Title: Identity Assurance Framework: NIST SP 800-63B Service Assessment Criteria (SAC) & Statement of Criteria Applicability (SoCA)
Document id: KIAF-1440
Version: 4.0
Document type: Recommendation
Publication Date: 2020-10-15
Effective Date: 2021-02-01
Status: Final
Approval Authority: IAWG
Original Sponsor: ID.me

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 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 and AAL3, 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.

Though this document is structured with headers, footers etc. for document management purposes, the 63B_SAC worksheet is not intended to be published in a printed page format, and hence 'Normal' View is recommended at all times.

Revision history: See Revision History

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

Version	*Date*	*Status*	*Summary of changes*
Note re. version numbers:		*From v4.0 onwards 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.
v3.0	2018-11-09	Final - Non-Material changes - released for application	Typo tidying and clarifications of some criteria's applicability: Criteria amended: #1300, #1310, #1320.
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	12/14/17	For Public review	Initial set of mature draft criteria.

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
4		Authenticator Assurance Levels						n/a								
4		Authenticator Assurance Levels	To satisfy the requirements of a given AAL, a claimant SHALL be authenticated with at least a given level of strength to be recognized as a subscriber.	✓				63B#0010			The CSP SHALL authenticate a Claimant at at least the ~~same~~ requested AAL .	✓	✓		This requires that the Claimant must have been issued with and be in possession of a Credential of the same level or higher than that which has been requested before the CSP can consider subjecting the Claimant to an authentication process. The table below considers the acceptability for authentication processing of all AAL1/2/3 combinations. **Requested AAL / Lowest Cred AAL / Min Authn AAL which can be attempted** 1 / 1 / 1 (Note - IAL1 / AAL1 1 / 2 / 2 are not supported 1 / 3 / 3 by Kantara) 2 / 1 / No Authn permissible 2 / 2 / 2 2 / 3 / 3 3 / 1 / No Authn permissible 3 / 2 / No Authn permissible 3 / 3 / 3	
4		Authenticator Assurance Levels	The result of an authentication process is an identifier that SHALL be used each time that subscriber authenticates to that RP.	✓				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		Authenticator Assurance Levels	The identifier MAY be pseudonymous.					n/a								
4		Authenticator Assurance Levels	Subscriber identifiers SHOULD NOT be reused for a different subject but SHOULD be reused when a previously-enrolled subject is re-enrolled by the CSP.					n/a								
								n/a								
4		Authenticator Assurance Levels	Other attributes that identify the subscriber as a unique subject MAY also be provided.					n/a								
4		Authenticator Assurance Levels	[Therefore] Agencies SHALL select a minimum of AAL2 when self-asserted PII or other personal information is made available online				✓	63B#0030			Agencies SHALL require a minimum of AAL2 when self-asserted PII or other personal information is made available to the Subject online.	✓	✓			
4.1		*AAL1 - disregarded*														
4.2 (AAL 2)		Authenticator Assurance Level 2														
4.2 (AAL 2)		Authenticator Assurance Level 2	Proof of possession and control of two distinct authentication factors is required through secure authentication protocol(s).	✓				63B#0040			The CSP SHALL use secure authentication protocol(s) to prove that the Claimant has both possession and control over two distinct authentication factors.	✓	✓		Note - this is expressly a 'SHALL' @AAL3, yet is expressed with the same degree of rigour but only 'required' at AAL2. It seems reasonable to inlude it as being applicable at both ALs.	
4.2.1 (AAL 2)		Permitted Authenticator Types	At AAL2, authentication SHALL occur by the use of either a multi-factor authenticator or a combination of two single-factor authenticators	✓				63B#0050			The CSP SHALL perform authentication using EITHER a multi-factor authenticator OR a combination of two single-factor authenticators.	✓				
4.2.1 (AAL 2)		Permitted Authenticator Types	When a multi-factor authenticator is used, any of the following MAY be used:	✓				63B#0060			When a multi-factor authenticator is used,the CSP SHALL employ any one of the following:	✓				
4.2.1 (AAL 2)		Permitted Authenticator Types	· Multi-Factor OTP Device (Section 5.1.5)	✓				63B#0060	a)		Multi-Factor OTP Device;	✓				
4.2.1 (AAL 2)		Permitted Authenticator Types	· Multi-Factor Cryptographic Software (Section 5.1.8)	✓				63B#0060	b)		Multi-Factor Cryptographic Software;	✓				
4.2.1 (AAL 2)		Permitted Authenticator Types	· Multi-Factor Cryptographic Device (Section 5.1.9)	✓				63B#0060	c)		Multi-Factor Cryptographic Device.	✓			Equivalent to 63B#0260 a)	

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
4.2.1 (AAL 2)		Permitted Authenticator Types	When a combination of two single-factor authenticators is used, it SHALL include a Memorized Secret authenticator (Section 5.1.1) and one possession-based (i.e., "something you have") authenticator from the following list:	✓				63B#0070			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:	✓				
4.2.1 (AAL 2)		Permitted Authenticator Types	· Look-Up Secret (Section 5.1.2)	✓				63B#0070	a)		Look-Up Secret;	✓				
4.2.1 (AAL 2)		Permitted Authenticator Types	· Out-of-Band Device (Section 5.1.3)	✓				63B#0070	b)		Out-of-Band Device;	✓				
4.2.1 (AAL 2)		Permitted Authenticator Types	· Single-Factor OTP Device (Section 5.1.4)	✓				63B#0070	c)		Single-Factor OTP Device;	✓				
4.2.1 (AAL 2)		Permitted Authenticator Types	· Single-Factor Cryptographic Software (Section 5.1.6)	✓				63B#0070	d)		Single-Factor Cryptographic Software;	✓				
4.2.1 (AAL 2)		Permitted Authenticator Types	· Single-Factor Cryptographic Device (Section 5.1.7)	✓				63B#0070	e)		Single-Factor Cryptographic Device.	✓			Equivalent to 63B#0260 b) i)	
4.2.2 (AAL 2)		Authenticator and Verifier Requirements	Cryptographic authenticators used at AAL2 SHALL use approved cryptography.	✓				63B#0080			The CSP SHALL ensure that all cryptographic authenticators employ cryptographic techniques approved by a Federal or industry body.	✓				
4.2.2 (AAL 2)		Authenticator and Verifier Requirements	Authenticators procured by government agencies SHALL be validated to meet the requirements of FIPS 140 Level 1.				✓	63B#0090			Federal agencies SHALL only procure authenticators which have been validated as meeting FIPS 140 Level 1 or higher.	✓			NIST guidance (2020-07-05): The intent of the text "procured by" is to exempt user-provided ("bring-your-own) authenticators from having to meet the FIPS 140 requirements, particularly on the government-to-public use case.	
4.2.2 (AAL 2)		Authenticator and Verifier Requirements	Software-based authenticators that operate within the context of an operating system MAY, where applicable, attempt to detect compromise of the platform in which they are running (e.g., by malware) and SHOULD NOT complete the operation when such a compromise is detected.					n/a								
4.2.2 (AAL 2)		Authenticator and Verifier Requirements	At least one authenticator used at AAL2 SHALL be replay resistant as described in Section 5.2.8.	✓				63B#0100			The CSP SHALL ensure that at least one authenticator used is replay resistant.	✓	✓		Note - the same requirement exists at AAL3 without any change in rigour	
4.2.2 (AAL 2)		Authenticator and Verifier Requirements	Authentication at AAL2 SHOULD demonstrate authentication intent from at least one authenticator as discussed in Section 5.2.9.					n/a								
4.2.2 (AAL 2)		Authenticator and Verifier Requirements	Communication between the claimant and verifier (the primary channel in the case of an out-of-band authenticator) SHALL be via an authenticated protected channel to provide confidentiality of the authenticator output and resistance to MitM attacks.	✓				63B#0110			The CSP SHALL use only mutually-authenticated protected channels when communicating with Claimants	✓	✓		Note - the same requirement exists at AAL3 without any change in rigour.	
4.2.2 (AAL 2)		Authenticator and Verifier Requirements	Verifiers operated by government agencies at AAL2 SHALL be validated to meet the requirements of FIPS 140 Level 1.				✓	63B#0120			Federal agencies SHALL only operate verifiers which have been validated as meeting FIPS 140 Level 1 or higher.	✓				
4.2.2 (AAL 2)		Authenticator and Verifier Requirements	When a device such a smartphone [sic] is used in the authentication process, the unlocking of that device (typically done using a PIN or biometric) SHALL NOT be considered one of the authentication factors.	✓				63B#0130			The CSP SHALL NOT consider the unlocking of a device used in the authentication process to be an authentication factor.	✓	✓			

