Title:	Identity Assurance Framework: NIST SP 800-63A Service Assessment Criteria
Document id:	KIAF-1430
Version:	2
Document type:	Recommendation
Publication Date:	pending
Effective Date:	Immediate on Publication
Status:	Final
Approval Authority:	IAWG
Editor:	R.G. Wilsher
Sponsor:	ID.me
IAWG Sub-group participants	Don CAMPBELL (MedAllies) Ken DAGG (Independent) Mark HAPNER (Resilient Networks) Ruth PUENTE (Kantara Initiative) Colin WALLIS (Kantara Initiative) Ken CROWL (Experian) Nathan FAUT (KPMG) Andrew HUGHES (Independent) Scott SHORTER (Kuma) Aakash YADAV (Okta)
IPR:	Patent and Copyright Option: Reciprocal Royalty Free with Opt-Out to Reasonable and Non-Discriminatory terms (RAND)
Abstract:	This document 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, 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, revision, etc.
Revision history:	v1.0 14/12/2017 For Public review v2.0 2018-02-15 Final - Released for application

Users' Guide

Structure of these criteria:

The criteria in this document relate to the requirements of NIST SP 800-63A at IAL2 exclusively. Principal criteria are in the worksheet '63A_SAC' and three tables from SP 800-63A are interpreted in Kantara terms in The original NIST criteria headings and text FOR NORMATIVE SECTIONS ONLY are available in columns A to H, giving the heading components of the applicable levels and then the actual text of the NIST clause. However, as downloaded from Kantara, columns B to H are hidden, so as to focus attention on the Kantara criteria. Kantara's criteria (i.e. the 63A_SAC) are set out in columns I to M, commencing with a unique tag in the form '63A#9999', possible sub-indexes following, and then the actual criteria in col. M. Criteria are generally Because there is not a Kantara criterion derived from each and every clause in the original NIST SP some rows in the criteria columns may not bear a criterion - in this case they are shaded and marked 'n/a', in an attempt The three worksheets which address Tables 5-1, 5-2 and 5-3 in SP 800-63A have a similar, but not precisely the same, layout which Users will readily recognize after working-through the 63A_SAC worksheet.

Use as a Statement of Conformity (SoC)

Users (principally Assessors and CSPs) are at liberty to adopt this document for their own use as an SoC, for use in applications to Kantara's ARB (ref KIAF-1340 'SAH') for initial Registration, to record findings etc during

PLEASE DO NOT:

i) alter the structure of any of the worksheets;
ii) insert any additional rows.

NIST	Kantara IAF 63A Services Assessment Criteria		
§(H1)	63A tag	indx	KI_criterion
4	63A#0010		The CSP SHALL NOT perform identity proofing to determine suitability or entitlement to gain access to services or benefits.
4	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	63A#0030		The CSP SHALL document and publish a Privacy Policy 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	63A#0040		The CSP SHALL explicitly make its Privacy Policy available to the applicant at the time of collection of the attributes necessary for the Applicant's identity proofing,
4	63A#0050		The CSP shall state in its Credential Policy (CrP) any legitimate 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.
4	63A#0060		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	63A#0060	a)	document and apply predictability and manageability measures associated with those additional processes based on the results of its privacy risk assessment; (see 63A#0180)

NIST	Kantara IAF 63A Services Assessment Criteria		
§(H1)	63A tag	indx	KI_criterion
4	n/a		
4	63A#0060	b)	NOT make consent to processing of these additional attributes a condition of provision of the service.
4	63A#0070		The CSP SHALL document and publish, in a manner which is easy for Applicants to find and use, its mechanisms for redress of Applicant complaints or problems arising from the identity proofing processes.
4	63A#0080		The CSP SHALL assess its redress mechanisms for their efficacy in achieving resolution of complaints or problems and implement corrective action when efficacy falls below defined thresholds of performance or accomplishment.
4	63A#0090		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 mutliple types differ. a) Supervised (In-person); b) Supervised (Remote); c) Unsupervised.
4	63A#0100		The CSP SHALL document and publish in a Credential Policy (CrP) its identity proofing and enrollment policy/ies.
4	63A#0110		The CSP SHALL document in its Credentialling Practice Statement (CrPS) the practices which it implements to fulfil its CrP intentions.
4	63A#0120		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.

