Title:	Identity Assurance Framework: NIST SP 800-63B Service Assessment Criteria
Document id:	KIAF-1440
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 CROWL (Experian)
Ken DAGG (Independent)	Nathan FAUT (KPMG)
Mark HAPNER (Resilient Networks)	Andrew HUGHES (Independent)
Ruth PUENTE (Kantara Initiative)	Scott SHORTER (Kuma)
Colin WALLIS (Kantara Initiative)	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 800-63B as published 2017-12-01 (with errata) at AAL2, to be generally referred-to as the '63B_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 800-63B at AAL2 exclusively, and are
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 63B_SAC) are set out in columns I to M, commencing with a unique tag in the form '63B#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

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 63B Service Assessment Criteria		
§(H1)	63B tag	indx	KI_criterion
4	n/a		
4	63B#0010		The CSP SHALL authenticate a Claimant at at least the same AAL as the IAL at which the claimant was identity-proofed.
4	63B#0020		The CSP SHALL ensure that, for a given Subject and authenticator, the result of a successful authentication results in a consistent identifier.
4	n/a		
4	n/a		
	n/a		
4	n/a		
4	n/a		
4			
4			
4	63B#0030		The CSP SHALL perform authen tication using EITHER a multi-factor authenticator OR a combination of two single-factor authenticators.
4	63B#0040		When a multi-factor authenticator is used,the CSP SHALL employ at least one of the following:
4	63B#0040	a)	Multi-Factor OTP Device;
4	63B#0040	b)	Multi-Factor Cryptographic Software;
4	63B#0040	c)	Multi-Factor Cryptographic Device.
4	63B#0050		When a combination of two single-factor authenticators is used, the CSP SHALL employ a Memorized Secret authenticator plus one of the following possession-based authenticators:
4	63B#0050	a)	Look-Up Secret;
4	63B#0050	b)	Out-of-Band Device;
4	63B#0050	c)	Single-Factor OTP Device;
4	63B#0050	d)	Single-Factor Cryptographic Software;

NIST §(H1)	63B tag	indx	KI_criterion
	Kantara IAF 63B Service Assessment Criteria		
4	*63B#0050*	*e)*	*Single-Factor Cryptographic Device.*
4	*63B#0060*		*The CSP SHALL ensure that software cryptographic authenticators are validated against FIPS 140 Level 1.*
4	*n/a*		
4	*n/a*		
4	*63B#0070*		*The CSP SHALL ensure that at least one authenticator used is replay resistant.*
4	*n/a*		
4	*63B#0080*		*The CSP SHALL ensure that all communication between the Claimant and Verifier is via an authenticated protected channel, excepting the secondary channel in the case of an OOB authenticator.*
4	*n/a*		
4	*63B#0090*		*The CSP SHALL NOT consider the unlocking of a device used in the authentication process to be an authentication factor.* GUIDANCE - differentiate between unlocking as a passive function and activation as an intent to enable functionaility.
4	*n/a*		
4	*63B#0100*		*If a biometric factor is used in an authentication the CSP SHALL ensure that all criteria 63B#1180 to 63B#1260 are fulfilled.*
4	*n/a*		
4	*n/a*		
4	*n/a*		
4	*n/a*		

NIST	Kantara IAF 63B Service Assessment Criteria		
§(H1)	63B tag	indx	KI_criterion
7	63B#0110		The CSP SHALL issue a session secret at the time of initial verification of a User and SHALL maintain that session secret OR a refreshed replacement session secret for the duration of the session.
7	n/a		
7	n/a		
7	n/a		
7	63B#0120		The CSP SHALL NOT allow session secrets (whether one issued initially or one refreshed) to persist beyond the termination of a session.
4	63B#0130		The CSP SHALL time out sessions after a maximum of 30 minutes of inactivity.
7	n/a		See 63B#0130
4	63B#0140		The CSP SHALL re-authenticate the User at least once per 12 hours during an extended usage session, regardless of user activity.
7	n/a		See 63B#0140
7	63B#0150		Prior to terminating a session for reason of inactivity the CSP SHALL prompt the Subject for their memorized secret or biometric attribute to extend the re-authentication time limit.
4	63B#0160		The CSP SHALL terminate a session and the life of the current session secret whenever the Subject fails to present themselves for re-authentication prior to any timeout period.
7	63B#0170		The CSP SHALL require a new session to be started, with re-authentication of the Subject after any session termination (for whatever reason).
7	n/a		
	63B#0173		Unless the CSP is supporting a federation protocol which permits RPs to specify a acceptable authentication age then the CSP SHALL make no assumptions of correlation between its session with the Subscriber and those of any other party.