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
4.2.2 (AAL 2)		Authenticator and Verifier Requirements	Generally, it is not possible for a verifier to know that the device had been locked or if the unlock process met the requirements for the relevant authenticator type.					n/a								
4.2.2 (AAL 2)		Authenticator and Verifier Requirements	When a biometric factor is used in authentication at AAL2, the performance requirements stated in Section 5.2.3 SHALL be met, …	✓				63B#0140			If a biometric factor is used in an authentication the CSP SHALL ensure that all criteria 63B#1470 to 63B#1550 are fulfilled.	✓				
4.2.2 (AAL 2)		Authenticator and Verifier Requirements	… and the verifier SHOULD make a determination that the biometric sensor and subsequent processing meet these requirements.					n/a								
4.2.3 (AAL 2)		Reauthentication	Periodic re-authentication of subscriber sessions SHALL be performed as described in Section 7.2 .					n/a			Addressed by 63B#0150					
4.2.3 (AAL 2)		Reauthentication	Re-authentication of a session that has not yet reached its time limit MAY require only a memorized secret or a biometric in conjunction with the still-valid session secret. The verifier MAY prompt the user to cause activity just before the inactivity timeout .					n/a								
4.2.3 (AAL 2)		Reauthentication	The verifier MAY prompt the user to cause activity just before the inactivity timeout .					n/a								
4.2.3 (AAL 2)		Reauthentication	Re-authentication of the subscriber SHALL be repeated following any period of inactivity lasting 30 minutes or longer	✓	✓			63B#0150			The RP SHALL terminate a session and the life of the current session secret whenever they are unable to receive affirmative re-authentication of the Subject, either:	✓				
4.2.3 (AAL 2)		Reauthentication	At AAL2, authentication of the subscriber SHALL be repeated at least once per 12 hours during an extended usage session, regardless of user activity.	✓	✓			63B#0150	a)		a) prior to a period of session inactivity reaching 30 minutes; OR	✓				
4.2.3 (AAL 2)		Reauthentication	Reauthentication of the subscriber SHALL be repeated following any period of inactivity lasting 30 minutes or longer	✓	✓			63B#0150	b)		b) prior to an extended usage session reaching 12 hours since the last successful re-authentication, regardless of user activity.	✓				
4.2.3 (AAL 2)		Reauthentication	The session SHALL be terminated (i.e., logged out) when either of these time limits is reached.					n/a			Addressed by 63B#0150					
4.2.4 (AAL 2)		Security Controls	The CSP SHALL employ appropriately-tailored security controls from the *moderate* baseline of security controls defined in SP 800-53 or equivalent federal (e.g., FEDRAMP) or industry standard.	✓				63B#0160			The CSP SHALL employ appropriately-tailored moderate baseline security controls, as defined in SP 800-53 or equivalent Federal or industry standards.	✓				
4.2.4 (AAL 2)		Security Controls	The CSP SHALL ensure that the minimum assurance-related controls for moderate-impact systems or equivalent are satisfied.	✓				63B#0170			When fulfilling criterion 63A#0210 the CSP SHALL ensure that minimum assurance-related control needs for moderate-impact systems or equivalent are satisfied.	✓				
4.2.5 (AAL 2)		Records Retention Policy	The CSP shall comply with its respective records retention policies in accordance with applicable laws, regulations, and policies, including any NARA records retention schedules that may apply.	✓				63B#0180			The CSP SHALL document, periodically review and comply with, a data retention schedule, accounting for:	✓	✓			
4.2.5 (AAL 2)				✓				63B#0180	a)		results of a privacy and security risk assessment;	✓	✓			
4.2.5 (AAL 2)				✓				63B#0180	b)		applicable laws, regulations, policies, and specific record retention schedules;	✓	✓		Whilst SP 800-63B refers explicitly to NARA record retention schedules the Kantara sub-criterion is deliberately broader.	

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
4.2.5 (AAL 2)				✓				63B#0180	c)		its own records retention policy.	✓	✓			
4.2.5 (AAL 2)		Records Retention Policy	If the CSP opts to retain records in the absence of any mandatory requirements, the CSP SHALL conduct a risk management process, including assessments of privacy and security risks to determine how long records should be retained and ...					n/a			See 63B#0180					
4.2.5 (AAL 2)		Records Retention Policy	... SHALL inform the subscriber of ~~that~~ its retention policy.	✓				63B#0190			The CSP SHALL publish to Subjects its data retention schedule, to the extent appropriate to the context.	✓	✓			
4.3 (AAL 3)		Authenticator Assurance Level 3	AAL3 authentication SHALL use a hardware-based authenticator ...	✓				63B#0200			**The CSP SHALL ensure that at least one authenticator used is hardware-based.**		✓			
4.3 (AAL 3)			... and an authenticator that provides verifier-impersonation resistance	✓				63B#0210			**The CSP SHALL ensure that at least one authenticator used is verifier-impersonation resistant.**		✓		it is permissable to use a single authenticator which fulfills both 63B#0030 and this criterion.	
4.3 (AAL 3)		Authenticator Assurance Level 3	In order to authenticate at AAL3, claimants SHALL prove possession and control of two distinct authentication factors through secure authentication protocol(s).					n/a			Addressed by 63B#0040					
4.3 (AAL 3)		Authenticator Assurance Level 3	Approved cryptographic techniques are required.	✓				63B#0220			**The CSP SHALL ensure that all authenticators employ hardware cryptographic techniques approved by a Federal or industry body.**		✓		Although the NIST clause states 'are required' this is taken to be a normative assertion and since it follows the above clause immediately within the same paragraph is taken to have a normative weight. Furthermore (confusingly) an equivalent clasue at AAL2 uses 'SHALL'. *NOTE - need to find the stock phrase for approved std and use throughtout this SAC (hasn't been done before, so potentially changes to 'old' criteria which may need to be amended.*	
4.3.1 (AAL 3)		Permitted Authenticator Types	AAL3 authentication SHALL occur by the use of one of a combination of authenticators satisfying the requirements in Section 4.3. Possible combinations are:	✓				63B#0230			**The CSP SHALL perform authentication using EITHER**		✓			
4.3.1 (AAL 3)			• Multi-Factor Cryptographic Device (Section 5.1.9)	✓				63B#0230	a)		*a Multi-Factor Cryptographic Device*		✓		Essentially the same as 63B#0040 c)	
4.3.1 (AAL 3)				✓				63B#0230	b)		**OR one of the following combinations of authenticators**		✓			
4.3.1 (AAL 3)			• Single-Factor Cryptographic Device (Section 5.1.7) used in conjunction with Memorized Secret (Section 5.1.1)	✓				63B#0230	b)	i)	*Single-Factor Cryptographic Device and a Memorized Secret;*		✓		Essentially the same as 63B#0040 e)	
4.3.1 (AAL 3)			• Multi-Factor OTP device (software or hardware) (Section 5.1.5) used in conjunction with a Single-Factor Cryptographic Device (Section 5.1.7)	✓				63B#0230	b)	ii)	**Single-Factor Cryptographic Device and a Multi-Factor OTP device (software or hardware);**		✓			
4.3.1 (AAL 3)			• Multi-Factor OTP Device (hardware only) (Section 5.1.5) used in conjunction with a Single-Factor Cryptographic Software (Section 5.1.6)	✓				63B#0230	b)	iii)	**Multi-Factor OTP Device (hardware only) and a Single-Factor Cryptographic Software;**		✓			
4.3.1 (AAL 3)			• Single-Factor OTP Device (hardware only) (Section 5.1.4) used in conjunction with a Multi-Factor Cryptographic Software Authenticator (Section 5.1.8)	✓				63B#0230	b)	iv)	**Single-Factor OTP Device (hardware only) and a Multi-Factor Cryptographic Software Authenticator;**		✓			

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
4.3.1 (AAL 3)			• Single-Factor OTP Device (hardware only) (Section 5.1.4) used in conjunction with a Single-Factor Cryptographic Software Authenticator (Section 5.1.6) and a Memorized Secret (Section 5.1.1)	✓				63B#0230	b)	v)	***Single-Factor OTP Device (hardware only) and a Single-Factor Cryptographic Software Authenticator, and a Memorized Secret.***		✓			
4.3.2 (AAL 3)		Authenticator and Verifier Requirements	Communication between the claimant and verifier SHALL be via an authenticated protected channel to provide confidentiality of the authenticator output and resistance to MitM attacks.					*n/a*			*Addressed by 63B#0110*				The CSP SHALL ensure that at least one authenticator used is replay resistant.	
4.3.2 (AAL 3)		Authenticator and Verifier Requirements	All cryptographic device authenticators used at AAL3 SHALL be verifier impersonation resistant as described in Section 5.2.5 and ...	✓				63B#0240			***The CSP SHALL ensure that all authenticators used are verifier impersonation resistant.***		✓		This almost implies that non-crypto authenticator devices NEED NOT be resistant, yet only such devices are permitted acording to #3030.	
4.3.2 (AAL 3)		Authenticator and Verifier Requirements	... SHALL be replay resistant as described in Section 5.2.8					*n/a*			*Addressed by 63B#0110*					
4.3.2 (AAL 3)		Authenticator and Verifier Requirements	All authentication and reauthentication processes at AAL3 SHALL demonstrate authentication intent from at least one authenticator as described in Section 5.2.9	✓				63B#0250			***The CSP SHALL ensure that each authentication and re-authentication instance demonstrates authentication intent from at least one authenticator.***		✓			
4.3.2 (AAL 3)		Authenticator and Verifier Requirements	Multi-factor authenticators used at AAL3 SHALL be hardware cryptographic modules validated at FIPS 140 Level 2 or higher overall with at least FIPS 140 Level 3 physical security.	✓				63B#0260			***The CSP SHALL require multi-factor hardware cryptographic module authenticator which are validated at FIPS 140 Level 2 or higher overall with at least FIPS 140 Level 3 physical security.***		✓			
4.3.2 (AAL 3)		Authenticator and Verifier Requirements	Single-factor cryptographic devices used at AAL3 SHALL be validated at FIPS 140 Level 1 or higher overall with at least FIPS 140 Level 3 physical security.	✓				63B#0270			***The CSP SHALL require single-factor hardware cryptographic module authenticator which are validated at FIPS 140 Level 1 or higher with at least FIPS 140 Level 3 physical security.***		✓			
4.3.2 (AAL 3)			Verifiers at AAL3 SHALL be validated at FIPS 140 Level 1 or higher	✓				63B#0280			***The CSP SHALL only use verifiers which have been validated at FIPS 140 Level 1 or higher***		✓			
4.3.2 (AAL 3)		Authenticator and Verifier Requirements	Verifiers at AAL3 SHALL be verifier compromise resistant as described in Section 5.2.7 with respect to at least one authentication factor.	✓				63B#0290			***The CSP SHALL ensure that verifiers are verifier compromise resistant with respect to at least one authentication factor in accordance with 63B#1630 & '1640.***		✓			
4.3.2 (AAL 3)		Authenticator and Verifier Requirements	Relevant side-channel attacks SHALL be determined by a risk assessment performed by the CSP.	✓				63B#0300			***The CSP SHALL include in its risk assessment an evaluation as to which side-channel attacks are relevant.***		✓			
4.3.2 (AAL 3)		Authenticator and Verifier Requirements	When a device such a smartphone *[sic]* is used in the authentication process — presuming that the device is able to meet the requirements above — the unlocking of that device SHALL NOT be considered to satisfy one of the authentication factors.					63B#0305			***The CSP SHALL NOT consider the unlocking of a smartphone to be an authentication factor.***		✓		NIST's manner of experessing this requirement makes the fulfillment of preceding criteria almost an aside. Cf. 63B#0090.	
4.3.2 (AAL 3)		Authenticator and Verifier Requirements	When a biometric factor is used in authentication at AAL3, the verifier SHALL make a determination that the biometric sensor and ...					*n/a*								
4.3.2 (AAL 3)			... subsequent processing meet the performance requirements stated in Section 5.2.3.	✓				63B#0310			*If a biometric factor is used in an authentication the CSP SHALL ensure that the biometric sensor* ***and subsequent processing*** *meet the performance requirements stated in 63B#1470 - '#1550 inc.*		✓		Note - the 'biometric sensor requirement is taken from the AAL2 source which is not mandatory.	
4.3.3 (AAL 3)		Reauthentication	Periodic reauthentication of subscriber sessions SHALL be performed as described in Section 7.2.	✓	✓			63B#0320			*The RP SHALL terminate a session and the life of the current session secret whenever they are unable to receive affirmative re-authentication of the Subject, either:*		✓		This is essentially the same as 63B#0130, subject to the paramter change in the sub-clauses.	

