Title:	Identity Assurance Framework: NIST SP 800-63A Service Assessment Criteria (SAC) & Statement of Criteria Applicability (SoCA)
Document id:	KIAF-1430
Version:	4.0
Document type:	Recommendation
Publication Date:	2020-10-15
Effective Date:	2021-02-01
Status:	Final
Approval Authority:	IAWG
Sponsor:	ID.me Inc.
IAWG Sub-group Participants / Non-participants	Ken DAGG (Individual contributor) Nathan FAUT (KPMG) Mark HAPNER (Resilient Networks) Andrew HUGHES (IDEMIA) James JUNG (Slandala) Martin SMITH (Individual contributor) Richard WILSHER (Zygma Inc.)
IPR:	Patent and Copyright Option: Reciprocal Royalty Free with Opt-Out to Reasonable and Non-Discriminatory terms (RAND) | © 2020
Abstract:	This Specification sets forth KI's Service Assessment Criteria for assessments against the requirements of NIST's SP 800-63A as published 2017-12-01 (with errata) at IAL2 & IAL3, to be generally referred-to as the '63A_SAC'. It is anticipated that these criteria will be reviewed 12 months after publication, for any required re-expression,
Notice:	All rights reserved. This Specification has been prepared by Participants of the Identity Assurance Working Group of the Kantara Initiative. No rights are granted to Non-Participants of the Identity Assurance Working Group nor any other person or entity to reproduce or otherwise prepare derivative works without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. Entities seeking permission to reproduce portions of this Specification for other uses must contact the Kantara Initiative to determine whether an appropriate license for [illegible] Implementation or use of certain elements of this Specification may require licenses under third party intellectual property rights, including without limitation, patent rights. The Participants of and any other contributors to the document are not and shall not be held responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights. This document is provided "AS IS" and no Participant in the Kantara Initiative makes any warranty of any kind, expressed or implied, including any implied warranties of merchantability, non-infringement of third party intellectual property rights, and fitness for a particular purpose.

Though this document is structured with headers, footers etc. for document management purposes, the 63A_SAC and other criteria-related worksheets are not intended to be published in a printed page format, and hence 'Normal' View is recommended at all times.

KIAF-1430 SP 800-63A Service Assessment Criteria - Revision History

Version	*Date*	*Status*	*Summary of changes*
Note re. version numbers:		*Changes which the IAWG considers to be Non-Material shall be incremented by '0.1', whereas changes considered to be MATERIAL shall be raised to the next whole number.*	
v4.0	10/15/20	Final - Material changes - released for application	Addition of criteria to: 1) cover IAL3; 2) requirements on Federal Agencies and Relying Parties. Also, addition of explicit SoCA and SoC columns.
v3.1	2019-01-31	Final - Non-Material changes - released for application	Adoption within the 63A criteria set of certain 63**B**_SAC criteria which are twice-referenced from SP 800-63A for identity proofing purposes: 63A criteria introduced: 63A#1300 - '1380 inc.; 63A#2300 - '2380 inc.; 63A criteria amended (to now reference the above new criteria): #0380; 63A-T5-3#strg a) i) & ii), 63A-T5-3#supr a). Clarification of applicability of some specific criteria to specific modes of proofing: 63A criteria amended: #0360, #0370, #0380. Introduction of a column for Guidance. Addition of this revision history as a separate worksheet.
v3.0	2018-11-09	Final - Non-Material changes - released for application	Typo tidying and clarifications of some criteria's wording; alignment of -63A requirements to pre-existing CO_SAC criteria (re. risk management review period); amendment to applicable -63**B** criteria: 63A criteria amended: #0090, #0100, #0110, #0140, #0350, 63A-T5-3#strg a) i) & ii), 63A-T5-3#supr a)
v2.0	2018-02-15	Final - Material changes - released for application	First release for application, following resolution of public comments on v1.0.
v1.0	14/12/2017	For Public review	Initial set of mature draft criteria.

NIST SP 800-63A (rev.3) SAC & SoCA v4.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				IAL		CRITERION APPLICABILITY (SoCA)	Guidance
4.2	1	General Requirements	Identity proofing SHALL NOT be performed to determine suitability or entitlement to gain access to services or benefits.	✓				63A#0010			*The CSP SHALL NOT perform identity proofing to determine suitability or entitlement to gain access to services or benefits.*	✓	✓		*This apparent prohibition need not preclude the collection, at the time of the collection of necessary proofing information, of additional information for post-proofing use so long as that additional information is not used during the proofing process.*
4.2	2	General Requirements	Collection of PII SHALL be limited to the minimum necessary to validate the existence of the claimed identity and associate the claimed identity with the applicant providing identity evidence for appropriate identity resolution, validation, and verification. This MAY include attributes that correlate identity evidence to authoritative sources and to provide RPs with attributes used to make authorization decisions.	✓				63A#0020			*The CSP SHALL limit collection of PII to the minimum necessary to validate and resolve the existence of the claimed identity uniquely in a given context, and to associate the claimed identity with the Applicant providing identity evidence for appropriate identity resolution, validation, and verification.*	✓	✓		
4.2	3	General Requirements	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.	✓				63A#0030			*The CSP SHALL document and publish a Privacy Notice which describes its purposes in collecting and maintaining a record of the attributes necessary for identity proofing, including whether such attributes are voluntary or mandatory to complete the identity proofing process, and the consequences for not providing the attributes.*	✓	✓		
4.2	3+	General Requirements		✓				63A#0040			*The CSP SHALL explicitly make its Privacy Notice available to the Applicant at the time of collection of the attributes necessary for the Applicant's identity proofing,*	✓	✓		
4.2	4	General Requirements	If CSPs process attributes for purposes other than identity proofing, authentication, or attribute assertions (collectively "identity service"), related fraud mitigation, or to comply with law or legal process, ...	✓				63A#0050			*If the CSP processes attributes which it collects and stores for purposes other than identity proofing, authentication, or attribute assertions, related fraud mitigation, or to comply with law or legal process), it SHALL:*	✓	✓		
4.2	4	General Requirements	... CSPs SHALL implement measures to maintain predictability and manageability commensurate with the privacy risk arising from the additional processing.	✓				63A#0050	a)		*document and apply predictability and manageability measures associated with those additional processes based on the results of its privacy risk assessment; (see 63A#0160)*	✓	✓		
4.2	4	General Requirements	When CSPs use consent measures,CSPs SHALL NOT make consent with these additional purposes a condition of the service.	✓				63A#0050	b)		*NOT make consent to processing of these additional attributes a condition of provision of the service.*	✓	✓		
4.2	5	General Requirements	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.	✓				63A#0060			*The CSP SHALL provide mechanisms to redress Applicant complaints or problems arising from their use of the identity proofing service.*	✓	✓		
				✓				63A#0062			*The CSP SHALL document and publish its redress mechanisms in a manner which is easy for Applicants to find and use.*	✓	✓		