NIST §(H1)	Kantara IAF 63B Service Assessment Criteria 63B tag	indx	KI_criterion
	n/a		
7	*n/a*		
	63B#0176		*If the CSP is supporting a federation protocol which permits RPs to specify a maximum acceptable authentication age then the CSP SHALL modify its conformity to [tag above re 12 hrs] so as to:*
	63B#0176	*a)*	*re-authenticate the Subscriber within the RP-specified time period;*
	63B#0176	*b)*	*communicate the authentication event time to the RP;*
4	*63B#0180*		*The CSP SHALL employ appropriately-tailored moderate baseline 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.* GUIDANCE: Ref to SP 800-53 will show that assurance controls (per the original NIST 800-63B reqt) are a subset of the moderate sec ctrls.
4	*63B#0190*		*The CSP SHALL document, periodically review and comply with, a data retention schedule, accounting for*
	63B#0190	*a)*	*results of a privacy and security risk assessment;*
	63B#0190	*b)*	*applicable laws, regulations, and policies, including any NARA records retention schedules that may apply;*
	63B#0190	*c)*	*its own records retention policie.*
4	*n/a*		See 63B#0190 a)
4	*63B#0200*		*The CSP SHALL publish to Subjects its data retention schedule, to the extent appropriate to the context.*
4			
4	*63B#0210*		*The CSP SHALL employ appropriately-tailored privacy controls, to include control enhancements,for moderate-impact systems as defined in SP 800-53 or equivalent Federal (e.g., FEDRAMP) or industry standards.*

NIST §(H1)	63B tag	indx	KI_criterion
			Kantara IAF 63B Service Assessment Criteria
4	63B#0220		*Unless the Subject has agreed to additional use of their PII, the CSP SHALL NOT use or disclose Subjects' PII for any purpose other than conducting authentication, related fraud mitigation, or to comply with law or legal process.*
	63B#0230		*The CSP SHALL provide clear notice and obtain the Subject's consent for any additional uses of their PII, prior to making any such use.*
4	63B#0240		*The CSP SHALL NOT make consent a condition of the service.*
4	63B#0250		*The CSP SHALL ensure that use of PII is limited to the purposes for which it was collected, as stated in the Terms of Service / Privacy Policy (see 63A#0030) / CrP (see 63A#0100).*
4	n/a		
4	n/a		
4	n/a		
4	n/a		
4	n/a		
4	n/a		
4	n/a		
5	n/a		
5	n/a		
5	63B#0250		*The CSP SHALL require memorized secrets chosen by the Subject to be at least 8 characters in length.*
5	63B#0260		*The CSP SHALL require memorized secrets generated by itself or a Verifier to be at least 6 characters in length and randomly-generated.*

NIST §(H1)	63B tag	indx	KI_criterion
	Kantara IAF 63B Service Assessment Criteria		
5	*63B#0265*		*If the CSP [or Verifier] determines that a chosen memorized secret appears on a list of compromised values it SHALL require the Subject to choose a different memorized secret.*
5	*n/a*		
5	*63B#0270*		*The CSP SHALL require memorized secrets chosen by the Subject to be at least 8 characters in length.*
5	*n/a*		
5	*n/a*		
5	*63B#0273*		*The CSP SHALL NOT truncate Subject-chosen passwords*
5	*63B#0277*		*If Unicode is accepted then the CSP SHALL count each Unicode code point as a single character.*
5	*n/a*		
5	*n/a*		
5	*n/a*		
5	*63B#0280*		*The CSP SHALL require memorized secrets generated by itself or a Verifier to be at least 6 characters in length and randomly-generated using an approved random-bit generator [SP 800-90Ar1].*
5	*63B#0290*		*The CSP SHALL NOT permit Subjects to store password-recollection hints.*

NIST §(H1)	Kantara IAF 63B Service Assessment Criteria		
	63B tag	indx	KI_criterion
5	63B#0300		The CSP SHALL NOT prompt Subjects in any manner when Subjects are choosing secrets
5	63B#0310		The CSP SHALL compare Subjects' chosen secrets against a list that contains values known to be commonly-used, expected, or compromised and if found:
5	n/a		
5	n/a		
	63B#0310	a)	provide the reason for rejection;
	63B#0310	b)	require the Subject to choose another secret.
5	n/a		
5	n/a		
5	63B#0320		The Verifier SHALL implement a rate-limiting mechanism which:
5	63B#0320	a)	protects against online guessing attacks;

NIST §(H1)	63B tag	indx	KI_criterion
			Kantara IAF 63B Service Assessment Criteria
5	*63B#0320*	*b)*	*limits consecutive failed authentication attempts on a single account to no more than 100.*
5	*n/a*		
5	*63B#0340*		*IF there is evidence of compromise of the Claimants authenticator the CSP SHALL force the Claimant to select a new memorized secret, consistent with 63B#0270 - 63B#0310.*
5	*n/a*		
5	*n/a*		
5	*n/a*		
5	*63B#0350*		*The CSP SHALL use approved encryption and an authenticated protected channel when requesting memorized secrets.*
5	*63B#0360*		*The CSP SHALL store memorized secrets in a form that is resistant to offline attacks.*
5	*63B#0370*		*The CSP SHALL salt and hash stored memorized secrets using an approved algorithm, ensuring that:*
5	*n/a*		
5	*n/a*		*Though this list is not embodied within a criterion (because it is exemplar, not definitive), CSPs should be able to demonstrate that their choice is on a recognized 'approved' list.*
5	*n/a*		
5	*n/a*		