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
4.3.3 (AAL 3)		Reauthentication	At AAL3, authentication of the subscriber SHALL be repeated at least once per 12 hours during an extended usage session, regardless of user activity, as described in Section 7.2.	~~✓~~	✓			63B#0320	a)		prior to a period of session inactivity reaching **15** minutes; OR		✓			
4.3.3 (AAL 3)		Reauthentication	Reauthentication of the subscriber SHALL be repeated following any period of inactivity lasting 15 minutes or longer.	~~✓~~	✓			63B#0320	b)		b) prior to a session reaching **12** hours since the last successful re-authentication, regardless of user activity.		✓			
4.3.3 (AAL 3)		Reauthentication	*REPOSITIONED FOR REASONS OF LOGICAL SEQUENCE:* The session SHALL be terminated (i.e., logged out) when either of these time limits is reached.	~~✓~~	✓			n/a			Addressed by 63B#4343					
4.3.3 (AAL 3)		Reauthentication	Reauthentication SHALL use both authentication factors.	✓				63B#0320			**When re-authenticating, the CSP SHALL require the user to prove possession of both authentication factors**		✓		This has to be fulfilled by the CSP, but they must necessarilly know that it was a RE authentication for this to be proven. The criterion cannot be applied if the CSP ihas no knowledge of any re-authentication attempt.	
4.3.4 (AAL 3)		Security Controls	The CSP SHALL employ appropriately-tailored security controls from the high baseline of security controls defined in SP 800-53 or an equivalent federal (e.g., FEDRAMP) or industry standard.	✓				63B#0330			The CSP SHALL employ appropriately-tailored **high** baseline security controls defined in SP 800-53 or equivalent Federal or industry standards.		✓			
4.3.4 (AAL 3)			The CSP SHALL ensure that the minimum assurance-related controls for high-impact systems or equivalent are satisfied.	✓				63B#0340			When fulfilling criterion 63A#3200 the CSP SHALL ensure that its system satisfies the minimum assurance-related control requirements for **high** -impact systems or equivalent.		✓			
4.3.5 (AAL 3)		Records Retention Policy	The CSP shall SHALL comply with its respective records retention policies in accordance with applicable laws, regulations, and policies, including any NARA records retention schedules that may apply.					n/a			Addressed by 63B#0220					
4.3.5 (AAL 3)		Records Retention Policy	If the CSP opts to retain records in the absence of any mandatory requirements, the CSP SHALL conduct a risk management process, including assessments of privacy and security risks, to determine how long records should be retained and ...					n/a			Adressed by 63B#0220 a)					
4.3.5 (AAL 3)		Records Retention Policy	... SHALL inform the subscriber of that retention policy					n/a			Addressed by 63B#0230					
4.4		Privacy Requirements	The CSP SHALL employ appropriately-tailored privacy controls defined in SP 800-53 or equivalent industry standard.	✓				63B#0350			The CSP SHALL employ appropriately-tailored privacy controls, to include control enhancements (appropriate for the AAL being souight - refer to 63B#0210 and '#3200) as defined in SP 800-53 or equivalent Federal or industry standards.	✓	✓			
4.4		Privacy Requirements	CSPs SHALL NOT use or disclose information about subscribers for any purpose other than conducting authentication, related fraud mitigation, or to comply with law or legal process, ...	✓				63B#0360			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.	✓	✓			
4.4		Privacy Requirements	... unless the CSP provides clear notice and obtains consent from the subscriber for additional uses .	✓				63B#0370			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.	✓	✓			
4.4		Privacy Requirements	CSPs SHALL NOT make consent a condition of the service.	✓				63B#0380			The CSP SHALL NOT make consent a condition of the service.	✓	✓			
4.4		Privacy Requirements	Care SHALL be taken to ensure that use of such information is limited to its original purpose for collection	✓				63B#0390			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).	✓	✓			

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
4.4		Privacy Requirements	If the use of such information does not fall within uses related to authentication or to comply with law or legal process, the CSP SHALL provide notice and obtain consent from the subscriber.					n/a								
4.4		Privacy Requirements	This notice SHOULD follow the same principles as described in Notice and Consent in SP 800-63A Section 8.2 and SHOULD NOT be rolled up into a legalistic privacy policy or general terms and conditions. Rather, if there are uses outside the bounds of these explicit purposes, the subscriber SHOULD be provided with a meaningful way to understand the purpose for additional uses, and the opportunity to accept or decline.					n/a								
4.4		Privacy Requirements	Regardless of whether the CSP is an agency or private sector provider, the following requirements apply to an agency offering or using the authentication service:				✓	63B#0400			Federal Agencies SHALL:	✓	✓			
4.4		Privacy Requirements	· The agency SHALL consult with their Senior Agency Official for Privacy (SAOP) and conduct an analysis to determine whether the collection of PII to issue or maintain authenticators triggers the requirements of the *Privacy Act of 1974* [Privacy Act] (see Section 9.4).				✓	63B#0400	a)		*in consultation with the Agency's Senior Agency Official for Privacy, conduct an analysis determining whether the requirements of the Privacy Act are triggered, according to the agency's CSP and/or RP role(s).*	✓	✓			
4.4		Privacy Requirements	o The agency SHALL publish a System of Records Notice (SORN) to cover such collections, as applicable.				✓	63B#0400	b)		*according to the outcome of the analysis in a) above, publish or identify coverage by a System of Records Notice, as applicable;*	✓	✓			
4.4		Privacy Requirements	o The agency SHALL consult with their SAOP and conduct an analysis to determine whether the collection of PII to issue or maintain authenticators triggers the requirements of the E-Government Act of 2002 [EGov].				✓	63B#0400	c)		*in consultation with the Agency's Senior Agency Official for Privacy, conduct an analysis determining whether the requirements of the E-Government Act are triggered, according to the agency's CSP and/or RP role(s);*	✓	✓			
4.4		Privacy Requirements	o The agency SHALL publish a Privacy Impact Assessment (PIA) to cover such collection, as applicable.				✓	63B#0400	d)		*according to the outcome of the analysis in c) above, publish or identify coverage by a Privacy Impact Assessment, as applicable.*	✓	✓			
5		Authenticator and Verifier Requirements						n/a								
5.1		Requirements by Authenticator Type						n/a								
5.1.1.1		Memorized Secret Authenticators	Memorized secrets SHALL be at least 8 characters in length if chosen by the subscriber.	✓				63B#0410			*The CSP SHALL require memorized secrets chosen by the Subject to be at least 8 characters in length.*	✓	✓			
5.1.1.1		Memorized Secret Authenticators	Memorized secrets chosen randomly by the CSP or verifier SHALL be at least 6 characters in length and MAY be entirely numeric.	✓				63B#0420			*The CSP SHALL require memorized secrets generated by itself or a Verifier to be at least 6 characters in length and randomly-generated.*	✓	✓			
5.1.1.1		Memorized Secret Authenticators	If the CSP or verifier disallows a chosen memorized secret based on its appearance on a blacklist of compromised values, the subscriber SHALL be required to choose a different memorized secret.	✓				63B#0430			*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.*	✓	✓			

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
5.1.1.1		Memorized Secret Authenticators	No other complexity requirements for memorized secrets SHOULD be imposed. A rationale for this is presented in Appendix A Strength of Memorized Secrets.					n/a								
5.1.1.2		Memorized Secret Verifiers	Verifiers SHALL require subscriber-chosen memorized secrets to be at least 8 characters in length.	✓				63B#0440			The CSP SHALL require memorized secrets chosen by the Subject to be at least 8 characters in length.	✓	✓			
5.1.1.2		Memorized Secret Verifiers	Verifiers SHOULD permit subscriber-chosen memorized secrets ...					n/a								
5.1.1.2		Memorized Secret Verifiers	... at least 64 characters in length. All printing ASCII [RFC 20] characters as well as the space character SHOULD be acceptable in memorized secrets. Unicode [ISO/ISC 10646] characters SHOULD be accepted as well. To make allowances for likely mistyping, verifiers MAY replace multiple consecutive space characters with a single space character prior to verification, provided that the result is at least 8 characters in length.					n/a								
5.1.1.2		Memorized Secret Verifiers	Truncation of the secret SHALL NOT be performed.	✓				63B#0450			The CSP SHALL NOT truncate Subject-chosen memorized secrets	✓	✓			
5.1.1.2		Memorized Secret Verifiers	For purposes of the above length requirements, each Unicode code point SHALL be counted as a single character.	✓				63B#0460			If Unicode is accepted then the CSP SHALL count each Unicode code point as a single character.	✓	✓			
5.1.1.2		Memorized Secret Verifiers	If Unicode characters are accepted in memorized secrets, the verifier SHOULD ...					n/a								
5.1.1.2		Memorized Secret Verifiers	... apply the Normalization Process for Stabilized Strings using either the NFKC or NFKD normalization defined in Section 12.1 of Unicode Standard Annex 15 [UAX 15]. This process is applied before hashing the byte string representing the memorized secret.					n/a								
5.1.1.2		Memorized Secret Verifiers	Subscribers choosing memorized secrets containing Unicode characters SHOULD be advised that some characters may be represented differently by some endpoints, which can affect their ability to authenticate successfully.					n/a								
5.1.1.2		Memorized Secret Verifiers	Memorized secrets that are randomly chosen by the CSP (e.g., at enrollment) or by the verifier (e.g., when a user requests a new PIN) SHALL be at least 6 characters in length and SHALL be generated using an approved random bit generator [SP 800-90Ar1].	✓				63B#0470			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].	✓	✓			
5.1.1.2		Memorized Secret Verifiers	Memorized secret verifiers SHALL NOT permit the subscriber to store a "hint" that is accessible to an unauthenticated claimant.	✓				63B#0480			The CSP SHALL NOT permit Subjects to store password-recollection hints.	✓	✓			
5.1.1.2		Memorized Secret Verifiers	Verifiers SHALL NOT prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing memorized secrets.	✓				63B#0490			The CSP SHALL NOT prompt Subjects in any manner when Subjects are choosing secrets	✓	✓			