NIST SP 800-63A (rev.3) SAC & SoCA v4.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				IAL		CRITERION APPLICABILITY (SoCA)	Guidance
4.2	5	General Requirements	The CSP SHALL assess the mechanisms for their efficacy in achieving resolution of complaints or problems.	✓				63A#0070			The CSP SHALL review its redress mechanisms at least every 12 months and assess their efficacy in achieving resolution of complaints or problems , implementing corrective action when efficacy falls below defined thresholds of performance or accomplishment.	✓	✓		
4.2	6	General Requirements	The identity proofing and enrollment processes SHALL be performed according to an applicable written policy …	✓				63A#0080			The CSP SHALL:	✓	✓		
4.2	6	General Requirements		✓				63A#0080	a)		document in a Credential Policy (CrP) its identity proofing and enrollment policy/ies;	✓	✓		
4.2	6	General Requirements	*Kantara note - see SP 800-63-3 definition of 'Authoritative Source'.*	✓				63A#0080	b)		for each type of identity proofing offered (see 63A#0260), state which issuing and authoritative sources are used to prove identities;	✓	✓		
4.2	6	General Requirements		✓				63A#0080	c)		state any eligibility requirements or limitations which it applies to the scope of Applicants to its identity proofing service, subject to such limitations not breaching the restriction placed by 63A#0010;	✓	✓		Moved from being the prior 63A#0050
4.2	6	General Requirements		✓				63A#0080	d)		publish its CrP such that it is available to members of the intended community (e.g. Applicants, Subscribers, Relying Parties, …) before they are required to commit to signing-up to being a subject of the policy.	✓	✓		See also CO_SAC/CO#0090, if included in the assessment. Previously c) of this set.
4.2	6	General Requirements	… or *practice statement* that specifies the particular steps taken to verify identities.	✓				63A#0090			The CSP SHALL document in its Credentialing Practices Statement (CrPS) the practices which it implements to fulfil its CrP intentions.	✓	✓		
4.2	6	General Requirements	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.	✓				63A#0100			The CSP's CrPS SHALL reflect the structure of its CrP and SHALL include control information detailing how the CSP handles proofing errors or other circumstances that result in an Applicant not being successfully enrolled.	✓	✓		
4.2	7+	General Requirements	The CSP SHALL conduct a risk management process, including assessments of privacy and security risks to determine:	✓				63A#0110			The CSP SHALL document both its risk management process (at least in the context of its identity proofing policy and practices) and the outcomes of applying that process.	✓	✓		
				✓				63A#0120			The CSP SHALL conduct its risk management process at least once every six months and whenever there is a material change to its CrP, and SHALL include assessment of privacy and security risks, accounting for:	✓	✓		
4.2	7	General Requirements	Any steps that it will take to verify the identity of the applicant beyond any mandatory requirements specified herein;	✓				63A#0120	a)		Any steps that it will take to verify the identity of the Applicant beyond any mandatory requirements specified herein;	✓	✓		
4.2	7	General Requirements	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	✓				63A#0120	b)		The PII which the CSP shall collect and store (per its CrP), including any biometrics, images, scans, or other copies of the identity evidence that the CSP will maintain as a record of identity proofing; and	✓	✓		
4.2	7	General Requirements	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).	✓				63A#0120	c)		The CSP's Retention Schedule requirements for collected PII and associated records, accounting for applicable laws, regulations, contracts, and policies.	✓	✓		
4.2	7	General Requirements	The CSP SHALL maintain a record, including audit logs, of …	✓				63A#0130			The CSP SHALL maintain a record, including audit logs, of:	✓	✓		

NIST SP 800-63A (rev.3) SAC & SoCA v4.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				IAL		CRITERION APPLICABILITY (SoCA)	Guidance
4.2	7	General Requirements		✓				63A#0130	a)		the type of identity proofing performed;	✓	✓		
4.2	7	General Requirements	… all steps taken to verify the identity of the applicant and … [see e)]	✓				63A#0130	b)		the types of and a unique reference to identity evidence collected from the Applicant in the proofing process;	✓	✓		
4.2	7	General Requirements		✓				63A#0130	c)		PII or other responses collected from authoritative and/or issuing sources;	✓	✓		
4.2	7	General Requirements	… SHALL record the types of identity evidence presented in the proofing process. [see b)]	✓				63A#0130	d)		all steps taken to validate the identity evidence;	✓	✓		
4.2	7	General Requirements		✓				63A#0130	e)		all steps taken to verify the identity of the Applicant;	✓	✓		
4.2	7	General Requirements		✓				63A#0130	f)		the outcome of each step, culminating in the final proofing result.	✓	✓		
4.2	8	General Requirements	All PII collected as part of the enrollment process SHALL be protected to ensure confidentiality, integrity, and attribution of the information source.	✓				63A#0140			The CSP SHALL protect all PII collected as part of the enrollment process, including validation and verification sources used, to ensure its confidentiality, integrity, and attribution of the information source.	✓	✓		
4.2	9	General Requirements	The entire proofing transaction, including transactions that involve a third party, SHALL occur over an authenticated protected channel.	✓				63A#0150			The CSP shall use authenticated protected channels during the entire proofing transaction, including exchanges with third parties.	✓	✓		
4.2	10	General Requirements	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.	✓				63A#0160			IF the CSP uses fraud mitigation measures, it SHALL include these measures in its privacy risk assessment for these mitigation measures.	✓	✓		
4.2	11	General Requirements	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.	✓				63A#0170			The CSP SHALL define the practices in place for fully disposing of or destroying any sensitive data including PII, or its protection from unauthorized access for the duration of retention. Specific details of these practices must be made available.	✓	✓		
4.4.1.2 (IAL2)		Evidence Collection Requirements	The CSP SHALL collect the following from the applicant:	✓				63A#0180			The CSP SHALL collect from the Applicant at least the following strength of evidence, as determined by the further requirements in Table 5-1:	✓			
4.4.1.2 (IAL2)	1	Evidence Collection Requirements	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	✓				63A#0180	a)		One piece of 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**	✓			
4.4.1.2 (IAL2)	2	Evidence Collection Requirements	Two pieces of STRONG evidence; OR	✓				63A#0180	b)		Two pieces of STRONG evidence; OR	✓			
4.4.1.2 (IAL2)	3	Evidence Collection Requirements	One piece of STRONG evidence plus two pieces of FAIR evidence.	✓				63A#0180	c)		One piece of STRONG evidence plus two pieces of FAIR evidence.	✓			
4.4.1.2 (IAL2)		Evidence Collection Requirements		✓				63A#0190			The CSP SHALL document its justification, for each form of evidence it recognises and collects in fulfilling its CrP and these criteria, of how the strength of the evidence it collects satisfies the qualities identified in Table 5-1 [see worksheet 63A_T5-1].	✓			