NIST §(H1)	Kantara IAF 63B Service Assessment Criteria		
	63B tag	indx	KI_criterion
5	n/a		
5	n/a		
5	n/a		
5	n/a		
5	n/a		
5	63B#0370	a)	a randomly-chosen salt value of at least 32 bits in length is used;
5	63B#0370	b)	both the salt value and the resulting hash are stored for each subscriber using a memorized secret authenticator;
5	n/a		
5	n/a		
5	n/a		
5	n/a		
5	n/a		
5	63B#0377		The CSP SHALL secret store separately salt value(s) and the hashed memorized secrets.
5	63B#0380		The CSP SHALL create lists of look-up secret authenticators using an approved random bit generator [SP 800-90Ar1] which creates secrets having at least 20 bits of entropy;
5	63B#0390		The CSP SHALL create lists of look-up secret authenticators using an approved random bit generator [SP 800-90Ar1].
5	n/a		
5	n/a		

NIST §(H1)	Kantara IAF 63B Service Assessment Criteria		
	63B tag	indx	KI_criterion
5	63B#0400		IF the CSP distributes lists of look-up secret authenticators it SHALL do so using a secure channel which meets the criteria defined in 63B#1330.
5	n/a		
5	63B#0410		The CSP SHALL prompt the Claimant for the next secret from their authenticator or for a specific (e.g., numbered) secret.
5	63B#0420		The CSP SHALL succesfully use a secret from an authenticator list only once.
5	63B#0430		IF a look-up secret is derived from a grid card, the CSP SHALL use each cell of the grid only once.
5	63B#0440		The CSP SHALL store look-up secrets in a form that is resistant to offline attacks.
5	63B#0450		IF a look-up secret has at least 112 bits of entropy the CSP SHALL hash the secret iaw 63B#0370
5	63B#0460		IF a look-up secret has fewer than 112 bits of entropy the CSP SHALL hash the secret iaw 63B#0370
5	n/a		
5	63B#0470		IF a look-up secret has fewer than 64 bits of entropy the CSP SHALL enforce a rate-limiting mechanism iaw 63B#0320
5	63B#0480		The CSP SHALL use approved encryption and an authenticated protected channel when requesting look-up secrets.
5	n/a		
5	63B#0490		The CSP SHALL establish a separate channel with the Claimant's OOB authenticator in order to retrieve out-of-band secrets or authentication requests.
5	n/a		
5	n/a		

NIST §(H1)	63B tag	indx	KI_criterion
	Kantara IAF 63B Service Assessment Criteria		
5	63B#0500		When performing out-of-band authentication the CSP SHALL use an authentication method which positively establishes the Claimant's possession of a specific device.
5	63B#0510		The CSP SHALL ensure that the Claimant's authentictor is positively authenticated by one of the following ways:
5	63B#0510	a)	establishing an authenticated protected channel using approved cryptography whilst ensuring that the key used is stored in suitably secure storage available to the authenticator application;
5	63B#0510	b)	Authenticating via a public mobile telephone network using a SIM card or equivalent that uniquely identifies the device, whilst ensuring that the secret is sent to the out-of-band device via the PSTN.
5			
5	n/a		
5	n/a		
5	63B#0520		The CSP SHALL ensure that if the out-of-band authenticator sends an approval message over the secondary communication channel one of the following is done:
5	63B#0520	a)	the OOB Authenticator accepts transfer of the secret from the primary channel which it sends to the CSP over the secondary channel to associate the approval with the authentication transactio; OR
5	63B#0520	b)	the OOB Authenticator accepts transfer of the secret from the primary channel which it sends to the CSP over the secondary channel to associate the approval with the authentication transaction and then:
5	63B#0520	b) i)	the OOB Authenticator accepts a 'yes/no' response from the Claimant;

NIST §(H1)	Kantara IAF 63B Service Assessment Criteria		
	63B tag	indx	KI_criterion
5	63B#0520	b) ii)	the OOB Authenticator sends that response to the CSP
5	n/a		
5	n/a		
5	63B#0530		The CSP SHALL use a verification method to securely and uniquely identify the Claimant's authenticator without storing the actual identifying key.
5	63B#0540		The CSP SHALL, according to the type of OOB authenticator used, effect one of the following three options:.
5	n/a		
5	63B#0540	b)	When transferring the secret via the secondary channel: *transmit a random authentication secret to the Claimant via the primary channel and then wait for the secret to be returned from the Claimant's OOB authenticator via the secondary channel; OR*
5	63B#0540	c)	When the Claimant is verifying the secret: *send a random authentication secret to the claimant via the primary channel, and to their OOB authenticator via the secondary channel and then wait for an approval (or disapproval) message via the secondary channel.*
5	63B#0550		The CSP SHALL time-out and fail the authentication process if no response is received within 10 minutes of its initiation
5	63B#0560		The CSP SHALL accept a given authentication secret only once during its validity period.
5	63B#0570		The CSP SHALL create lists of look-up secret authenticators using an approved random bit generator [SP 800-90Ar1] which creates secrets having at least 20 bits of entropy;

