or obtained from validated and verified evidence, such as a driver's license.*]*

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

4.4.1.7 Biometric Collection

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

4.4.1.8 Security Controls

[4.4#0080: The CSP SHALL employ appropriately tailored security controls, to include control enhancements, from the moderate or high baseline of security controls defined in SP 800-53 or equivalent federal (e.g., FEDRAMP) or industry standard. The CSP SHALL ensure that the minimum assurance-related controls for *moderate-impact* systems or equivalent are satisfied.
The CSP SHALL employ appropriately-tailored security controls, to include control enhancements, for moderate-impact systems as defined in SP 800-53 or equivalent federal (e.g., FEDRAMP) or industry standards.]

4.4.2 IAL2 Trusted Referee Proofing Requirements

[Editor's note: The following criteria have been extracted from §5.3.4.]

The CSP MAY use trusted referees — such as notaries, legal guardians, medical professionals, conservators, persons with power of attorney, or some other form of trained and approved or certified individuals — that can vouch for or act on behalf of the applicant in accordance with applicable laws, regulations, or agency policy. The CSP MAY use a trusted referee for both.

The CSP SHALL establish written policy and procedures as to how a trusted referee is determined and the lifecycle by which the trusted referee retains their status as a valid referee, to include any restrictions, as well as any revocation and suspension requirements.

The CSP SHALL proof the trusted referee at the same IAL as the applicant proofing. In addition, the CSP SHALL determine the minimum evidence required to bind the relationship between the trusted referee and the applicant.

/The CSP SHOULD perform re-proofing of the subscriber at regular intervals defined in the written policy specified in item 1 above, with the goal of satisfying the requirements of Section 4.4.1.

[EDITOR's NOTE – in the following the highlighting is purely to validate the fulfilment of the preceeding original requirements.]

[4.4#0090: CSPs SHALL identity-proof Trusted Referees according to the same criteria that are applied to normal applicants, i.e. criteria in §4.2 and §4.4 EXCLUDING THIS §4.4.2.]

EDITOR's NOTE – It is not clear what item a), below, really means (only judges? Only judges, dentists and attorneys: no schmucks???, i.e. might it refer to a required attribute in this case), but it could be this requirement, in which case this text should take the place of that in a) below.]

[4.4#0100: The CSP SHALL include in its CrP the following:

a) how a trusted referee is determined;
b) the lifecycle by which the trusted referee retains their status as a valid referee;
c) the minimum evidence required to bind the relationship between the trusted referee and the applicant;
d) any restrictions, as well as any revocation and suspension requirements;]

4.5 Identity Assurance Level 3

This section is normative.
[No treatment is given to this section – IAL3 is not addressed in this modification.]

4.6 Enrollment Code

This section is normative.

Comment [ZYG_RGW8]: This implicit through criteria 4.2#0070 (CrP)

Comment [ZYG_RGW9]: This implicit through criteria 4.2#0080 (CrPS)

Comment [ZYG_RGW10]: Insofar as trusted referees are concerned, this clause appears to be a *non sequitur*. No criteria applied, pending clarification with NIST: Is this intended to be applicable solely to subjects which required a TR, or for all subjects? And in either case, is this a practical proposition?

Comment [ZYG_RGW11]: otherwise we achieve recursion that the NIST doc doesn't explicitly exlcude

[4.6#0010: Binding NEED NOT be completed in the same session as the original identity proofing transaction.*]*

[4.6#0020: An enrollment code SHALL be comprised of one of the following:

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

5 Identity Resolution, Validation, and Verification

This section is normative.

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

5.1 Identity Resolution

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

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

5.2 Identity Evidence Collection and Validation

The goal of identity validation is to collect the most appropriate identity evidence (e.g., a passport or driver's license) from the applicant and determine its authenticity, validity, and accuracy. Identity validation is made up of three process steps: collecting the appropriate identity

evidence, confirming the evidence is genuine and authentic, and confirming the data contained on the identity evidence is valid, current, and related to a real-life subject.

5.2.1 Identity Evidence Quality Requirements

This section provides quality requirements for identity evidence collected during identity proofing.
[The IAL2-relevant parts of this table have been moved to §4.4.1.2.]

5.2.2 Validating Identity Evidence

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

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

Error! Reference source not found. lists strengths, ranging from unacceptable to superior, of identity validation performed by the CSP to validate the evidence presented for the current proofing session and the information contained therein.