NIST SP 800-63A (rev.3) SAC & SoCA v4.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				IAL		CRITERION APPLICABILITY (SoCA)	Guidance
4.4.1.3 (IAL2)		Validation Requirements	The CSP SHALL validate identity evidence 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	✓				63A#0200			*The CSP SHALL, at a minimum, validate identity evidence at the same strength as that at which the evidence was collected.*	✓	✓		
			Kantara-specific requirement	✓				63A#0210			*The CSP SHALL document its justification, for each form of evidence it recognises and collects in fulfilling its CrP and these criteria, of how the strength of validation of the evidence it collects satisfies the qualities identified in Table 5-2 [see worksheet 63A_T5-2].*	✓	✓		
4.4.1.3 (IAL2)		Validation Requirements	Training requirements for personnel validating evidence SHALL be based on the policies, guidelines, or requirements of the CSP or RP.	✓				63A#0220			*The CSP SHALL document its policies, guidelines, and requirements for the training of personnel validating evidence*	✓	✓		
4.4.1.4 (IAL2)	1	Verification Requirements	At a minimum, the applicant's binding to identity evidence must be verified by a process that is able to achieve a strength of STRONG.	✓				63A#0230			*The CSP SHALL, at a minimum, verify the Applicant's binding to the identity evidence at a strength of STRONG;*	✓			
4.4.1.4 (IAL2)	2	Verification Requirements	Knowledge-based verification (KBV) SHALL NOT be used for in-person (physical or supervised remote) identity verification.	✓				63A#0240			*Knowledge-based verification (KBV) SHALL NOT be used for Supervised (In-person or Remote) identity verification.*	✓			
4.4.1.4 (IAL2)		Verification Requirements		✓				63A#0250			*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 verification of the evidence it collects meets, at a minimum, the STRONG qualities identified in Table 5-3 [see worksheet 63A_T5-3].*	✓			
4.4.1.5 (IAL2)		Presence Requirement	The CSP SHALL support in-person or remote identity proofing. The CSP SHOULD offer both in-person and remote proofing.	✓				63A#0260			*The CSP SHALL offer at least one of the following types of identity proofing and SHALL clearly state in its CrP which of those types it provides, describing clearly how requirements between multiple*	✓			Cf. 63A#0380 for IAL3
4.4.1.5 (IAL2)		Presence Requirement		✓				63A#0260	a)		*Supervised (In-person);*	✓			
4.4.1.5 (IAL2)		Presence Requirement		✓				63A#0260	b)		*Supervised (Remote);*	✓			
4.4.1.5 (IAL2)		Presence Requirement		✓				63A#0260	c)		*Unsupervised.*	✓			
4.4.1.6 (IAL2)	2	Address Confirmation	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.	✓				63A#0270			*The CSP SHALL validate and confirm the Applicant's address of record by relying only upon issuing source(s) or authoritative source(s).*	✓	✓		
4.4.1.6 (IAL2)	3	Address Confirmation	Self-asserted address data that has not been confirmed in records SHALL NOT be used for confirmation.	✓				63A#0280			*The CSP SHALL NOT accept un-validated self-asserted addresses.*	✓	✓		
4.4.1.6 (IAL2)	4	Address Confirmation	If CSP performs in-person proofing (physical or supervised remote):	✓				63A#0290			*If the CSP performs Supervised (In-person or Remote) proofing it SHALL document the maximum validities it allows for enrollment codes and only issue codes that meet that limitation, which SHALL NOT exceed 7 days.*	✓	✓		
4.4.1.6 (IAL2)	5	Address Confirmation	If the CSP performs remote proofing (unsupervised):	✓				63A#0300			*If the CSP performs Unsupervised proofing it SHALL:*	✓			
4.4.1.6 (IAL2)	5	Address Confirmation	The CSP SHALL send an enrollment code to a confirmed address of record for the applicant.	✓				63A#0300	a)		*send an enrollment code to a confirmed address of record for the Applicant;*	✓			

NIST SP 800-63A (rev.3) SAC & SoCA v4.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				IAL		CRITERION APPLICABILITY (SoCA)	Guidance
4.4.1.6 (IAL2)	5	Address Confirmation	The applicant SHALL present a valid enrollment code to complete the identity proofing process.	✓				63A#0300	b)		*require the Applicant to present a valid enrollment code to complete the identity proofing process;*	✓			
4.4.1.6 (IAL2)	5	Address Confirmation	If the enrollment code is also intended to be an authentication factor, it SHALL be reset upon first use.	✓				63A#0300	c)		*If the enrollment code is also intended to be an authentication factor, reset the code upon first use;*	✓			
4.4.1.6 (IAL2)	5	Address Confirmation	Enrollment codes SHALL have the following maximum validities:	✓				63A#0300	d)		*document the maximum validities it allows for enrollment codes and only issue codes that meet the following limitations:*	✓			
4.4.1.6 (IAL2)	5	Address Confirmation	10 days when sent to a postal address of record within the contiguous United States;	✓				63A#0300	d)	i)	*10 days, when sent to a postal address of record within the contiguous United States;*	✓			
4.4.1.6 (IAL2)	5	Address Confirmation	30 days when sent to a postal address of record outside the contiguous United States;	✓				63A#0300	d)	ii)	*30 days, when sent to a postal address of record outside the contiguous United States;*	✓			
4.4.1.6 (IAL2)	5	Address Confirmation	10 minutes when sent to a telephone of record (SMS or voice);	✓				63A#0300	d)	iii)	*10 minutes, when sent to a telephone number of record (SMS or voice);*	✓			
4.4.1.6 (IAL2)	5	Address Confirmation	24 hours when sent to an email address of record.	✓				63A#0300	d)	iv)	*24 hours, when sent to an email address of record.*	✓			
4.4.1.6 (IAL2)	5	Address Confirmation	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	✓				63A#0300	e)		*ensure that the enrollment code and notification of proofing are sent to different addresses of record.*	✓			
4.4.1.8 (IAL2)		Security Controls	The CSP SHALL employ appropriately tailored security controls, to include control enhancements, from the moderate or high baseline of security controls defined in SP 800-53 or equivalent federal (e.g., FEDRAMP) or industry standard.	✓				63A#0310			*The CSP SHALL employ appropriately-tailored security controls, to include control enhancements, from the moderate or high baseline of security controls, as defined in SP 800-53 or equivalent federal (e.g., FEDRAMP) or industry standards.*	✓			
4.4.1.8 (IAL2)		Security Controls	The CSP SHALL ensure that the minimum assurance-related controls for moderate-impact systems or equivalent are satisfied.	✓				63A#0320			When fulfilling criterion 63A#0310 the CSP SHALL ensure that the minimum assurance-related controls for moderate-impact systems or equivalent are satisfied.	✓			
4.4.2		IAL2 Trusted Referee proofing requirements	In instances where an individual cannot meet the identity evidence requirements specified in Section 4.4.1, the agency MAY use a trusted referee to assist in identity proofing the applicant. See Section 5.3.4 for more details.	✓				63A#0330			*CSPs SHALL identity-proof Trusted Referees according to the same criteria and , as a minimum, at the same IAL that are applied to normal Applicants on whose behalf they act.*	✓	✓		
4.5.1 (IAL3)		Resolution Requirements	Collection of PII SHALL be limited to the minimum necessary to resolve to a unique identity record. This MAY include the collection of attributes that assist in data queries. See Section 5.1 for general resolution requirements.	✓				63A#0340			***The CSP SHALL limit collection of PII to the minimum necessary to validate and resolve the existence of the claimed identity uniquely in a given context, and to associate the claimed identity with the Applicant providing identity evidence for appropriate identity resolution, validation, and verification. (See 63A#0020)***		✓		
4.5.2 (IAL3)		Evidence Collection Requirements	The CSP SHALL collect the following from the applicant:	✓				63A#0350			***The CSP SHALL collect from the Applicant at least the following strength of evidence, as determined by the further requirements in Table 5-1:***		✓		
4.5.2 (IAL3)	1		Two pieces of SUPERIOR evidence; OR	✓				63A#0350	a)		***Two pieces of SUPERIOR evidence; OR***		✓		