NIST §(H1)	63B tag	indx	KI_criterion
			Kantara IAF 63B Service Assessment Criteria
5	63B#0580		IF an authentication secret has fewer than 64 bits of entropy the CSP SHALL enforce a rate-limiting mechanism iaw 63B#0320
5			
5	63B#0590		The CSP shall determine that a pre-registered 'phone number is registered to a specific physical device before using that device in OOB verification attempts.
5	63B#0600		IF the CSP allows the Subject to register a new 'phone as an authenticator it shall do so in a manner which fulfills the criteria in 63B#1510 - 63B#1530.
5	n/a		
5	63B#0610		The CSP SHALL use SF-OTP Devices whose secret key and associated algorithm provide at least the minimum security strength specified in the latest revision of SP 800-131A.
5	63B#0620		The CSP SHALL ensure that the nonce used to generate a OTP is of sufficient length to ensure that it is unique for each operation of
5	63B#0630		Thd CSP SHALL ensure that it uses SF-OTP Devices which do not facilitate the cloning of the secret key onto multiple devices.
5	n/a		
5	63B#0640		The CSP SHALL ensure that, if the nonce used to generate the authenticator output is based on a real-time clock, the nonce is changed at least once every 2 minutes.
5	63B#0650		The CSP SHALL ensure that,the OTP value associated with a given nonce is accepted only once.
5	n/a		
5	63B#0660		The CSP SHALL use approved cryptography to ensure that a Subject's SF-OTP authenticator to either:
5	63B#0660	a)	generate and exchange the secrets required to duplicate the authenticator output.

NIST §(H1)	63B tag	indx	KI_criterion
	63B#0660	b	obtain the secrets required to duplicate the authenticator output; OR
5	63B#0666		The CSP SHALL use approved encryption and an authenticated protected channel when retrieving the OTP.
5	63B#0680		The CSP SHALL ensure that, when using time-based OTPs [RFC238], their lifetime is determined taking into account:
5	63B#0680	a)	the expected clock drift (in either direction) of the authenticator over its lifetime;
5	63B#0680	b)	allowance for network delay;
5	63B#0680	c)	an allowance for user entry of the OTP.
5	63B#0690		The CSP SHALL accept a given time-based OTP only once during its validity period.
5	63B#0700		IF an authentication secret has fewer than 64 bits of entropy the CSP SHALL enforce a rate-limiting mechanism iaw 63B#0320
5	63B#0710		The CSP shall ensure that each use of a MF-OTP authenticator equires both factors to be input
5	n/a		
5	63B#0720		The CSP SHALL use MF-OTP Devices whose secret key and associated algorithm provide at least the minimum security strength specified in the latest revision of SP 800-131A.
5	63B#0730		The CSP SHALL ensure that the nonce used to generate a OTP is of sufficient length to ensure that it is unique for each operation of the device over its lifetime.
5	63B#0740		Thd CSP SHALL ensure that it uses MF-OTP Devices which do not facilitate the cloning of the secret key onto multiple devices.
5	n/a		

NIST §(H1)	63B tag	indx	KI_criterion
			Kantara IAF 63B Service Assessment Criteria
5	63B#0750		The CSP SHALL ensure that, if the nonce used to generate the authenticator output is based on a real-time clock, the nonce is changed at least once every 2 minutes.
5	63B#0760		The CSP SHALL ensure that,the OTP value associated with a given nonce is accepted only once.
5	63B#0770		The CSP SHALL ensure that memorized secrets used by the authenticator for activation are a randomly-chosen numeric secret at least 6 decimal digits in length or other memorized secret of equivalent complexity
5	63B#0780		The CSP SHALL enforce a rate-limiting mechanism iaw 63B#0320 (without qualification regarding the degree of entropy the memorized secret exhibits).
5	63B#0790		If a biometric factor is used in an authentication the CSP SHALL ensure that all criteria [ref] are fulfilled.
5	63B#0800		The CSP SHALL zeroize the unencrypted secret key and the activation secret or biometric sample (including any associated biometric data) immediately after an OTP has been generated.
5	63B#0810		The CSP SHALL ensure that MF-OTP authenticators strongly protected against compromise the associated symmetric keys.
5	63B#0820		The CSP SHALL use approved cryptography to ensure that a Subject's MF-OTP authenticator to either:
	63B#0820	a)	generate and exchange the secrets required to duplicate the authenticator output; OR
	63B#0820	b)	obtain the secrets required to duplicate the authenticator output.
5	63B#0830		The CSP SHALL treat all authenticators as being single-factor devices unelss they establish, via the authenticator source, that the authenticator device is a multi-factor.
	n/a		
5	63B#0840		The CSP SHALL ensure that all communication between the Claimant and Verifier use approved encryption and is via an authenticated protected channel.
5	63B#0850		The CSP SHALL use verification methods which ensure that, when using time-based OTPs [RFC238], their lifetime is determined taking into account:
	63B#0850	a)	the expected clock drift (in either direction) of the authenticator