[The IAL2-relevant parts of this section, including Table 5-2, have been moved to §4.4.1.3.]

5.3 Identity Verification

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

5.3.1 Identity Verification Methods

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

[The IAL2-relevant parts of this section, including Table 5-3, have been moved to §4.4.1.4.]

5.3.2 Knowledge-Based Verification Requirements

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

[5.3#0010: The following KBV requirements SHALL be observed:

a) The CSP SHALL NOT use KBV to verify an applicant's identity against more than one piece of validated identity evidence.

b) The CSP SHALL only use information that is expected to be known only to the applicant and the authoritative source, to include any information needed to begin the KBV process. Information accessible freely, for a fee in the public domain, or via the black market, SHALL NOT be used.
c) The CSP SHALL allow a resolved and validated identity to opt out of KBV and leverage another process for verification.
d) The CSP SHOULD perform KBV by verifying knowledge of recent transactional history in which the CSP is a participant. The CSP SHALL ensure that transaction information has at least 20 bits of entropy. For example, to reach minimum entropy requirements, the CSP could ask the applicant for verification of the amount(s) and transaction numbers(s) of a micro-deposit(s) to a valid bank account, so long as the total number of digits is seven or greater.
e) The CSP MAY perform KBV by asking the applicant questions to demonstrate they are the owner of the claimed information. However, the following requirements apply:
    1) KBV SHOULD be based on multiple authoritative sources.
    2) The CSP SHALL require a minimum of four KBV questions with each requiring a correct answer to successfully complete the KBV step.
    3) The CSP SHOULD require free-form response KBV questions. The CSP MAY allow multiple choice questions, however, if multiple choice questions are provided, the CSP SHALL require a minimum of four answer options per question.
    4) The CSP SHOULD allow two attempts for an applicant to complete the KBV. A CSP SHALL NOT allow more than three attempts to complete the KBV.
    5) The CSP SHALL time out KBV sessions after two minutes of inactivity per question. In cases of session timeout, the CSP SHALL restart the entire KBV process and consider this a failed attempt.
    6) The CSP SHALL NOT present a majority of diversionary KBV questions (i.e., those where "none of the above" is the correct answer).
    7) The CSP SHOULD NOT ask the same KBV questions in subsequent attempts *in any given application*.
    8) The CSP SHALL NOT ask a KBV question that provides information that could assist in answering any future KBV question in a single session or a subsequent session after a failed attempt.
    9) The CSP SHALL NOT use KBV questions for which the answers do not change (e.g., "What was your first car?").
    10) The CSP SHALL ensure that any KBV question does not reveal PII that the applicant has not already provided, nor personal information that, when combined with other information in a KBV session, could result in unique identification.*]*

5.3.3 In-Person Proofing Requirements

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

A physical interaction with the applicant, supervised by an operator.
A~~n~~ remote interaction with the applicant, supervised by an operator, based on the specific requirements *in* Section 5.3.3.2.

5.3.3.1 General Requirements

1. *[5.3#0020:* The CSP SHALL have the operator view the biometric source (e.g., fingers, face) for presence of non-natural materials and perform such inspections as part of the proofing process.*]*
2. *[5.3#0030:* The CSP SHALL collect biometrics in such a way that ensures that the biometric is collected from the applicant, and not another subject. All biometric performance requirements in SP 800-63B, Section 5.2.3 SHALL apply. *]*

5.3.3.2 Requirements for Supervised Remote In-Person Proofing

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

[5.3#0040: Supervised remote identity proofing and enrollment transactions SHALL meet the following requirements, in addition to the IAL3 validation and verification requirements specified in Section 4.6:

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

5.3.4 Trusted Referee Requirements

[These requirements have been re-expressed at §4.4.2.]

5.3.4.1 Additional Requirements for Minors

1. *[5.3#0050:* The CSP SHALL give special consideration to the legal restrictions of interacting with minors unable to meet the evidence requirements of identity proofing to

ensure compliance with the Children's Online Privacy Protection Act of 1998, and other laws, as applicable.*]*

2. *[5.3#0060:* Minors under age 13 require additional special considerations under COPPA, and other laws, to which the CSP SHALL ensure compliance, as applicable.*]*
3. The CSP SHOULD involve a parent or legal adult guardian as a trusted referee for an applicant that is a minor, as described elsewhere in this section.

5.4 Binding Requirements

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

6 Derived Credentials

This section is informative.

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

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

There are two specific use cases for deriving identity:

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

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