NIST SP 800-63A (rev.3) SAC & SoCA v4.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				IAL		CRITERION APPLICABILITY (SoCA)	Guidance
4.5.2 (IAL3)	2		One piece of SUPERIOR evidence and one piece of STRONG evidence if the issuing source of the STRONG evidence, during its identity proofing event, confirmed the claimed identity by collecting two or more forms of SUPERIOR or STRONG evidence and the CSP validates the evidence directly with the issuing source; OR	✓				63A#0350	b)		***One piece of SUPERIOR evidence and one piece of STRONG evidence IF the STRONG 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***		✓		
4.5.2 (IAL3)	3		Two pieces of STRONG evidence plus one piece of FAIR evidence.	✓				63A#0350	c)		***Two pieces of STRONG evidence plus one piece of FAIR evidence.***		✓		
4.5.2 (IAL3)			See Section 5.2.1 Identity Evidence Quality Requirements for more information on acceptable identity evidence	✓				63A#0355			***Refer to Worksheet 63A_T5-1 as applicable for IAL3***		✓		
4.5.3 (IAL3)		Validation Requirements	The CSP SHALL validate identity evidence as follows: Each piece of evidence must be validated with a process that is able to achieve the	✓				63A#0360			***The CSP SHALL, at a minimum, validate identity evidence at the same strength as that at which the evidence was collected. (see 63A#0200 & #0210)***		✓		
4.5.3 (IAL3)			See Section 5.2.2 Validating Identity Evidence for more information on validating identity evidence.	✓				63A#0365			***Refer to Worksheet 63A_T5-2 as applicable for IAL3***		✓		
4.5.4 (IAL3)	1		At a minimum, the applicant's binding to identity evidence must be verified by a process that is able to achieve a strength of SUPERIOR.	✓				63A#0370			***The CSP SHALL verify the Applicant's binding to the identity evidence by a process which demonstrates a strength of SUPERIOR.[Inc. ref to T5-3]***		✓		
4.5.5 (IAL3)		Presence Requirements	The CSP SHALL perform all identity proofing steps with the applicant in-person	✓				63A#0380			***The CSP SHALL perform all identity proofing using either Supervised (In-person) or Supervised (Remote)***		✓		Cf. 63A#0260 for IAL2
4.5.6 (IAL3)	1	Address Confirmation	The CSP SHALL confirm address of record. The CSP SHOULD confirm address of record through validation of the address contained on any supplied, valid piece of identity evidence. The CSP MAY confirm address of record by validating information supplied by the applicant, not contained on any supplied, valid piece of identity evidence.	✓				63A#0390			***The CSP SHALL confirm the Applicant's address of record using either:***		✓		Refer to SP 800-63A rev.3, §4.6, 1st para, as guidance
4.5.6 (IAL3)				✓				63A#0390	a)		***only information taken from any piece of valid identity evidence; or***		✓		
4.5.6 (IAL3)				✓				63A#0390	b)		***for information values which might reasonably be amended from time-to-time, information substituted by the Applicant which SHALL be validated with the issuing source of the information.***		✓		Information substituted may only be of the same type of class, e.g. a revised address or change of name for the same issuing source.
4.5.6 (IAL3)	3		A notification of proofing SHALL be sent to the confirmed address of record.	✓				63A#0400			***The CSP SHALL send a notification of proofing outcome to the confirmed address of record.***		✓		
4.5.6 (IAL3)			The enrollment code SHALL be valid for a maximum of 7 days.	✓				63A#0410			*Superseded by 63A#0290*				
4.5.7 (IAL3)		Biometric Collection	The CSP SHALL collect and record a biometric sample at the time of proofing (e.g., facial image, fingerprints) for the purposes of non-repudiation and re-proofing.	✓				63A#0420			***The CSP SHALL collect and record a biometric sample at the time of proofing.***		✓		The fundamental reason recording the biometric data is for the purposes of non-repudiation and re-proofing.
4.5.8 (IAL3)		Security Controls	The CSP SHALL employ appropriately tailored security controls, to include control enhancements, from the high baseline of security controls defined in SP 800-53 or an equivalent federal (e.g., FEDRAMP) or industry standard.	✓				63A#0430			***The CSP SHALL employ appropriately-tailored security controls, to include control enhancements, from the high baseline of security controls defined in SP 800-53 or equivalent federal (e.g., FEDRAMP) or industry standards. (see 63A#0310)***		✓		
4.5.8 (IAL3)		Security Controls	The CSP SHALL ensure that the minimum assurance-related controls for high-impact systems or equivalent are satisfied.	✓				63A#0440			***When fulfilling criterion 63A#0430 the CSP SHALL ensure that the minimum assurance-related controls for high-impact systems or equivalent are satisfied.***		✓		