NIST §(H1)	63B tag	indx	KI_criterion
	63B#0850	b)	allowance for network delay;
	63B#0850	c)	an allowance for user entry of the OTP.
5	63B#0860		The CSP SHALL accept a given time-based OTP only once during its validity period.
5	n/a		
5	63B#0870		IF an authentication output or activation secret has fewer than 64 bits of entropy the CSP SHALL enforce a rate-limiting mechanism iaw 63B#0320
5	63B#0880		If a biometric factor is used in an authentication the CSP SHALL ensure that all criteria [ref] are fulfilled.
5	63B#0890		The CSP SHALL ensure that SF-CS keys are stored in suitably secure storage available to the authenticator application.
5	63B#0900		The CSP SHALL ensure that SF-CS keys are strongly protected against unauthorized disclosure by the use of access controls that limit access to the key to only those software components on the device requiring access.
5	63B#0910		The CSP SHALL ensure that SF-CS key authenticators DO NOT facilitate the cloning of the secret key onto multiple devices.
5	n/a		Criteria 63B#0940 to '#0970 SHALL be fulfilled.
5	63B#0920		The CSP SHALL use SF-CD authenticators that are incapable of exporting their [unique] secret key.

NIST §(H1)	Kantara IAF 63B Service Assessment Criteria 63B tag	indx	KI_criterion
5	n/a		
5	63B#0930		The CSP SHALL use SF-CD authenticators whose secret key and associated algorithm provide at least the minimum security strength specified in the latest revision of SP 800-131A.
5	63B#0930		The CSP SHALL use SF-CD authenticators which employ a nonce of at least 64 bits length.
5	63B#0930		The CSP SHALL use SF-OTP Devices that use approved cryptography
5	n/a		
5	n/a		
5	63B#0940		The CSP SHALL use SF-CD verification methods which protect any secret keys against modification.
5	63B#0950		The CSP SHALL use SF-CD verification methods which protect symmetric secret keys against unauthorized disclosure.
5	63B#0960		The CSP SHALL use SF-CD verification methods for which the nonce is:
	63B#0960	a)	at least 64 bits in length; AND
	63B#0960	b)	either:
	63B#0960	b) i)	unique over the authenticator’s lifetime; OR
	63B#0960	b) ii)	generated using an approved random bit generator [SP 800-90Ar1]

NIST §(H1)	Kantara IAF 63B Service Assessment Criteria 63B tag	indx	KI_criterion
5	*63B#0970*		*The CSP SHALL use SF-CD Devices that use approved cryptography.*
5	*n/a*		
5	*63B#0980*		*The CSP SHALL ensure that MF-CS authenticators are activated by either* something [the Claimant] knows *or* something [the Claimant] is.
5	*n/a*		
5	*63B#0990*		*The CSP SHALL ensure that MF-CS keys are strongly protected against unauthorized disclosure by the use of access controls that limit access to the key to only those software components on the device requiring access.*
5	*63B#1000*		*The CSP SHALL ensure that MF-CS key authenticators DO NOT facilitate the cloning of the secret key onto multiple devices.*
5	*63B#1010*		*The CSP SHALL ensure that MF-CS key authenticators require the input of all factors before performing the authentication operation.*
5	*63B#1020*		*The CSP SHALL ensure that memorized secrets used by the authenticator for activation are a randomly-chosen numeric value at least 6 decimal digits in length or other memorized secret meeting the requirements of the applicable criteria 63B#0270 - '0377.*
5	*63B#1030*		*The CSP SHALL enforce a rate-limiting mechanism iaw 63B#0320 (without qualification regarding the degree of entropy the memorized secret exhibits).*

NIST	Kantara IAF 63B Service Assessment Criteria		
§(H1)	63B tag	indx	KI_criterion
5	63B#1040		*If a biometric factor is used in an authentication the CSP SHALL ensure that all criteria [ref] are fulfilled.*
5	63B#1050		*The CSP SHALL zeroize the unencrypted secret key and the activation secret or biometric sample (including any associated biometric data) immediately after an authentication transaction has taken place.*
5	n/a		*Criteria 63B#0940 to '#0970 SHALL be fulfilled.*
5	63B#1060		*The CSP SHALL ensure that MF-CS authenticators are activated by either* something [the Claimant] knows *or* something [the Claimant] is.
5	n/a		
5	63B#1070		*The CSP SHALL use MF-CD authenticators whose secret key and associated algorithm provide at least the minimum security strength specified in the latest revision of SP 800-131A.*
5	63B#1080		*The CSP SHALL use MF-CD authenticators which employ a nonce of at least 64 bits length.*
5	63B#1090		*The CSP SHALL use MF-CD Devices that use approved cryptography*
5	n/a		