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
5.1.1.2		Memorized Secret Verifiers	When processing requests to establish and change memorized secrets, verifiers SHALL compare the prospective secrets against a list that contains values known to be commonly-used, expected, or compromised.	✓				63B#0500			The CSP SHALL compare Subjects' chosen secrets against a list that contains values known to be commonly-used, expected, or compromised and if found:	✓	✓			
5.1.1.2		Memorized Secret Verifiers	For example, the list MAY include, but is not limited to: • Passwords obtained from previous breach corpuses. • Dictionary words. • Repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd'). • Context-specific words, such as the name of the service, the username, and derivatives thereof.					n/a								
5.1.1.2		Memorized Secret Verifiers	If the chosen secret is found in the list, the CSP or verifier SHALL advise the subscriber that they need to select a different secret, ...					n/a			Addressed by 63B#0380					
5.1.1.2		Memorized Secret Verifiers	... SHALL provide the reason for rejection, ...	✓				63B#0500	a)		provide the reason for rejection;	✓	✓			
5.1.1.2		Memorized Secret Verifiers	... and SHALL require the subscriber to choose a different value	✓				63B#0500	b)		require the Subject to choose another secret.	✓	✓			
5.1.1.2		Memorized Secret Verifiers	Verifiers SHOULD NOT impose other composition rules (e.g., requiring mixtures of different character types or prohibiting consecutively repeated characters) for memorized secrets.					n/a								
5.1.1.2		Memorized Secret Verifiers	Verifiers SHOULD offer guidance to the subscriber, such as a password-strength meter [Meters], to assist the user in choosing a strong memorized secret. This is particularly important following the rejection of a memorized secret on the above list as it discourages trivial modification of listed (and likely very weak) memorized secrets [Blacklists].					n/a								
5.1.1.2		Memorized Secret Verifiers	Verifiers SHALL implement a rate-limiting mechanism that ...	✓				63B#0510			The Verifier SHALL implement a rate-limiting mechanism which:	✓	✓			
5.1.1.2		Memorized Secret Verifiers	... effectively limits the number of failed authentication attempts that can be made on the subscriber's account.	✓				63B#0510	a)		protects against online guessing attacks;	✓	✓			
5.1.1.2		Memorized Secret Verifiers	as described in Section 5.2.2.	✓				63B#0510	b)		limits consecutive failed authentication attempts on a single account to no more than 100.	✓	✓			
5.1.1.2		Memorized Secret Verifiers	Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically).					n/a								
5.1.1.2		Memorized Secret Verifiers	However, verifiers SHALL force a change if there is evidence of compromise of the authenticator.	✓				63B#0520			IF there is evidence of compromise of the Claimant's authenticator the CSP SHALL require the Claimant to select a new memorized secret, consistent with 63B#0440 - '0500.	✓	✓			
5.1.1.2		Memorized Secret Verifiers	Verifiers SHOULD ... permit claimants to use "paste" functionality when entering a memorized secret. This facilitates the use of password managers, which are widely used and in many cases increase the likelihood that users will choose stronger memorized secrets.					n/a								

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
5.1.1.2		Memorized Secret Verifiers	In order to assist the claimant in successfully entering a memorized secret, the verifier SHOULD offer an option to display the secret — rather than a series of dots or asterisks — until it is entered. This allows the claimant to verify their entry if they are in a location where their screen is unlikely to be observed.					n/a								
5.1.1.2		Memorized Secret Verifiers	The verifier MAY also permit the user's device to display individual entered characters for a short time after each character is typed to verify correct entry. This is particularly applicable on mobile devices.					n/a								
5.1.1.2		Memorized Secret Verifiers	The verifier SHALL use approved encryption and an authenticated protected channel when requesting memorized secrets in order to provide resistance to eavesdropping and MitM attacks.	✓				63B#0530			The CSP SHALL use approved encryption and an authenticated protected channel when requesting memorized secrets.	✓	✓			
5.1.1.2		Memorized Secret Verifiers	Verifiers SHALL store memorized secrets in a form that is resistant to offline attacks.	✓				63B#0540			The CSP SHALL store memorized secrets in a form that is resistant to offline attacks.	✓	✓			
5.1.1.2		Memorized Secret Verifiers	Memorized secrets SHALL be salted and hashed using a suitable one-way key derivation function.	✓				63B#0550			The CSP SHALL salt and hash stored memorized secrets using an approved algorithm, ensuring that:	✓	✓			
5.1.1.2		Memorized Secret Verifiers	The salt SHALL be at least 32 bits in length and be chosen arbitrarily so as to minimize salt value collisions among stored hashes.	✓				63B#0550	a)		a randomly-chosen salt value of at least 32 bits in length is used;	✓	✓			
5.1.1.2		Memorized Secret Verifiers	Both the salt value and the resulting hash SHALL be stored for each subscriber using a memorized secret authenticator.	✓				63B#0550	b)		both the salt value and the resulting hash are stored for each subscriber using a memorized secret authenticator;	✓	✓			
5.1.1.2		Memorized Secret Verifiers	This salt value, if used, SHALL be generated by an approved random bit generator [SP 800-90Ar1] and provide at least the minimum security strength specified in the latest revision of SP 800-131A (112 bits as of the date of this publication).	✓				63B#0560			The CSP SHALL generate salt values using an approved random-bit generator [SP 800-90Ar1] which provides at least the minimum security strength specified in the latest revision of SP 800-131A.	✓	✓			
5.1.1.2		Memorized Secret Verifiers	The secret salt value SHALL be stored separately from the hashed memorized secrets (e.g., in a specialized device like a hardware security module). With this additional iteration, brute-force attacks on the hashed memorized secrets are impractical as long as the secret salt value remains secret.	✓				63B#0570			The CSP SHALL store secret salt value(s) separately from the hashed memorized secrets.	✓	✓			
5.1.1.2		Memorized Secret Verifiers	Key derivation functions take a password, a salt, and a cost factor as inputs then generate a password hash. Their purpose is to make each password guessing trial by an attacker who has obtained a password hash file expensive and therefore the cost of a guessing attack high or prohibitive. Examples of suitable key derivation functions include Password-based Key Derivation Function 2 (PBKDF2) [SP 800-132] and Balloon [BALLOON]. A memory-hard function SHOULD be used because it increases the cost of an attack.					n/a								

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
5.1.1.2		Memorized Secret Verifiers	The key derivation function SHALL use an approved one-way function such as ...	✓				63B#0570			The CSP SHALL use only approved one-way key derivation functions.	✓	✓			
5.1.1.2		Memorized Secret Verifiers	Keyed Hash Message Authentication Code (HMAC) [FIPS 198-1],					n/a							NIST guidance remark: The listed items in the source reference are not considered to be exhaustive but were the only known approved functions at the time of its drafting.	
5.1.1.2		Memorized Secret Verifiers	any approved hash function in SP 800-107,					n/a								
5.1.1.2		Memorized Secret Verifiers	Secure Hash Algorithm 3 (SHA-3) [FIPS 202],					n/a								
5.1.1.2		Memorized Secret Verifiers	CMAC [SP 800-38B] or Keccak Message Authentication Code (KMAC),					n/a								
5.1.1.2		Memorized Secret Verifiers	Customizable SHAKE (cSHAKE),					n/a								
5.1.1.2		Memorized Secret Verifiers	or ParallelHash [SP 800-185].					n/a								
5.1.1.2		Memorized Secret Verifiers	The chosen output length of the key derivation function SHOULD be the same as the length of the underlying one-way function output.					n/a								
5.1.1.2		Memorized Secret Verifiers	For PBKDF2, ...					n/a								
5.1.1.2		Memorized Secret Verifiers	?????					n/a								
5.1.1.2		Memorized Secret Verifiers	... the cost factor is an iteration count: the more times the PBKDF2 function is iterated, the longer it takes to compute the password hash. Therefore, the iteration count SHOULD be as large as verification server performance will allow, typically at least 10,000 iterations.					n/a								
5.1.1.2		Memorized Secret Verifiers	In addition, verifiers SHOULD perform an additional iteration of a key derivation function using a salt value that is secret and known only to the verifier.					n/a								
5.1.2		Look-Up Secrets	CSPs creating look-up secret authenticators SHALL use an approved random bit generator [SP 800-90Ar1] to generate the list of secrets and ...	✓				63B#0580			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;	✓	✓			
5.1.2		Look-Up Secrets	... SHALL deliver the authenticator securely to the subscriber.	✓				63B#0590			The CSP SHALL securely deliver the authenticator to the Subject .	✓	✓			
5.1.2		Look-Up Secrets	Look-up secrets SHALL have at least 20 bits of entropy.					n/a			Addressed within 63B#0580					
5.1.2.1		Look-Up Secret Authenticators	Look-up secrets MAY be distributed by the CSP in person, by postal mail to the subscriber's address of record, or by online distribution.					n/a								
5.1.2.1		Look-Up Secret Authenticators	If distributed online, look-up secrets SHALL be distributed over a secure channel in accordance with the post-enrollment binding requirements in Section 6.1.2.	✓				63B#0600			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#1400.	✓	✓			
5.1.2.1		Look-Up Secret Authenticators	If the authenticator uses look-up secrets sequentially from a list, the subscriber MAY dispose of used secrets, but only after a successful authentication.					n/a								