NIST SP 800-63A (rev.3) SAC & SoCA v4.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				IAL		CRITERION APPLICABILITY (SoCA)	Guidance
4.6		Enrollment Code	An enrollment code SHALL be comprised of one of the following:	✓				63A#0450			*The CSP SHALL only issue enrollment codes that are, minimally, a random six character alphanumeric sequence or other value of equivalent entropy, represented either as:*	✓	✓		
4.6	1	Enrollment Code	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.	✓				63A#0450	a)		*a human-readable text string; OR*	✓	✓		
4.6	2	Enrollment Code	A machine-readable optical label, such as a QR Code, that contains data of similar or higher entropy as a random six character alphanumeric.	✓				63A#0450	b)		*A machine-readable optical label.*	✓	✓		
5.3.1			The CSP SHALL adhere to the requirements in Section 5.3.2 if KBV is used to verify an identity.	✓				63A#0460			*If the CSP uses KBV to verify identities it SHALL observe the practices required by 63A#0470 and 63A#0480.*	✓			
5.3.2	3	Knowledge-Based Verification Requirements	The CSP SHALL allow a resolved and validated identity to opt out of KBV and leverage another process for verification. *THIS SOURCE CLAUSE HAS BEEN DELIBERATELY REPOSITIONED SINCE IT DOES NOT 'FLOW' WITH THE OTHER REQUIREMENTS IN THIS SECTION*	✓				63A#0470			*If the CSP uses KBV to verify identities it SHALL allow the Applicant the choice to opt-out of the KBV process and SHALL employ other means of equivalent rigour to achieve verification (in accordance with T5-3).*	✓			
5.3.2	1	Knowledge-Based Verification Requirements	The CSP SHALL NOT use KBV to verify an applicant's identity against more than one piece of validated identity evidence.	✓				63A#0480			*The CSP SHALL verify an Applicant's identity against only a single piece of validated evidence, in accordance with the following restrictions:*	✓			
5.3.2	2	Knowledge-Based Verification Requirements	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	✓				63A#0480	a)		*information used to formulate KBQ/KBA SHALL be expected to be known only to the Applicant and the authoritative source;*	✓			*Guidance: Conversely, information used to formulate KBQ/KBA SHALL NOT be readily accessible from public or black market sources;*
5.3.2	4	Knowledge-Based Verification Requirements	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.	✓				63A#0480	b)		*KBQ/KBA SHALL be composed so as to ensure that the information transacted has at least 20 bits of entropy;*	✓			
5.3.2	5	Knowledge-Based Verification Requirements	The CSP SHALL require a minimum of four KBV questions with each requiring a correct answer to successfully complete the KBV step.	✓				63A#0480	c)		*a minimum of four KBQ SHALL be presented and each question SHALL*	✓			
5.3.2	5	Knowledge-Based Verification	The CSP SHOULD require free-form response KBV questions. The CSP MAY	✓				63A#0480	c)	i)	*have a minimum of four possible answers of which only one SHALL be correct; OR*	✓			
5.3.2	5	Knowledge-Based Verification Requirements	… however, if multiple choice questions are provided, the CSP SHALL require a minimum of four answer options per question.	✓				63A#0480	c)	ii)	*require responses which are not based on a selection from a pre-determined list.*	✓			
5.3.2	5	Knowledge-Based Verification Requirements	A CSP SHALL NOT allow more than three attempts to complete the KBV.	✓				63A#0480	d)		*a maximum of three attemps to answer each question SHALL be permitted;*	✓			
5.3.2	5	Knowledge-Based Verification Requirements	The CSP SHALL time out KBV sessions after two minutes of inactivity per question.	✓				63A#0480	e)		*the KBV session SHALL terminate if no attempt has been made to submit a response to a question within 2 minutes;*	✓			

NIST SP 800-63A (rev.3) SAC & SoCA v4.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				IAL		CRITERION APPLICABILITY (SoCA)	Guidance
5.3.2	5	Knowledge-Based Verification Requirements	In cases of session timeout, the CSP SHALL restart the entire KBV process and consider this a failed attempt.	✓				63A#0480	f)		*termination of a session SHALL require a complete re-start of the KBV process;*	✓			
5.3.2	5	Knowledge-Based Verification Requirements	The CSP SHALL NOT present a majority of diversionary KBV questions (i.e., those where "none of the above" is the correct answer).	✓				63A#0480	g)		*the presence of 'diversionary' questions in the set of possible responses SHALL be minimised;*	✓			
5.3.2	5	Knowledge-Based Verification Requirements	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.	✓				63A#0480	h)		*no question SHALL provide the Applicant the opportunity to infer answers to any other KBQs in any subsequent session;*	✓			
5.3.2	5	Knowledge-Based Verification Requirements	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	✓				63A#0480	i)		*no question SHALL offer the Applicant the opportunity to infer answers to any other KBQs;*	✓			
5.3.2	5	Knowledge-Based Verification Requirements	The CSP SHALL NOT use KBV questions for which the answers do not change (e.g., "What was your first car?").	✓				63A#0480	j)		*KBQ/KBA SHALL be composed] dynamically and NOT use KBQ for which the answer is in any way static.*	✓			
5.3.3.1	1	General Requirements	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.	✓				63A#0490			*If the CSP provides Supervised (In-person) proofing it SHALL document and apply technologies and procedures which ensure that the Proofing Supervisor reviews the biometric source (e.g., fingers, face) for presence of non-natural materials and perform such inspections as part of the proofing process.*	✓	✓		
5.3.3.1	2	General Requirements	The CSP SHALL collect biometrics in such a way that ensures that the biometric is collected from the applicant, and not another subject.	✓				63A#0500			*If the CSP provides Supervised (In-person) proofing it SHALL document and apply technologies and procedures such that the Proofing Supervisor SHALL ensure that biometric samples are taken from the Applicant themselves and not from another person.*	✓	✓		See CO#0290 for general training reqts
5.3.3.1	2	General Requirements	All biometric performance requirements in SP 800-63B, Section 5.2.3 apply.	✓				63A#0510			*If the CSP provides Supervised (In-person) proofing it SHALL ensure that the technologies and procedures applied by the Proofing Supervisor fulfill the biometric performance requirements expressed in 63A#0620 to 63A#0680 inclusive.*	✓	✓		
5.3.3.2	1	Requirements for Supervised Remote In-Person Proofing	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.	✓				63A#0520			*The CSP SHALL supervise the entirety of a Remote proofing session, from which the Applicant SHALL NOT depart.*	✓	✓		
5.3.3.2	2	Requirements for Supervised Remote In-Person Proofing	The CSP SHALL have a live operator participate remotely with the applicant for the entirety of the identity proofing session.	✓				63A#0530			*The CSP SHALL ensure that a live operator participates with the Applicant for the entirety of a Remote identity proofing session.*	✓	✓		
5.3.3.2	3	Requirements for Supervised Remote In-Person Proofing	The CSP SHALL require all actions taken by the applicant during the identity proofing session to be clearly visible to the remote operator.	✓				63A#0540			*The CSP SHALL ensure that a live operator clearly witnesses all actions taken by the Applicant, for the entirety of a Remote identity proofing session.*	✓	✓		
5.3.3.2	4	Requirements for Supervised Remote In-Person Proofing	The CSP SHALL require that all digital verification of evidence (e.g., via chip or wireless technologies) be performed by integrated scanners and sensors.	✓				63A#0550			*The CSP SHALL ensure that all digital verification of evidence is performed by scanners and sensors which are integrated into the CSP-owned/managed Remote proofing terminal.*	✓	✓		integrated meaning that the scanners/sensors are physically integrated within the remote terminal
5.3.3.2	5	Requirements for Supervised Remote In-Person Proofing	The CSP SHALL require operators to have undergone a training program to ...	✓				63A#0560			*The CSP SHALL train its live operators such that they:*	✓	✓		
5.3.3.2			... detect potential fraud and ...	✓				63A#0560	a)		*are competent to detect potential fraud; and*	✓	✓		
5.3.3.2			... to properly perform a virtual in-process proofing session.	✓				63A#0560	b)		*are capable of properly performing a virtual in-process proofing session.*	✓	✓		