NIST §(H1)	63B tag	indx	KI_criterion
	Kantara IAF 63B Service Assessment Criteria		
5	*63B#1100*		*The CSP SHALL ensure that memorized secrets used by the authenticator for activation are a randomly-chosen numeric value at least 6 decimal digits in length or other memorized secret meeting the requirements of the applicable criteria 63B#0270 - '0377.*
	63B#1110		*The CSP SHALL enforce a rate-limiting mechanism iaw 63B#0320 (without qualification regarding the degree of entropy the memorized secret exhibits).*
5	*63B#1120*		*If a biometric factor is used in an authentication the CSP SHALL ensure that all criteria [ref] are fulfilled.*
5	*63B#1130*		*The CSP SHALL zeroize the unencrypted secret key and the activation secret or biometric sample (including any associated biometric data) immediately after an authentication transaction has taken place.*
5	*n/a*		*Criteria 63B#0940 to '#0970 SHALL be fulfilled.*
5	*n/a*		
5	*63B#1140*		*The CSP SHALL provide Subjects instructions on how to appropriately protect the authenticator against theft or loss.*
5	*63B#1150*		*The CSP SHALL provide a documented mechanism to revoke or suspend the authenticator immediately upon notification from the Subject that loss or theft of the authenticator is suspected.*
5	*63B#1160*		*The CSP SHALL implement controls to protect against online guessing attacks.*
5	*63B#1170*		*The CSP SHALL limit consecutive failed authentication attempts on a single account to no more than 100.*
5	*n/a*		
5	*n/a*		
5	*n/a*		

NIST	Kantara IAF 63B Service Assessment Criteria		
§(H1)	63B tag	indx	KI_criterion
5	n/a		
5	n/a		
5	n/a		
5	n/a		
5	63B#1180		The CSP SHALL only use biometric techniques as part of a multi-factor authentication which requires the Claimaint to utilise a physical authenticator.
5	63B#1190		The CSP SHALL establish an authenticated protected channel between the sensor (or an endpoint containing a sensor that resists sensor replacement) and the verifier.
5	63B#1200		The CSP SHALL ensure that the sensor or endpoint is authenticated prior to capturing the biometric sample from the Claimant.
5	63B#1210		The CSP shall implement biometric systems which have at least the following characteristics:
5	63B#1210	a)	operate with an FMR [ISO/IEC 2382-37] of 1 in 1000 or better;
5	63B#1210	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	n/a		
5	63B#1210	c)	perfrom testing of presentation attack resistance in accordance with §12 of ISO/IEC 30107-3.
5	n/a		
5	63B#1220		The CSP SHALL implement rate-limiting measures on failed authentication attemps as follows:

NIST §(H1)	63B tag	indx	KI_criterion
	63B#1220	*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*
	63B#1220	*b)*	*no more than 5 consecutive failed authentication attempts can occur.*
5	*63B#1230*		*If the either limit set in 63B#1220 is reached the CSP SHALL:*
5	*63B#1230*	*a)*	*disable the biometric user authentication, and if an alternative authentication factor is already available use that other factor; OR OTHERWISE*
5	*63B#1230*	*b)*	*impose a delay of at least 30 seconds before the next attempt, increasing exponentially with each successive attempt.*
5	*63B#1240*		*When using biometric data in an authentication the CSP SHALL ensure that the sensor and endpoint performance, integrity, and authenticity are such as to not present unacceptable risk during the operation of the authentication protocol.*
5	*n/a*		
5	*n/a*		
5	*n/a*		
5	*n/a*		
5	*n/a*		
5	*63B#1250*		*If biometric comparisom is performed centrally rather than locally the CSP SHALL:*
5	*63B#1250*	*a)*	*limit use of the biometric as an authentication factor to one or more specific devices that are authenticated using approved cryptography;*
5	*63B#1250*	*b)*	*use a separate key to identify the device;*

NIST §(H1)	Kantara IAF 63B Service Assessment Criteria		
	63B tag	*indx*	*KI_criterion*
5	*63B#1250*	*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	*63B#1250*	*d)*	*transmit all biometric data over an authenticated protected channel.*
5	*n/a*		
5	*63B#1260*		*The CSP SHALL zeroize the biometric sample (including any associated biometric data) immediately after any training or research data has been derived.*
5	*n/a*		
5	*n/a*		
5	*n/a*		
5	*n/a*		
5	*n/a*		
5	*n/a*		
5	*63B#1270*		*If it signs authentication attestations the CSP SHALL use a digital signature that provides at least the minimum security strength specified in the latest revision of SP 800-131A.*
5	*n/a*		
5	*n/a*		
5	*63B#1280*		*The CSP SHALL employ a verifier impersonation-resistant authentication protocol so as to establish an authenticated protected channel with the ???? Authenticator?.*
5	*63B#1290*		*After establishing an authenticated protected channel with the [Authenticator?] the CSP SHALL strongly and irreversibly bind a channel identifier, that was negotiated in establishing the authenticated protected channel, to the authenticator output.*