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
5.1.2.2		Look-Up Secret Verifiers	Verifiers of look-up secrets SHALL prompt the claimant for the next secret from their authenticator or for a specific (e.g., numbered) secret.	✓				63B#0610			The CSP SHALL prompt the Claimant for the next secret from their authenticator or for a specific (e.g., numbered) secret.	✓	✓			
5.1.2.2		Look-Up Secret Verifiers	A given secret from an authenticator SHALL be used successfully only once.	✓				63B#0620			The CSP SHALL succesfully use a secret from an authenticator list only once.	✓	✓			
5.1.2.2		Look-Up Secret Verifiers	If the look-up secret is derived from a grid card, each cell of the grid SHALL be used only once.	✓				63B#0630			IF a look-up secret is derived from a grid card, the CSP SHALL use each cell of the grid only once.	✓	✓			
5.1.2.2		Look-Up Secret Verifiers	Verifiers SHALL store look-up secrets in a form that is resistant to offline attacks.	✓				63B#0640			The CSP SHALL store look-up secrets in a form that is resistant to offline attacks.	✓	✓			
5.1.2.2		Look-Up Secret Verifiers	Look-up secrets having at least 112 bits of entropy SHALL be hashed with an approved one-way function as described in Section 5.1.1.2.	✓				63B#0650			IF a look-up secret has at least 112 bits of entropy the CSP SHALL hash the secret iaw 63B#0550	✓	✓			
5.1.2.2		Look-Up Secret Verifiers	Look-up secrets with fewer than 112 bits of entropy SHALL be salted and hashed using a suitable one-way key derivation function, also described in Section 5.1.1.2.	✓				63B#0660			IF a look-up secret has fewer than 112 bits of entropy the CSP SHALL hash the secret iaw 63B#0550	✓	✓			
5.1.2.2		Look-Up Secret Verifiers	The salt value SHALL be at least 32 in bits in length and arbitrarily chosen so as to minimize salt value collisions among stored hashes.	✓				63B#0670			The CSP SHALL use an arbitrarily-chosen salt value of at least 32 bits length.	✓	✓			
5.1.2.2		Look-Up Secret Verifiers	Both the salt value and the resulting hash SHALL be stored for each look-up secret.	✓				63B#0680			The CSP SHALL, for each look-up secret, store the salt value and the resulting hash.	✓	✓			
5.1.2.2		Look-Up Secret Verifiers	For look-up secrets that have less than 64 bits of entropy, the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account as described in Section 5.2.2.	✓				63B#0690			IF a look-up secret has fewer than 64 bits of entropy the CSP SHALL enforce a rate-limiting mechanism iaw 63B#0510	✓	✓			
5.1.2.2		Look-Up Secret Verifiers	The verifier SHALL use approved encryption and an authenticated protected channel when requesting look-up secrets in order to provide resistance to eavesdropping and MitM attacks.	✓				63B#0700			The CSP SHALL use approved encryption and an authenticated protected channel when requesting look-up secrets.	✓	✓			
5.1.3		Out-of-Band Devices						n/a								
5.1.3.1		Out-of-Band Authenticators	The out-of-band authenticator SHALL establish a separate channel with the verifier in order to retrieve the out-of-band secret or authentication request.	✓				63B#0710			The CSP SHALL establish a separate channel with the Claimant's OOB authenticator in order to retrieve out-of-band secrets or authentication requests.	✓	✓			
5.1.3.1		Out-of-Band Authenticators	This channel is considered to be out-of-band with respect to the primary communication channel (even if it terminates on the same device) provided the device does not leak information from one channel to the other without the authorization of the claimant.					n/a								
5.1.3.1		Out-of-Band Authenticators	The out-of-band device SHOULD be uniquely addressable and …					n/a								
5.1.3.1		Out-of-Band Authenticators	Methods that do not prove possession of a specific device, such as voice-over-IP (VOIP) or email, SHALL NOT be used for out-of-band authentication.	✓				63B#0720			When performing out-of-band authentication the CSP SHALL use an authentication method which positively establishes the Claimant's possession of a specific device.	✓	✓			
5.1.3.1		Out-of-Band Authenticators	The out-of-band authenticator SHALL uniquely authenticate itself in one of the following ways when communicating with the verifier:	✓				63B#0730			The CSP SHALL ensure that the Claimant's authentictor is positively authenticated by one of the following ways:	✓	✓			

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
5.1.3.1		Out-of-Band Authenticators	• Establish an authenticated protected channel to the verifier using approved cryptography. The key used SHALL be stored in suitably secure storage available to the authenticator application (e.g., keychain storage, TPM, TEE, secure element).	✓				63B#0730	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;	✓	✓			
5.1.3.1		Out-of-Band Authenticators	• Authenticate to a public mobile telephone network using a SIM card or equivalent that uniquely identifies the device. This method SHALL only be used if a secret is being sent from the verifier to the out-of-band device via the PSTN (SMS or voice).	✓				63B#0730	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.	✓	✓			
5.1.3.1		Out-of-Band Authenticators	If a secret is sent by the verifier to the out-of band device, the device SHOULD NOT display the authentication secret while it is locked by the owner (i.e., requires an entry of a PIN, passcode, or biometric to view).					n/a								
5.1.3.1		Out-of-Band Authenticators	However, authenticators SHOULD indicate the receipt of an authentication secret on a locked device.					n/a								
5.1.3.1		Out-of-Band Authenticators	If the out-of-band authenticator sends an approval message over the secondary communication channel — rather than by the claimant transferring a received secret to the primary communication channel — it SHALL do one of the following:	✓				63B#0740			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:	✓	✓			
5.1.3.1		Out-of-Band Authenticators	· The authenticator SHALL accept transfer of the secret from the primary channel which it SHALL send to the verifier over the secondary channel to associate the approval with the authentication transaction. The claimant MAY perform the transfer manually or use a technology such as a barcode or QR code to effect the transfer.	✓				63B#0740	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	✓	✓			
5.1.3.1		Out-of-Band Authenticators	· The authenticator SHALL present a secret received via the secondary channel from the verifier and prompt the claimant to verify the consistency of that secret with the primary channel, ...	✓				63B#0740	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:	✓	✓			
5.1.3.1		Out-of-Band Authenticators	. ... prior to accepting a yes/no response from the claimant.	✓				63B#0740	b)	i)	the OOB Authenticator accepts a 'yes/no' response from the Claimant;	✓	✓			
5.1.3.1		Out-of-Band Authenticators	. ... It SHALL then send that response to the verifier.	✓				63B#0740	b)	ii)	the OOB Authenticator sends that response to the CSP	✓	✓			
5.1.3.2		Out-of-Band Verifiers	For additional verification requirements specific to the PSTN, see Section 5.1.3.3.					n/a								
5.1.3.2		Out-of-Band Verifiers	If out-of-band verification is to be made using a secure application, such as on a smart phone, the verifier MAY send a push notification to that device. The verifier then waits for the establishment of an authenticated protected channel and verifies the authenticator's identifying key.					n/a								

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
5.1.3.2		Out-of-Band Verifiers	The verifier SHALL NOT store the identifying key itself, but SHALL use a verification method (e.g., an approved hash function or proof of possession of the identifying key) to uniquely identify the authenticator. Once authenticated, the verifier transmits the authentication secret to the authenticator.	✓				63B#0750			The CSP SHALL use a verification method to securely and uniquely identify the Claimant's authenticator without storing the actual identifying key.	✓	✓			
5.1.3.2		Out-of-Band Verifiers	Depending on the type of out-of-band authenticator, one of the following SHALL take place:	✓				63B#0760			The CSP SHALL, according to the type of OOB authenticator used, effect one of the following three options:.	✓	✓			
5.1.3.2		Out-of-Band Verifiers	· Transfer of secret to primary channel: The verifier MAY signal the device containing the subscriber's authenticator to indicate readiness to authenticate. It SHALL then transmit a random secret to the out-of-band authenticator. The verifier SHALL then wait for the secret to be returned on the primary communication channel.					63B#0760	a)		Transferring the secret to the primary channel; OR					
5.1.3.2		Out-of-Band Verifiers	· Transfer of secret to secondary channel: The verifier SHALL display a random authentication secret to the claimant via the primary channel. It SHALL then wait for the secret to be returned on the secondary channel from the claimant's out-of-band authenticator.	✓				63B#0760	b)		transferring the secret via the secondary channel by transmitting a random authentication secret to the Claimant via the primary channel and then waiting for the secret to be returned from the Claimant's OOB authenticator via the secondary channel; OR	✓	✓			
5.1.3.2		Out-of-Band Verifiers	· Verification of secrets by claimant: The verifier SHALL display a random authentication secret to the claimant via the primary channel, and SHALL send the same secret to the out-of-band authenticator via the secondary channel for presentation to the claimant. It SHALL then wait for an approval (or disapproval) message via the secondary channel.	✓				63B#0760	c)		requiring the Claimant to verify the secret by sending a random authentication secret to the claimant via the primary channel, and also to their OOB authenticator via the secondary channel and then waiting for an approval (or disapproval) message via the secondary channel	✓	✓			
5.1.3.2		Out-of-Band Verifiers	In all cases, the authentication SHALL be considered invalid if not completed within 10 minutes.	✓				63B#0770			The CSP SHALL time-out and fail the authentication process if no response is received within 10 minutes of its initiation	✓	✓			
5.1.3.2		Out-of-Band Verifiers	In order to provide replay resistance as described in Section 5.2.8, verifiers SHALL accept a given the authentication secret only once during the validity period.	✓				63B#0780			The CSP SHALL accept a given authentication secret only once during its validity period.	✓	✓			
5.1.3.2		Out-of-Band Verifiers	The verifier SHALL generate random authentication secrets with at least 20 bits of entropy using an approved random bit generator [SP 800-90Ar1].	✓				63B#0790			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;	✓	✓			
5.1.3.2		Out-of-Band Verifiers	If the authentication secret has less than 64 bits of entropy, the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account as described in Section 5.2.2.	✓				63B#0800			IF an authentication secret has fewer than 64 bits of entropy the CSP SHALL enforce a rate-limiting mechanism iaw 63B#0510	✓	✓			
5.1.3.3		Authentication using the Public Switched Telephone Network	Use of the PSTN for out-of-band verification is RESTRICTED as described in this section and in Section 5.2.10.					n/a								