NIST SP 800-63A (rev.3) SAC & SoCA v4.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				IAL		CRITERION APPLICABILITY (SoCA)	Guidance
5.3.3.2	6	Requirements for Supervised Remote In-Person Proofing	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.	✓				63A#0570			*The CSP SHALL employ physical tamper detection and resistance features at its Remote proofing terminal appropriate for the environment in which it is located.*	✓	✓		
5.3.3.2	7	Requirements for Supervised Remote In-Person Proofing	The CSP SHALL ensure that all communications occur over a mutually authenticated protected channel.	✓				63A#0580			*The CSP SHALL ensure that all communications between the live operator and the remote proofing terminal occur over mutually authenticated protected channels.*	✓	✓		There might be multiple 'channels' or a channel singular, independently of the logical / physical routing it may take.
5.3.4	2	Trusted Referee Requirements	The CSP SHALL establish written policy and procedures as to ...	✓				63A#0590			*The CSP SHALL include in its CrP the following:*	✓	✓		
5.3.4	2	Trusted Referee Requirements	... how a trusted referee is determined and ...	✓				63A#0590	a)		*how a Trusted Referee is determined;*	✓	✓		
5.3.4	2	Trusted Referee Requirements	... the lifecycle by which the trusted referee retains their status as a valid referee, ...	✓				63A#0590	b)		*the lifecycle by which the Trusted Referee retains their status as a valid referee;*	✓	✓		
5.3.4	2	Trusted Referee Requirements	... to include any restrictions, as well as any revocation and suspension requirements.	✓				63A#0590	c)		*any restrictions, as well as any revocation and suspension requirements, which are applicable to Trusted Referees;*	✓	✓		
5.3.4			In addition, the CSP SHALL determine the minimum evidence required to bind the relationship between the trusted referee and the applicant.	✓				63A#0600	d)		*the minimum evidence required to bind the relationship between the Trusted Referee and the Applicant.*	✓	✓		
5.3.4.1	1	Additional Requirements for Minors	... the legal restrictions of interacting with minors unable to meet the evidence requirements of identity proofing to ensure compliance with the Children's Online Privacy Protection Act of 1998 (COPPA) [COPPA], and other laws, as applicable.	✓				63A#0610			*The CSP SHALL document and apply policies and practices which show that it identifies and complies with all applicable laws and regulations, concerning interacting with minors unable to meet the evidence requirements of identity proofing .*	✓	✓		
								Referenced 63B_SAC criteria - NOTE - the following criteria are required to be met in the context of 63A#0510 and evidence for that purpose may differ from evidence to meet these criteria under AAL2 / 63B or under 63A Table 5-3. They are therefore replicated here under 63A and have been given discrete '63A#' tags to indicate their discrete 63A applicability. Where, for the purposes of applicability to 63A, any criterion is not intended to be observed it is marked 'No stipulation'. If responses to these criteria are different when responding to T5-3 requirements these criteria should be replicated within that worksheet.							
5.2.3		Use of Biometrics	The biometric system SHALL ...	✓				63A#0620			*The CSP shall implement biometric systems which have at least the following characteristics:*	✓	✓		
5.2.3		Use of Biometrics	... operate with an FMR [ISO/IEC 2382-37] of 1 in 1000 or better.	✓				63A#0620	a)		*operate with an FMR [ISO/IEC 2382-37] of 1 in 1000 or better;*	✓	✓		
5.2.3		Use of Biometrics	This FMR SHALL be achieved under conditions of a conformant attack (i.e., zero-effort impostor attempt) as defined	✓				63A#0620	b)		*achieved that FMR operation under conditions of a conformant attack (i.e., zero-effort impostor attempt) in accordance with ISO/IEC 30107-1.*	✓	✓		
5.2.3		Use of Biometrics	Testing of presentation attack resistance SHALL be in accordance with Clause 12 of ISO/IEC 30107-3.	✓				63A#0630			*If Presentation Attack Detection is implemented the CSP SHALL perform testing of presentation attack resistance in accordance with §12 of ISO/IEC 30107-3.*	✓	✓		
5.2.3		Use of Biometrics	The biometric system SHALL allow no more than 5 consecutive failed authentication attempts or 10 consecutive failed attempts if PAD meeting the above requirements is implemented.	✓				63A#0640				✓	✓		

NIST SP 800-63A (rev.3) SAC & SoCA v4.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				IAL		CRITERION APPLICABILITY (SoCA)	Guidance
5.2.3				✓				63A#0640	a)		*where analysis has shown at least 90% resistance to presentation attacks for each relevant attack type (i.e., species), where resistance is defined as the number of thwarted presentation attacks divided by the number of trial presentation attacks, THEN up to 10 consecutive failed authentication attempts can occur; OTHERWISE*	✓	✓		
5.2.3				✓				63A#0640	b)		*no more than 5 consecutive failed authentication attempts can occur.*	✓	✓		
5.2.3		Use of Biometrics	Once that limit has been reached, the biometric authenticator SHALL either:	✓				63A#0650			*If either limit set in 63A#0640 is reached the CSP SHALL:*	✓	✓		
5.2.3		Use of Biometrics	· Impose a delay of at least 30 seconds before the next attempt, increasing exponentially with each successive attempt (e.g., 1 minute before the following failed	✓				63A#0650	a)		*disable the biometric user authentication, and if an alternative authentication factor is already available use that other factor; OR OTHERWISE*	✓	✓		
5.2.3		Use of Biometrics	· Disable the biometric user authentication and offer another factor (e.g., a different biometric modality or a PIN/Passcode if it is not already a required factor) if such an alternative method is already available.	✓				63A#0650	b)		*impose a delay of at least 30 seconds before the next attempt, increasing exponentially with each successive attempt.*	✓	✓		
5.2.3		Use of Biometrics	The verifier SHALL make a determination of sensor and endpoint performance, integrity, and authenticity.	✓				63A#0660			*No stipulation - not applicable to identity proofing.*	✓	✓		
5.2.3		Use of Biometrics	If comparison is performed centrally:	✓				63A#0670			*If biometric comparisom is performed centrally rather than locally the CSP SHALL:*	✓	✓		
5.2.3		Use of Biometrics	· Use of the biometric as an authentication factor SHALL be limited to one or more specific devices that are	✓				63A#0670	a)		*limit use of the biometric as an authentication factor to one or more specific devices that are authenticated using approved cryptography;*	✓	✓		
5.2.3		Use of Biometrics	Since the biometric has not yet unlocked the main authentication key, a separate key SHALL be used for identifying the device	✓				63A#0670	b)		*use a separate key to identify the device;*	✓	✓		
5.2.3		Use of Biometrics	· Biometric revocation, referred to as biometric template protection in ISO/IEC 24745, SHALL be implemented.	✓				63A#0670	c)		*implement biometric revocation (a.k.a. biometric template protection);* Note - this is for both revocation of the credential as much as for privacy protection	✓	✓		
5.2.3		Use of Biometrics	· All transmission of biometrics SHALL be over the authenticated protected channel.	✓				63A#0670	d)		*transmit all biometric data over an authenticated protected channel.*	✓	✓		
5.2.3		Use of Biometrics	Biometric samples and any biometric data derived from the biometric sample such as a probe produced through signal processing SHALL be zeroized immediately after any training or research data has been derived.	✓				63A#0680			*The CSP SHALL zeroize the biometric sample (including any associated biometric data) immediately after any training or research data has been derived.*	✓	✓		