NIST	Kantara IAF 63A Services Assessment Criteria		
§(H1)	63A tag	indx	KI_criterion
4	63A#0130		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.
4	63A#0140		The CSP SHALL conduct its risk management process at least annually and whenever there is a material change to its CrP, and SHALL include assessment of privacy and security risks, accounting for:
4	63A#0140	a)	Any steps that it will take to verify the identity of the applicant beyond any mandatory requirements specified herein;
4	63A#0140	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	63A#0140	c)	The CSP's Retention Schedule requirements for collected PII and associated records, accounting for applicable laws, regulations, contracts, and policies.
4	63A#0150		The CSP SHALL maintain a record, including audit logs, of:
4	63A#0150	a)	the type of identity proofing performed;
4	63A#0150	b)	the types of and a unique reference to identity evidence collected from the Applicant in the proofing process;
4	63A#0150	c)	PII or other responses collected from authoritative and/or issuing sources;
4	63A#0150	d)	all steps taken to validate the identity evidence;
4	63A#0150	e)	all steps taken to verify the identity of the applicant;
4	63A#0150	f)	the outcome of each step, culminating in the final proofing result.
4	63A#0160		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.

NIST	Kantara IAF 63A Services Assessment Criteria		
§(H1)	63A tag	indx	KI_criterion
4	63A#0170		The CSP shall use authenticated protected channels during the entire proofing transaction, including exchanges with third parties.
4	n/a		
4	63A#0180		IF the CSP uses fraud mitigation measures, it SHALL include these measures in its privacy risk assessment for these mitigation measures.
4	63A#0190		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.

NIST	Kantara IAF 63A Services Assessment Criteria		
§(H1)	63A tag	indx	KI_criterion
4	n/a		
4	n/a		
4	n/a		
4	n/a		
4	n/a		See 63A#0100 - the requirement that the CSP document their proofing policy allows them to express their choices in that document, and whether they choose one or both of these options, for whatever reason, will be shown therein.
4	n/a		
4	n/a		See 63A#0020

NIST	Kantara IAF 63A Services Assessment Criteria		
§(H1)	63A tag	indx	KI_criterion
4	63A#0200		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	63A#0200	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	63A#0200	b)	Two pieces of STRONG evidence; OR
4	63A#0200	c)	One piece of STRONG evidence plus two pieces of FAIR evidence.
4	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 the evidence it collects satisfies the qualities identified in Table 5 -1 [see worksheet 63A T5-1].
4	n/a		
4	n/a		
4	n/a		Refer to Worksheet 63A T5-1

NIST	Kantara IAF 63A Services Assessment Criteria		
§(H1)	63A tag	indx	KI_criterion
4	63A#0220		The CSP SHALL, at a minimum, validate identity evidence at the same strength as that at which the evidence was collected.
4	63A#0230		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	n/a		Refer to Worksheet 63A_T5-2
4	63A#0240		The CSP SHALL document its policies, guidelines, and requirements for the training of personnel validating evidence
4	n/a		
4	63A#0250		The CSP SHALL, at a minimum, verify the applicant's binding to the identity evidence at a strength of STRONG;
4	63A#0260		Knowledge-based verification (KBV) SHALL NOT be used for Supervised (In-person or Remote) identity verification.
4	63A#0270		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			Refer to Worksheet 63A_T5-3
4	n/a		
4	n/a		
4	n/a		

NIST	Kantara IAF 63A Services Assessment Criteria		
§(H1)	63A tag	indx	KI_criterion
4	63A#0290		The CSP SHALL validate and confirm the Applicant's address of record by relying only upon issuing source(s) or authoritative source(s).
4	63A#0300		The CSP SHALL NOT accept un-validated self-asserted addresses.
4	n/a		
4	n/a		
4	63A#0310		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	63A#0310	a)	a human-readable text string; OR
4	63A#0310	b)	A machine-readable optical label.
4	63A#0320		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	n/a		
4	n/a		
4	n/a		See 63A#0300
4	63A#0330		If the CSP performs Unsupervised proofing it SHALL:

NIST	Kantara IAF 63A Services Assessment Criteria		
§(H1)	63A tag	indx	KI_criterion
4	63A#0330	a)	send an enrollment code to a confirmed address of record for the Applicant;
4	63A#0330	b)	require the applicant to present a valid enrollment code to complete the identity proofing process;
4	n/a		
4	63A#0330	c)	If the enrollment code is also intended to be an authentication factor, reset the code upon first use;
4	63A#0330	d)	document the maximum validities it allows for enrollment codes and only issue codes that meet the following limitations:
4	63A#0330	d) i)	10 days, when sent to a postal address of record within the contiguous United States;
4	63A#0330	d) ii)	30 days, when sent to a postal address of record outside the contiguous United States;
4	63A#0330	d) iii)	10 minutes, when sent to a telephone number of record (SMS or voice);
4	63A#0330	d) iv)	24 hours, when sent to an email address of record.
4	63A#0330	e)	ensure that the enrollment code and notification of proofing are sent to different addresses of record.
4	n/a		

NIST	Kantara IAF 63A Services Assessment Criteria		
§(H1)	63A tag	indx	KI_criterion
4	n/a		
4	63A#0340		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			See 63A#0340
4	63A#0350		CSPs SHALL identity-proof Trusted Referees according to the same criteria and at the same IAL that are applied to normal Applicants on whose behalf they act.
5	n/a		
5	63A#0360		The CSP SHALL include in its CrP the following:
5	63A#0360	a)	how a Trusted Referee is determined;
5	63A#0360	b)	the lifecycle by which the Trusted Referee retains their status as a valid referee;
5	63A#0360	c)	any restrictions, as well as any revocation and suspension requirements, which are applicable to Trsuted Referees;
5	n/a		See 63A#0350

NIST	Kantara IAF 63A Services Assessment Criteria		
§(H1)	63A tag	indx	KI_criterion
5	63A#0360	d)	the minimum evidence required to bind the relationship between the trusted referee and the applicant;
5	n/a		
4	n/a		
4	n/a		
5	n/a		
5	n/a		
5	n/a		Refer to Worksheet 63A_T5-1
5	n/a		Refer to Worksheet 63A_T5-2

NIST	Kantara IAF 63A Services Assessment Criteria		
§(H1)	63A tag	indx	KI_criterion
5	n/a		Refer to Worksheet 63A_T5-3
5	63A#0370		n/a - not assigned
5	n/a		
5	n/a		
5	n/a		
5	n/a		
5	n/a		
5	n/a		
5	n/a		
5	n/a		
5	n/a		

NIST	Kantara IAF 63A Services Assessment Criteria		
§(H1)	63A tag	indx	KI_criterion
5	n/a		
5	n/a		
5	n/a		
5	n/a		
5	n/a		
5	n/a		
5	n/a		
5	n/a		
5	n/a		
5	n/a		
5	n/a		
5	n/a		
5	n/a		

NIST	Kantara IAF 63A Services Assessment Criteria		
§(H1)	63A tag	indx	KI_criterion
5	n/a		
5	n/a		
5	n/a		
5	n/a		
5	63A#0380		The CSP 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	63A#0390		The CSP SHALL document and apply technologies and procedures such that it can ensure that biometroic samples are taken from the applicant themselves and not another person
5	63A#0400		The CSP SHALL fulfill the biometric performance requirements expessed in 63B#1180 - 1260.
	n/a		
5	63A#0410		n/a - not assigned
5	n/a		

NIST	Kantara IAF 63A Services Assessment Criteria		
§(H1)	63A tag	indx	KI_criterion
5	n/a		
5	n/a		
5	n/a		
5	n/a		
5	n/a		
5	n/a		
5	n/a		
5			See 63A#0400
5	63A#0420		*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*
5			See 63A#0420

NIST	Kantara IAF 63A Services Assessment Criteria		
§(H1)	63A tag	indx	KI_criterion
5	n/a		
5	n/a		
	End of 63A criteria		

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:
	63A-T5-1#strg	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) ii)	has its written procedures subjected to recurring oversight by regulatory or publicly-accountable institutions;
	63A-T5-1#strg	a) iii)	delivered the evidence into the possession of the subject to whom it relates.
	63A-T5-1#strg	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.

NIST SP 800-63A Table 5-1 Strengths of Identity Evidence

Strength	63A tag	indx	KI_criterion
	63A-T5-1#strg	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)	*Either the:*
	63A-T5-1#strg	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) ii)	*Applicant proves possession of an AAL2 authenticator bound to an IAL2 identity, at a minimum.*
	63A-T5-1#strg	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.*
	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).
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 1))	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 63B#1180 to 63B#1260 inclusive; OR biometric comparison of the applicant to the identity evidence. Biometric comparison performed remotely SHALL adhere to all criteria 63B#1180 to 63B#1260 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 reqcriteria 63B#1180 to 63B#1260 inclusive.