NIST	Kantara IAF 63B Service Assessment Criteria		
§(H1)	63B tag	indx	KI_criterion
5	63B#1300		The CSP SHALL validate the signature or other information used to prove verifier impersonation resistance.
5	63B#1310		Where the CSP's risk assessment requires the use of cryptography as a mitigating control the CSP SHALL use approved cryptographic algorithms to establish verifier impersonation resistance, using keys that provide at least the minimum security strength specified in the latest revision of SP 800-131A.
5	n/a		
5	63B#1320		The CSP SHALL NOT deploy Authenticators that involve the manual entry of an authenticator output as controls against verifier impersonation.
5	63B#1330		If the CSP uses the services of a remote/independent Verifier, all communications with that entity SHALL occur through a mutually-authenticated secure channel using approved cryptography.
5	n/a		
5	63B#1340		The CSP SHALL effect controls which resist verifier compromise attacks by doing the following:
5	63B#1340	a)	only storing public keys using approved cryptographic algorithms;
5	n/a		(see item iii), below)
5	63B#1340	b)	other store other secrets using approved hash algorithms
5	63B#1340	c)	in each of the above cases, using respective controls which have at least the minimum applicable security strength specified in the latest revision of SP 800-131A

NIST §(H1)	63B tag	indx	KI_criterion
	Kantara IAF 63B Service Assessment Criteria		
5	63B#1350		The CSP SHALL use cryptographic methods when its risk assessment outcome determines that secrets which might be hashed are vulnerable to dictionary or exhaustive search attack.
5	n/a		
5	n/a		
5	63B#1360		The CSP SHALL establish authentication intent by requiring the Subject to explicitly respond to each authentication or reauthentication request.
5	n/a		
5	n/a		
5	n/		
5	63B#1370		If the CSP employs RESTRICTED authenticators then the associated risks shall be considered in its risk assessments.
5	n/a		
5	63B#1380		If the CSP employs RESTRICTED authenticators then it SHALL:

NIST	Kantara IAF 63B Service Assessment Criteria		
§(H1)	63B tag	indx	KI_criterion
5	63B#1380	a)	require at least one alternate authenticator that is not RESTRICTED;
5	63B#1380	b)	provide meaningful notice to subscribers regarding the security risks of the RESTRICTED authenticator and availability of alternative(s) that are not RESTRICTED;
5	n/a		See 1370
5	n/a		DIAS is required only of agencies
6	n/a		
6	n/a		
6	63B#1390		The CSP SHALL bind authenticators to Subject accounts by either:
6	63B#1390	a)	issuing them at the time of enrollment; OR
6	63B#1390	b)	associating a subscriber-provided authenticator that is acceptable to the CSP.
6	n/a		
6	63B#1400		The CSP SHALL maintain, for the duration of the digital identity lifecycle accounting for the provisions of its data retention schedule, a record of all authenticators that are or have been associated with each identity and of all significant actions taken with regard to the maintenance of each authenticator.
6	63B#1410		The CSP SHALL maintain information required for throttling authentication attempts when required (see 63B#1160 & '#1170).
6	63B#1420		The CSP SHALL determine the type of user-provided authenticator and make that determination available to Verifiers to fulfill AAL2 requirements.
6	63B#1430		The CSP SHALL maintain, for the duration of the digital identity lifecycle accounting for the provisions of its data retention schedule, a record of all authenticators that are or have been associated with each identity:
6	n/a		
6	n/a		
6	n/a		

NIST	Kantara IAF 63B Service Assessment Criteria		
§(H1)	*63B tag*	*indx*	*KI_criterion*
6	*63B#1440*		*The CSP SHALL ensure that, when any new authenticator is bound to a subscriber account, the binding protocol and the protocol for provisioning the associated key(s) are done at a level of security commensurate with use of the authenticator at AAL2.*
6	*n/a*		
6	*63B#1450*		*The CSP SHALL NOT bind multifactor authenticators unless at the end of a session in which identity proofing has been completed or after multifactor authentication has already been accomplished.*
6	*n/a*		*Included within 63B#1450*
6	*n/a*		*Though not normatively-stated, accommodated within the foillowing criterion.*
6	*63B#1470*		*When the CSP binds an authenticator to an identity as a result of the CSP having performed a successful identity proofing of the Subject, the CSP SHALL bind to the Subject's online identity:*
6	*63B#1470*	*a)*	*at least one physical (* something [the Subject] has*) authenticator; AND*
6	*63B#1470*	*b)*	*a memorized secret or at least one biometric.*
6	*n/a*		
6	*n/a*		
6	*63B#1480*		*The CSP SHALL ensure that authenticators bound to the Subject's online identity are AAL2 or higher.*