NIST SP 800-63A Table 5-1 Strengths of Identity Evidence				
Strength	***63A tag***	***indx***		***KI_criterion***
FAIR	*63A-T5-1#fair*	*a)*		*The CSP can demonstrate or show other reasonable expectation that the Issuing Source of the evidence:*
	63A-T5-1#fair	*a)*	*i)*	*confirmed the claimed identity through an identity proofing process;*
	63A-T5-1#fair	*a)*	*ii)*	*delivered the evidence into the possession of the person to whom it relates.*
	63A-T5-1#fair	*b)*		*The evidence collected by the CSP:*
	63A-T5-1#fair	*b)*	*i)*	*Contains at least one reference number that uniquely identifies the person to whom it relates;* ***OR***
	63A-T5-1#fair	*b)*	*ii)*	*Contains a photograph or biometric template (any modality) of the person to whom it relates;* ***OR***
	63A-T5-1#fair	*b)*	*iii)*	*Can have ownership confirmed through KBV.*
	63A-T5-1#fair	*c)*		*Where the evidence collected by the CSP includes digital information, that information is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the claimed issuing source to be confirmed.*
	63A-T5-1#fair	*d)*		*Where the evidence collected by the CSP includes physical security features, it requires proprietary knowledge to be able to reproduce those features.*
	63A-T5-1#fair	*e)*		*The evidence collected by the CSP is unexpired.*
STRONG	*63A-T5-1#strg*	*a)*		*The CSP can demonstrate or show other reasonable expectation that the Issuing Source of the evidence:*

NIST SP 800-63A Table 5-1 Strengths of Identity Evidence				
Strength	***63A tag***	***indx***		***KI_criterion***
	63A-T5-1#strg a)	*a)*	*i)*	*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 Applicant.*
	63A-T5-1#strg a)	*a)*	*ii)*	*has its written procedures subjected to recurring oversight by regulatory or publicly-accountable institutions;*
	63A-T5-1#strg a)	*a)*	*iii)*	*delivered the evidence into the possession of the subject to whom it relates.*
	63A-T5-1#strg b)	*b)*		*The evidence collected by the CSP contains at least one reference number that uniquely identifies the person to whom it relates and to the Issuing Source.*
	63A-T5-1#strg c)	*c)*		*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.*
	63A-T5-1#strg d)	*d)*		*Either the:*
	63A-T5-1#strg d)	*d)*	*i)*	*evidence collected by the CSP contains a photograph or biometric template (of any modality) of the person to whom it relates,* ***OR***
	63A-T5-1#strg d)	*d)*	*ii)*	*Applicant proves possession of an AAL2 authenticator bound to an IAL2 identity, at a minimum.*
	63A-T5-1#strg e)	*e)*		*Where the evidence collected by the CSP includes digital information, that information is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the claimed issuing source to be confirmed.*

NIST SP 800-63A Table 5-1 Strengths of Identity Evidence				
Strength	***63A tag***	***indx***		***KI_criterion***
	63A-T5-1#strg	*f)*		*Where the evidence collected by the CSP contains physical security features, it requires proprietary knowledge and proprietary technologies to be able to reproduce it.*
	63A-T5-1#strg	*g)*		*The evidence collected by the CSP is unexpired.*
SUPERIOR	*63A-T5-1#supr*	*a)*		*It can be demonstrated that the issuing source of the evidence:*
		a)	*i)*	*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 applicant;*
		a)	*ii)*	*has its written procedures subjected to recurring oversight by regulatory or publicly-accountable institutions;*
		a)	*iii)*	*visually identified the applicant and performed further checks to confirm the existence of that person;*
		b)		*employed processes which ensured that the evidence was delivered into the possession of the person to whom it relates.*
		c)		*The evidence collected by the CSP contains at least one reference number that uniquely identifies the person to whom it relates and to the issuing source.*
		d)		*The full name on the evidence collected by the CSP is 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.*
		e)		*The evidence collected by the CSP contains a photograph of the person to whom it relates.*
		f)		*The evidence collected by the CSP contains a biometric template (of any modality) of the person to whom it relates.*

NIST SP 800-63A Table 5-1 Strengths of Identity Evidence			
Strength	***63A tag***	***indx***	***KI_criterion***
		g)	*The evidence collected by the CSP includes digital information, the information is protected using approved cryptographic or proprietary methods, or both, and those methods ensure the integrity of the information and enable the authenticity of the issuing source to be confirmed.*
		h)	*The evidence collected by the CSP includes physical security features that require proprietary knowledge and proprietary technologies to be able to reproduce it.*
		i)	*The evidence collected by the CSP is unexpired.*

NIST SP 800-63A Table 5-2 Validating Identity Evidence				
Strength	***63A tag***	***indx***		***KI_criterion***
FAIR	*63A-T5-2#fair*	*a)*		*The CSP can demonstrate that the evidence which it has collected:*
	63A-T5-2#fair	*a)*	*i)*	*has attributes confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s); OR*
	63A-T5-2#fair	*a)*	*ii)*	*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*
	63A-T5-2#fair	*a)*	*iii)*	*has been confirmed as genuine by trained personnel; OR*
	63A-T5-2#fair	*a)*	*iv)*	*has been confirmed as genuine by confirmation of the integrity of cryptographic security features.*
STRONG	*63A-T5-2#strg*	*a)*		*The CSP can demonstrate that the evidence which it has collected has been confirmed as genuine:*
	63A-T5-2#strg	*a)*	*i)*	*using appropriate technologies, confirming the integrity of physical security features and that the evidence is not fraudulent or inappropriately modified; OR*
	63A-T5-2#strg	*a)*	*ii)*	*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*
	63A-T5-2#strg	*a)*	*iii)*	*by confirmation of the integrity of cryptographic security features.*
	63A-T5-2#strg	*b)*		*The CSP can demonstrate that the evidence which it has collected has had all personal details and evidence details confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s).*