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
5.1.3.3		Authentication using the Public Switched Telephone Network	If out-of-band verification is to be made using the PSTN, the verifier SHALL verify that the pre-registered telephone number being used is associated with a specific physical device.	✓				63B#0810			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.	✓	✓			
5.1.3.3		Authentication using the Public Switched Telephone Network	Changing the pre-registered telephone number is considered to be the binding of a new authenticator and SHALL only occur as described in Section 6.1.2.	✓				63B#0820			IF the CSP allows the Subject to register a new 'phone number as an authenticator it shall do so in a manner which fulfills the criteria in 63B#1800 & '1810.	✓	✓			
5.1.3.3		Authentication using the Public Switched Telephone Network	Verifiers SHOULD consider risk indicators such as device swap, SIM change, number porting, or other abnormal behavior before using the PSTN to deliver an out-of-band authentication secret.					n/a								
		Single-Factor OTP Device	The secret key and its algorithm SHALL provide at least the minimum security strength specified in the latest revision of SP 800-131A (112 bits as of the date of this publication).	✓				63B#0830			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.	✓	✓			
5.1.4.1		Single-Factor OTP Authenticators	The nonce SHALL be of sufficient length to ensure that it is unique for each operation of the device over its lifetime.	✓				63B#0840			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.	✓	✓			
5.1.4.1		Single-Factor OTP Authenticators	OTP authenticators — particularly software-based OTP generators — SHOULD discourage and SHALL NOT facilitate the cloning of the secret key onto multiple devices.	✓				63B#0850			Thd CSP SHALL ensure that it uses SF-OTP Devices which do not facilitate the cloning of the secret key onto multiple devices.	✓	✓			
5.1.4.1		Single-Factor OTP Authenticators	The authenticator output is obtained by using an approved block cipher or hash function to combine the key and nonce in a secure manner. The authenticator output MAY be truncated to as few as 6 decimal digits (approximately 20 bits of entropy).					n/a								
5.1.4.1		Single-Factor OTP Authenticators	If the nonce used to generate the authenticator output is based on a real-time clock, the nonce SHALL be changed at least once every 2 minutes.	✓				63B#0860			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.	✓	✓			
5.1.4.1		Single-Factor OTP Authenticators	The OTP value associated with a given nonce SHALL be accepted only once.	✓				63B#0870			The CSP SHALL ensure that,the OTP value associated with a given nonce is accepted only once.	✓	✓			
5.1.4.2		Single-Factor OTP Verifiers	Single-factor OTP verifiers effectively duplicate the process of generating the OTP used by the authenticator. As such, the symmetric keys used by authenticators are also present in the verifier, and SHALL be strongly protected against compromise.	✓				63B#0880			The CSP SHALL employ techniques which strongly protect against compromise of symmetric keys used by authenticators.	✓	✓		The CSP should present a case for their protection warranting a claim of being 'strong'.	
5.1.4.2		Single-Factor OTP Verifiers	When a single-factor OTP authenticator is being associated with a subscriber account, the verifier or associated CSP SHALL use approved cryptography to either ...	✓				63B#0890			The CSP SHALL use approved cryptography to ensure that a Subject's SF-OTP authenticator to either:	✓	✓			
5.1.4.2		Single-Factor OTP Verifiers	generate and exchange OR ...	✓				63B#0890	a)		generate and exchange the secrets required to duplicate the authenticator output.	✓	✓			
			... to obtain the secrets required to duplicate the authenticator output.	✓				63B#0890	b		obtain the secrets required to duplicate the authenticator output; OR	✓	✓			
5.1.4.2		Single-Factor OTP Verifiers	The verifier SHALL use approved encryption and an authenticated protected channel when collecting the OTP in order to provide resistance to eavesdropping and MitM attacks.	✓				63B#0900			The CSP SHALL use approved encryption and an authenticated protected channel when retrieving the OTP.	✓	✓			

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
5.1.4.2		Single-Factor OTP Verifiers	Time-based OTPs [RFC 6238] SHALL have a defined lifetime that is determined by	✓				63B#0910			The CSP SHALL ensure that, when using time-based OTPs [RFC238], their lifetime is determined taking into account:	✓	✓			
5.1.4.2		Single-Factor OTP Verifiers	the expected clock drift — in either direction — of the authenticator over its lifetime, plus ...	✓				63B#0910	a)		the expected clock drift (in either direction) of the authenticator over its lifetime;	✓	✓			
5.1.4.2		Single-Factor OTP Verifiers	allowance for network delay and ...	✓				63B#0910	b)		allowance for network delay;	✓	✓			
5.1.4.2		Single-Factor OTP Verifiers	user entry of the OTP.	✓				63B#0910	c)		an allowance for user entry of the OTP.	✓	✓			
5.1.4.2		Single-Factor OTP Verifiers	In order to provide replay resistance as described in Section 5.2.8, verifiers SHALL accept a given time-based OTP only once during the validity period.	✓				63B#0920			The CSP SHALL accept a given time-based OTP only once during its validity period.	✓	✓			
5.1.4.2		Single-Factor OTP Verifiers	If the authenticator output has less than 64 bits of entropy, the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account as described in Section 5.2.2.	✓				63B#0930			IF an authentication secret has fewer than 64 bits of entropy the CSP SHALL enforce a rate-limiting mechanism iaw 63B#0510	✓	✓			
5		Multi-Factor OTP Devices	Multi-factor OTP authenticators operate in a similar manner to single-factor OTP authenticators (see Section 5.1.4.1), except that they require the entry of either a memorized secret or the use of a biometric to obtain the OTP from the authenticator. Each use of the authenticator SHALL require the input of the additional factor.	✓				63B#0940			The CSP shall ensure that each use of a MF-OTP authenticator equires both factors to be input	✓	✓			
5.1.5.1		Multi-Factor OTP Authenticators	In addition to activation information, multi-factor OTP authenticators contain two persistent values. The first is a symmetric key that persists for the device's lifetime. The second is a nonce that is either changed each time the authenticator is used or is based on a real-time clock.					n/a								
5.1.5.1		Multi-Factor OTP Authenticators	The secret key and its algorithm SHALL provide at least the minimum security strength specified in the latest revision of SP 800-131A (112 bits as of the date of this publication).	✓				63B#0950			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.	✓	✓			
5.1.5.1		Multi-Factor OTP Authenticators	The nonce SHALL be of sufficient length to ensure that it is unique for each operation of the device over its lifetime.	✓				63B#0960			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.	✓	✓			
5.1.5.1		Multi-Factor OTP Authenticators	OTP authenticators — particularly software-based OTP generators — SHOULD discourage and SHALL NOT facilitate the cloning of the secret key onto multiple devices.	✓				63B#0970			Thd CSP SHALL ensure that it uses MF-OTP Devices which do not facilitate the cloning of the secret key onto multiple devices.	✓	✓			
5.1.5.1		Multi-Factor OTP Authenticators	The authenticator output is obtained by using an approved block cipher or hash function to combine the key and nonce in a secure manner. The authenticator output MAY be truncated to as few as 6 decimal digits (approximately 20 bits of entropy).					n/a								
5.1.5.1		Multi-Factor OTP Authenticators	If the nonce used to generate the authenticator output is based on a real-time clock, the nonce SHALL be changed at least once every 2 minutes.	✓				63B#0980			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.	✓	✓			