NIST §(H1)	Kantara IAF 63B Service Assessment Criteria 63B tag	indx			KI_criterion
6	n/a				
6	n/a				
6	63B#1490				The CSP SHALL NOT expose personal information to the subscriber, even if self-asserted.
6	n/a				
6	63B#1500				If enrollment and binding cannot be completed in a single physical encounter or within a single protected electronic transactional session, the CSP SHALL employ the following methods to ensure that the same party acts as the Applicant throughout the processes:
6	63B#1500	a)			For remote transactions the CSP SHALL:
6	63B#1500	a)	i)		require the Applicant to identify themselves in each new binding transaction by presenting a temporary secret which was either:
6	63B#1500	a)	i)	1)	established during a prior transaction; or
6	63B#1500	a)	i)	2)	sent to the Applicant's phone number, email address, or postal address of record.
6	63B#1500	a)	ii)		Only issue long-term authenticator secrets to the Applicant within a protected session.
6	63B#1500	b)			For in-person transactions the CSP SHALL:
6	63B#1500	b)	i)		require the Applicant to identify themselves in person by either:
6	63B#1500	b)	i)	1)	using a secret as described in remote transaction a) i) above; OR
6	63B#1500	b)	i)	2)	through use of a biometric that was recorded during a prior encounter.
6	63B#1500	b)	ii)		only accepting a temporary secret once;
6	63B#1500	b)	iii)		only relying upon long-term authenticator secrets during a physical transaction, if they have been loaded locally onto a physical device that is issued in person to the Applicant or delivered in a manner that confirms the Applicant's address of record.
6	n/a				

NIST	Kantara IAF 63B Service Assessment Criteria		
§(H1)	63B tag	indx	KI_criterion
6	n/a		
6	n/a		
6	63B#1510		Prior to issuing the Subject with new/additional AAL2 authenticators the CSP SHALL first authenticate the Subject at AAL2.
6	n/a		
6	n/a		
6	n/a		
6	n/a		
6	63B#1520		If a Claimant loses all authenticators of a factor necessary to complete multi-factor authentication the CSP SHALL enable replacement of lost authentication factors by one of the following methods:
6	63B#1520	a)	require the Claimant to present themselves for full identity proofing as per the CSP's policies and processes as operated in conformity with the applicable 63A_SAC criteria; OR

NIST	Kantara IAF 63B Service Assessment Criteria		
§(H1)	63B tag	indx	KI_criterion
6	n/a		
6	63B#1520	b)	IF the CSP has retained evidence from the original proofing process pursuant to a privacy risk assessment iaw 63A#0180, the CSP SHALL authenticate the Claimant using an authenticator of the remaining factor, if any, to confirm binding to the existing identity.
6	n/a		
6	n/a		
6	n/a		
6	n/a		
6	n/a		
6	n/a		
6	n/a		
6	n/a		
	n/a		
6	n/a		

NIST §(H1)	Kantara IAF 63B Service Assessment Criteria 63B tag	indx	KI_criterion
6	*n/a*		
6	*n/a*		
6	*63B#1540*		*If the CSP accepts subscriber-provided authenticators the CSP SHALL ensure that such authenticators are bound to the Subject's online identity iaw 63B#1510.*
6	*n/a*		
6	*n/a*		
6	*n/a*		
6	*n/a*		
6	*n/a*		

NIST §(H1)	Kantara IAF 63B Service Assessment Criteria 63B tag	indx	KI_criterion
6	63B#1550		IF the CSP supports a method by which it can authenticate the Subject using a backup or alternate authenticator the CSP SHALL only accept backup authenticators which are either a memorized secret or a physical authenticator.
6	n/a		
6	n/a		
6	n/a		
6	n/a		
	63B#1560		If the CSP issues authenticators which expire the CSP SHALL NOT accept authentication claims which attempt to use an expired authenticator.
	n/a		
6	63B#1570		The CSP SHALL require Subjects to surrender or attest to destruction of any physical authenticator containing attribute certificates signed by the CSP as soon as practical after expiration or receipt of a renewed authenticator, or after receipt of notice of either revocation or termination.
6	n/a		
6	63B#1580		The CSP SHALL revoke promptly the binding of authenticators to the Subject's online identity, and give notice of such to the Subject, when any one of the following occurs:
		a)	the Subject's online identity ceases to exist; OR
		b)	the Subject requests revocation; OR

NIST	Kantara IAF 63B Service Assessment Criteria		
§(H1)	63B tag	indx	KI_criterion
		c)	the CSP determines that the Subject no longer meets its eligibility requirements; OR
		d)	the CSP is obligated to do so in response to a legal instrument.
6	n/a		
6	n/a		
7	n/a		This section applies to RPs
7	n/a		This section applies to RPs
7	n/a		This section applies to RPs
7	n/a		
	End of 63B_SAC criteria		