NIST SP 800-63A Table 5-2 Validating Identity Evidence			
Strength	*63A tag*	*indx*	*KI_criterion*
SUPERIOR	*63A-T5-2#supr*	*a)*	*The CSP can demonstrate that the evidence which it has collected has been confirmed as genuine by trained personnel and the use of appropriate technologies, including the integrity of any physical and cryptographic security features;*
	63A-T5-2#supr	*b)*	*The CSP can demonstrate that the evidence which it has collected has had all personal details and evidence details confirmed as valid by comparison with information held or published by the issuing source or authoritative source(s).*

NIST SP 800-63A Table 5-3 Verifying Identity Evidence			
Strength	***63A tag***	***indx***	***KI_criterion***
FAIR Not applicable since 'FAIR' verification is not permissable at IAL2 (§4.4.1.4	*n/a* *n/a* *n/a* *n/a*		
STRONG	*63A-T5-3#strg* *63A-T5-3#strg* *63A-T5-3#strg*	*a)* *a) i)* *a) ii)*	*The CSP SHALL confirm the Applicant's ownership of the claimed identity by:* *a physical comparison of the applicant to the strongest piece of identity evidence provided to support the claimed identity. Physical comparison performed remotely SHALL adhere to all criteria 63A#0620 to 63A#0680 inclusive; OR* *biometric comparison of the applicant to the identity evidence. Biometric comparison performed remotely SHALL adhere to all criteria 63A#0620 to 63A#0680 inclusive.*
SUPERIOR	*63A-T5-3#supr*	*a)*	*The CSP SHALL confirm the Applicant's ownership of the claimed identity 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 criteria 63A#0620 to 63A#0680 inclusive.*

Tag cross-reference:

old 63A tag	*new 63A tag*
63A#0010	63A#0010
63A#0020	63A#0020
63A#0030	63A#0030
63A#0040	63A#0040
63A#0060	63A#0050
63A#0070	63A#0060
63A#0070	63A#0062
63A#0080	63A#0070
63A#0090	63A#0260
63A#0100	63A#0080
63A#0110	63A#0090
63A#0120	63A#0100
63A#0130	63A#0110
63A#0140	63A#0120
63A#0150	63A#0130
63A#0160	63A#0140
63A#0170	63A#0150
63A#0180	63A#0160
63A#0190	63A#0170
63A#0200	63A#0180
63A#0200	63A#0180
63A#0200	63A#0180
63A#0210	63A#0190
63A#0220	63A#0200
63A#0230	63A#0210
63A#0240	63A#0220
63A#0250	63A#0230
63A#0260	63A#0240
63A#0270	63A#0250

new 63A tag	*old 63A tag*
63A#0010	63A#0010
63A#0020	63A#0020
63A#0030	63A#0030
63A#0040	63A#0040
63A#0050	63A#0060
63A#0060	63A#0070
63A#0062	63A#0070
63A#0070	63A#0080
63A#0080	63A#0100
63A#0090	63A#0110
63A#0100	63A#0120
63A#0110	63A#0130
63A#0120	63A#0140
63A#0130	63A#0150
63A#0140	63A#0160
63A#0150	63A#0170
63A#0160	63A#0180
63A#0170	63A#0190
63A#0180	63A#0200
63A#0180	63A#0200
63A#0180	63A#0200
63A#0190	63A#0210
63A#0200	63A#0220
63A#0210	63A#0230
63A#0220	63A#0240
63A#0230	63A#0250
63A#0240	63A#0260
63A#0250	63A#0270
63A#0260	63A#0090

63A#0280	63A#0270
63A#0290	63A#0280
63A#0300	63A#0450
63A#0310	63A#0290
63A#0310	63A#0450
63A#0320	63A#0300
63A#0330	63A#0310
63A#0340	63A#0330
63A#0350	63A#0590
63A#0350	63A#0600
63A#0360	63A#0490
63A#0370	63A#0500
63A#0380	63A#0510
63A#0390	63A#0610
63A#2330	63A#0620
63A#2335	63A#0630
63A#2340	63A#0640
63A#2350	63A#0650
63A#2360	63A#0660
63A#2370	63A#0670
63A#2380	63A#0680
63A#3010	63A#0340
63A#3020	63A#0350
63A#3030	63A#0360
63A#3040	63A#0370
63A#3040	n/a
63A#3050	63A#0380
63A#3060	63A#0390
63A#3080	63A#0400
63A#3090	63A#0410
63A#3100	63A#0420
63A#3120	63A#0430

63A#0270	63A#0280
63A#0280	63A#0290
63A#0290	63A#0310
63A#0300	63A#0320
63A#0310	63A#0330
63A#0320	n/a
63A#0330	63A#0340
63A#0340	63A#3010
63A#0350	63A#3020
63A#0360	63A#3030
63A#0370	63A#3040
63A#0380	63A#3050
63A#0390	63A#3060
63A#0390	n/a
63A#0400	63A#3080
63A#0410	63A#3090
63A#0420	63A#3100
63A#0430	63A#3120
63A#0440	63A#3130
63A#0450	63A#0300
63A#0450	63A#0310
63A#0460	n/a
63A#0470	n/a
63A#0480	n/a
63A#0490	63A#0360
63A#0500	63A#0370
63A#0510	63A#0380
63A#0520	63A#3200
63A#0530	63A#3210
63A#0540	63A#3220
63A#0550	63A#3230
63A#0560	63A#3240

63A#3130	63A#0440
63A#3200	63A#0520
63A#3210	63A#0530
63A#3220	63A#0540
63A#3230	63A#0550
63A#3240	63A#0560
63A#3250	63A#0570
63A#3260	63A#0580
n/a	63A#0320
n/a	63A#0390
n/a	63A#0460
n/a	63A#0470
n/a	63A#0480
n/a	63A#0560

63A#0560	n/a
63A#0570	63A#3250
63A#0580	63A#3260
63A#0590	63A#0350
63A#0600	63A#0350
63A#0610	63A#0390
63A#0620	63A#2330
63A#0630	63A#2335
63A#0640	63A#2340
63A#0650	63A#2350
63A#0660	63A#2360
63A#0670	63A#2370
63A#0680	63A#2380
n/a	63A#3040