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
5.1.5.1		Multi-Factor OTP Authenticators	The OTP value associated with a given nonce SHALL be accepted only once.	✓				63B#0990			The CSP SHALL ensure that,the OTP value associated with a given nonce is accepted only once.	✓	✓			
5.1.5.1		Multi-Factor OTP Authenticators	A memorized secret used by the authenticator for activation SHALL be a randomly-chosen numeric secret at least 6 decimal digits in length or other memorized secret of comparable complexity as described in Section 5.1.1.2 ...	✓				63B#1000			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	✓	✓			
5.1.5.1		Multi-Factor OTP Authenticators	.. and SHALL be rate limited as specified in Section 5.2.2.	✓				63B#1010			The CSP SHALL enforce a rate-limiting mechanism iaw 63B#1450 & '1460 (without qualification regarding the degree of entropy the memorized secret exhibits).	✓	✓			
5.1.5.1		Multi-Factor OTP Authenticators	A biometric activation factor SHALL meet the requirements of Section 5.2.3, including limits on the number of consecutive authentication failures.	✓				63B#1020			If a biometric factor is used in an authentication the CSP SHALL ensure that all criteria 63B#1470 - '1550 are fulfilled.	✓	✓			
5.1.5.1		Multi-Factor OTP Authenticators	The unencrypted secret key and activation secret or biometric sample (and any biometric data derived from the biometric sample such as a probe produced through signal processing) SHALL be zeroized immediately after an OTP has been generated.	✓				63B#1030			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.	✓	✓			
5.1.5.2		Multi-Factor OTP Verifiers	Multi-factor OTP verifiers effectively duplicate the process of generating the OTP used by the authenticator, but without the requirement that a second factor be provided. As such, the symmetric keys used by authenticators SHALL be strongly protected against compromise.	✓				63B#1040			The CSP SHALL ensure that MF-OTP authenticators strongly protected against compromise the associated symmetric keys.	✓	✓			
5.1.5.2		Multi-Factor OTP Verifiers	When a multi-factor OTP authenticator is being associated with a subscriber account, the verifier or associated CSP SHALL use approved cryptography to either ...	✓				63B#1050			The CSP SHALL use approved cryptography to ensure that a Subject's MF-OTP authenticator to either:	✓	✓			
5.1.5.2		Multi-Factor OTP Verifiers	... generate and exchange OR ...	✓				63B#1050	a)		generate and exchange the secrets required to duplicate the authenticator output; OR	✓	✓			
5.1.5.2		Multi-Factor OTP Verifiers	... to obtain the secrets required to duplicate the authenticator output.	✓				63B#1050	b)		obtain the secrets required to duplicate the authenticator output.	✓	✓			
5.1.5.2		Multi-Factor OTP Verifiers	The verifier or CSP SHALL also establish, via the authenticator source, that the authenticator is a multi-factor device.	✓				63B#1060			The CSP SHALL treat all authenticators as being single-factor devices unelss they establish, via the authenticator source, that the authenticator device is multi-factor.	✓	✓			
5.1.5.2		Multi-Factor OTP Verifiers	In the absence of a trusted statement that it is a multi-factor device, the verifier SHALL treat the authenticator as single-factor, in accordance with Section 5.1.4.	✓				63B#1070			Unless it is able to rely upon a statement via the authenticator source that a device is multi-factor the CSP SHALL treat the authenticator as if it was single-factor.	✓	✓			
5.1.5.2		Multi-Factor OTP Verifiers	The verifier SHALL use approved encryption and an authenticated protected channel when collecting the OTP in order to provide resistance to eavesdropping and MitM attacks.	✓				63B#1080			The CSP SHALL ensure that all communication between the Claimant and Verifier use approved encryption and is via an authenticated protected channel.	✓	✓			
5.1.5.2		Multi-Factor OTP Verifiers	Time-based OTPs [RFC 6238] SHALL have a defined lifetime that is determined by	✓				63B#1090			The CSP SHALL use verification methods which ensure that, when using time-based OTPs [RFC238], their lifetime is determined taking into account:	✓	✓			
5.1.5.2		Multi-Factor OTP Verifiers	the expected clock drift — in either direction — of the authenticator over its lifetime, plus ...	✓				63B#1090	a)		the expected clock drift (in either direction) of the authenticator over its lifetime;	✓	✓			
5.1.5.2		Multi-Factor OTP Verifiers	allowance for network delay and ...	✓				63B#1090	b)		allowance for network delay;	✓	✓			

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
5.1.5.2		Multi-Factor OTP Verifiers	user entry of the OTP.	✓				63B#1090	c)		an allowance for user entry of the OTP.	✓	✓			
5.1.5.2		Multi-Factor OTP Verifiers	In order to provide replay resistance as described in Section 5.2.8, verifiers SHALL accept a given time-based OTP only once during the validity period.	✓				63B#1100			The CSP SHALL accept a given time-based OTP only once during its validity period.	✓	✓			
5.1.5.2		Multi-Factor OTP Verifiers	In the event a claimant's authentication is denied due to duplicate use of an OTP, verifiers MAY warn the claimant in case an attacker has been able to authenticate in advance. Verifiers MAY also warn a subscriber in an existing session of the attempted duplicate use of an OTP.					n/a								
5.1.5.2		Multi-Factor OTP Verifiers	If the authenticator output or activation secret has less than 64 bits of entropy, the verifier SHALL implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber's account as described in Section 5.2.2.	✓				63B#1110			IF an authentication output or activation secret has fewer than 64 bits of entropy the CSP SHALL enforce a rate-limiting mechanism iaw 63B#0510	✓	✓			
5.1.5.2		Multi-Factor OTP Verifiers	A biometric activation factor SHALL meet the requirements of Section 5.2.3, including limits on the number of consecutive authentication failures.	✓				63B#1120			If a biometric factor is used in an authentication the CSP SHALL ensure that all criteria 63B#1470 - '1550 are fulfilled.	✓	✓			
		Single-Factor Cryptographic Software	Single-factor software cryptographic authenticators encapsulate a secret key that is unique to the authenticator. The key SHALL be stored in suitably secure storage available to the authenticator application (e.g., keychain storage, TPM, or TEE if available).	✓				63B#1130			The CSP SHALL ensure that SF-CS keys are stored in suitably secure storage available to the authenticator application.	✓	✓			
5.1.6.1		Single-Factor Cryptographic Software Authenticators	The key SHALL be 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.	✓				63B#1140			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.	✓	✓			
5.1.6.1		Single-Factor Cryptographic Software Authenticators	Single-factor cryptographic software authenticators SHOULD discourage and SHALL NOT facilitate the cloning of the secret key onto multiple devices.	✓				63B#1150			The CSP SHALL ensure that SF-CS key authenticators DO NOT facilitate the cloning of the secret key onto multiple devices.	✓	✓			
5.1.6.2		Single-Factor Cryptographic Software Verifiers	The requirements for a single-factor cryptographic software verifier are identical to those for a single-factor cryptographic device verifier, described in Section 5.1.7.2.	✓				63B#1160			Criteria 63B#1210 to '1240 SHALL be fulfilled.	✓	✓			
5		Single-Factor Cryptographic Devices	Single-factor cryptographic device authenticators encapsulate a secret key that is unique to the device and SHALL NOT be exportable (i.e., it cannot be removed from the device).	✓				63B#1170			The CSP SHALL use SF-CD authenticators that are incapable of exporting their [unique] secret key.	✓	✓			

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
5.1.7.1		Single-Factor Cryptographic Device Authenticators	The authenticator operates by signing a challenge nonce presented through a direct computer interface (e.g., a USB port). Alternatively, the authenticator could be a suitably secure processor integrated with the user endpoint itself (e.g., a hardware TPM). Although cryptographic devices contain software, they differ from cryptographic software authenticators in that all embedded software is under control of the CSP or issuer and that the entire authenticator is subject to all applicable FIPS 140 requirements at the AAL being authenticated.					n/a								
5.1.7.1		Single-Factor Cryptographic Device Authenticators	The secret key and its algorithm SHALL provide at least the minimum security length specified in the latest revision of SP 800-131A (112 bits as of the date of this publication).	✓				63B#1180			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.	✓	✓			
5.1.7.1		Single-Factor Cryptographic Device Authenticators	The challenge nonce SHALL be at least 64 bits in length.	✓				63B#1190			The CSP SHALL use SF-CD authenticators which employ a nonce of at least 64 bits length.	✓	✓			
5.1.7.1		Single-Factor Cryptographic Device Authenticators	Approved cryptography SHALL be used.	✓				63B#1200			The CSP SHALL use SF-CD Devices that use approved cryptography	✓	✓			
5.1.7.1		Single-Factor Cryptographic Device Authenticators	Single-factor cryptographic device authenticators SHOULD require a physical input (e.g., the pressing of a button) in order to operate. This provides defense against unintended operation of the device, which might occur if the endpoint to which it is connected is compromised.					n/a								
5.1.7.2		Single-Factor Cryptographic Device Verifiers	Single-factor cryptographic device verifiers generate a challenge nonce, send it to the corresponding authenticator, and use the authenticator output to verify possession of the device. The authenticator output is highly dependent on the specific cryptographic device and protocol, but it is generally some type of signed message.					n/a								
5.1.7.2		Single-Factor Cryptographic Device Verifiers	The verifier has either symmetric or asymmetric cryptographic keys corresponding to each authenticator. While both types of keys SHALL be protected against modification, ...	✓				63B#1210			The CSP SHALL use verification methods which protect any secret keys against modification.	✓	✓			
5.1.7.2		Single-Factor Cryptographic Device Verifiers	... symmetric keys SHALL additionally be protected against unauthorized disclosure.	✓				63B#1220			The CSP SHALL use verification methods which protect symmetric secret keys against unauthorized disclosure.	✓	✓			
5.1.7.2		Single-Factor Cryptographic Device Verifiers	The challenge nonce SHALL be ...	✓				63B#1230			The CSP SHALL use verification methods for which the nonce is:	✓	✓			
5.1.7.2		Single-Factor Cryptographic Device Verifiers	... at least 64 bits in length, ...	✓				63B#1230	a)		at least 64 bits in length; AND	✓	✓			
5.1.7.2		Single-Factor Cryptographic Device Verifiers	... and SHALL either be ...	✓				63B#1230	b)		either:	✓	✓			

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
5.1.7.2		Single-Factor Cryptographic Device Verifiers	... unique over the authenticator's lifetime or ...	✓				63B#1230	b)	i)	unique over the authenticator's lifetime; OR	✓	✓			
5.1.7.2		Single-Factor Cryptographic Device Verifiers	... statistically unique (i.e., generated using an approved random bit generator [SP 800-90Ar1]).	✓				63B#1230	b)	ii)	generated using an approved random bit generator [SP 800-90Ar1]	✓	✓			
5.1.7.2		Single-Factor Cryptographic Device Verifiers	The verification operation SHALL use approved cryptography.	✓				63B#1240			The CSP's verification methods SHALL use approved cryptography.	✓	✓			
5.1.8		Multi-Factor Cryptographic Software						n/a								
5.1.8		Multi-Factor Cryptographic Software	A multi-factor software cryptographic authenticator is a cryptographic key stored on disk or some other "soft" media that requires activation through a second factor of authentication. Authentication is accomplished by proving possession and control of the key. The authenticator output is highly dependent on the specific cryptographic protocol, but it is generally some type of signed message. The multi-factor software cryptographic authenticator is *something you have* , and it SHALL be activated by either *something you know* or *something you are* .	✓				63B#1250			The CSP SHALL ensure that MF-CS authenticators are activated by *either* something [the Claimant] knows *or* something [the Claimant] is.	✓	✓			
5.1.8.1		Multi-Factor Cryptographic Software Authenticators	Multi-factor software cryptographic authenticators encapsulate a secret key that is unique to the authenticator and is accessible only through the input of an additional factor, either a memorized secret or a biometric. The key SHOULD be stored in suitably secure storage available to the authenticator application (e.g., keychain storage, TPM, TEE).					n/a								
5.1.8.1		Multi-Factor Cryptographic Software Authenticators	The key SHALL be 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.	✓				63B#1260			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.	✓	✓			
5.1.8.1		Multi-Factor Cryptographic Software Authenticators	Multi-factor cryptographic software authenticators SHOULD discourage and SHALL NOT facilitate the cloning of the secret key onto multiple devices.	✓				63B#1270			The CSP SHALL ensure that MF-CS key authenticators DO NOT facilitate the cloning of the secret key onto multiple devices.	✓	✓			
5.1.8.1		Multi-Factor Cryptographic Software Authenticators	Each authentication operation using the authenticator SHALL require the input of both factors.	✓				63B#1280			The CSP SHALL ensure that MF-CS key authenticators require the input of all factors before performing the authentication operation.	✓	✓			
5.1.8.1		Multi-Factor Cryptographic Software Authenticators	Any memorized secret used by the authenticator for activation SHALL be a randomly-chosen numeric value at least 6 decimal digits in length, or equivalent complexity, and ...	✓				63B#1290			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#0410 - '0450.	✓	✓			
5.1.8.1		Multi-Factor Cryptographic Software Authenticators	... SHALL be rate limited as specified in Section 5.2.2.	✓				63B#1300			The CSP SHALL enforce a rate-limiting mechanism iaw 63B#1450 & '1460 (without qualification regarding the degree of entropy which the memorized secret exhibits).	✓	✓			
5.1.8.1		Multi-Factor Cryptographic Software Authenticators	A biometric activation factor SHALL meet the requirements of Section 5.2.3, and SHALL include limits on the allowable number of consecutive authentication failures.	✓				63B#1310			If a biometric factor is used in an authentication the CSP SHALL ensure that all criteria 63B#1470 - '1550 are fulfilled.	✓	✓			

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag		index	KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
5.1.8.1		Multi-Factor Cryptographic Software Authenticators	The unencrypted key and activation secret or biometric sample — and any biometric data derived from the biometric sample such as a probe produced through signal processing — SHALL be zeroized immediately after an authentication transaction has taken place.	✓				63B#1320			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.	✓	✓			
5.1.8.2		Multi-Factor Cryptographic Software Verifiers	The requirements for a multi-factor cryptographic software verifier are identical to those for a single-factor cryptographic device verifier, described in Section 5.1.7.2. Verification of the output from a multi-factor cryptographic software authenticator proves use of the activation factor.	✓				63B#1330			Criteria 63B#1040 to '1070 SHALL be fulfilled.	✓	✓			
5.1.9		Multi-Factor Cryptographic Devices	A multi-factor cryptographic device is a hardware device that performs cryptographic operations using one or more protected cryptographic keys and requires activation through a second authentication factor. Authentication is accomplished by proving possession of the device and control of the key. The authenticator output is provided by direct connection to the user endpoint and is highly dependent on the specific cryptographic device and protocol, but it is typically some type of signed message. The multi-factor cryptographic device is *something you have* , and it SHALL be activated by either *something you know* or *something you are* .	✓				63B#1340			The CSP SHALL ensure that MF-CS authenticators are activated by *either* something [the Claimant] knows *or* something [the Claimant] is.	✓	✓			
5.1.9.1		Multi-Factor Cryptographic Device Authenticators	*... informative preamble (excised) ...*					n/a								
5.1.9.1		Multi-Factor Cryptographic Device Authenticators	The secret key and its algorithm SHALL provide at least the minimum security length specified in the latest revision of SP 800-131A (112 bits as of the date of this publication).	✓				63B#1350			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.	✓	✓			
5.1.9.1		Multi-Factor Cryptographic Device Authenticators	The challenge nonce SHALL be at least 64 bits in length.	✓				63B#1360			The CSP SHALL use MF-CD authenticators which employ a nonce of at least 64 bits length.	✓	✓			
5.1.9.1		Multi-Factor Cryptographic Device Authenticators	Approved cryptography SHALL be used.	✓				63B#1370			The CSP SHALL use MF-CD Devices that use approved cryptography	✓	✓			
5.1.9.1		Multi-Factor Cryptographic Device Authenticators	Each authentication operation using the authenticator SHOULD require the input of the additional factor. Input of the additional factor MAY be accomplished via either direct input on the device or via a hardware connection (e.g., USB, smartcard).					n/a								
5.1.9.1		Multi-Factor Cryptographic Device Authenticators	Any memorized secret used by the authenticator for activation SHALL be a randomly-chosen numeric value at least 6 decimal digits in length or other memorized secret meeting the requirements of Section 5.1.1.2 and ...	✓				63B#1380			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#0410 - '0450.	✓	✓			

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
5.1.9.1		Multi-Factor Cryptographic Device Authenticators	... SHALL be rate limited as specified in Section 5.2.2.	✓				63B#1390			The CSP SHALL enforce a rate-limiting mechanism iaw 63B#0510 (without qualification regarding the degree of entropy the memorized secret exhibits).	✓	✓			
5.1.9.1		Multi-Factor Cryptographic Device Authenticators	A biometric activation factor SHALL meet the requirements of Section 5.2.3, and SHALL include limits on the number of consecutive authentication failures.	✓				63B#1400			If a biometric factor is used in an authentication the CSP SHALL ensure that all criteria 63B#1470 - '1550 are fulfilled.	✓	✓			
5.1.9.1		Multi-Factor Cryptographic Device Authenticators	The unencrypted key and activation secret or biometric sample — and any biometric data derived from the biometric sample such as a probe produced through signal processing — SHALL be overwritten in memory immediately after an authentication transaction has taken place.	✓				63B#1410			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.	✓	✓			
5.1.9.2		Multi-Factor Cryptographic Device Verifiers	The requirements for a multi-factor cryptographic device verifier are identical to those for a single-factor cryptographic device verifier, described in Section 5.1.7.2. Verification of the authenticator output from a multi-factor cryptographic device proves use of the activation factor.	✓				63B#1420			Criteria 63B#1040 to '1070 SHALL be fulfilled.	✓	✓			
5.2		General Authenticator Requirements						n/a								
5.2.1		Physical Authenticators	CSPs SHALL provide subscriber instructions on how to appropriately protect the authenticator against theft or loss.	✓				63B#1430			The CSP SHALL provide Subjects instructions on how to appropriately protect the authenticator against theft or loss.	✓	✓			
5.2.1		Physical Authenticators	The CSP SHALL provide a mechanism to revoke or suspend the authenticator immediately upon notification from subscriber that loss or theft of the authenticator is suspected.	✓				63B#1440			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.	✓	✓			
5.2.2		Rate Limiting (Throttling)	When required by the authenticator type descriptions in Section 5.1, the verifier SHALL implement controls to protect against online guessing attacks.	✓				63B#1450			The CSP SHALL implement controls to protect against online guessing attacks.	✓	✓			
5.2.2		Rate Limiting (Throttling)	Unless otherwise specified in the description of a given authenticator, the verifier SHALL limit consecutive failed authentication attempts on a single account to no more than 100.	✓				63B#1460			The CSP SHALL limit consecutive failed authentication attempts on a single account to no more than 100.	✓	✓			
5.2.2		Rate Limiting (Throttling)	Additional techniques MAY be used to reduce the likelihood that an attacker will lock the legitimate claimant out as a result of rate limiting. These include:					n/a								
5.2.2		Rate Limiting (Throttling)	· Requiring the claimant to complete a CAPTCHA before attempting authentication.					n/a								
5.2.2		Rate Limiting (Throttling)	· Requiring the claimant to wait following a failed attempt for a period of time that increases as the account approaches its maximum allowance for consecutive failed attempts (e.g., 30 seconds up to an hour).					n/a								
5.2.2		Rate Limiting (Throttling)	· Accepting only authentication requests that come from a white list of IP addresses from which the subscriber has been successfully authenticated before.					n/a								

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
5.2.2		Rate Limiting (Throttling)	· Leveraging other risk-based or adaptive authentication techniques to identify user behavior that falls within, or out of, typical norms.					n/a								
5.2.2		Rate Limiting (Throttling)	When the subscriber successfully authenticates, the verifier SHOULD disregard any previous failed attempts for that user from the same IP address.					n/a								
5.2.3		Use of Biometrics	*... informative preamble (excised) ...*					n/a								
5.2.3		Use of Biometrics	Biometrics SHALL be used only as part of multi-factor authentication with a physical authenticator (*something you have*).	✓				63B#1470			*The CSP SHALL only use biometric techniques as part of a multi-factor authentication which requires the Claimant to utilise a physical authenticator.*	✓	✓			
5.2.3		Use of Biometrics	An authenticated protected channel between sensor (or an endpoint containing a sensor that resists sensor replacement) and verifier SHALL be established and ...	✓				63B#1480			*When using biometrics for authentication, the CSP SHALL establish an authenticated protected channel between the sensor (or an endpoint containing a sensor that resists sensor replacement) and the verifier.*	✓	✓			
5.2.3		Use of Biometrics	... the sensor or endpoint SHALL be established and the sensor or endpoint authenticated prior to capturing the biometric sample from the claimant.	✓				63B#1490			*When using biometrics for authentication, the CSP SHALL ensure that the sensor or endpoint is authenticated prior to capturing the biometric sample from the Claimant.*	✓	✓			
5.2.3		Use of Biometrics	The biometric system SHALL ...	✓				63B#1500			*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.	✓				63B#1500	*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 in ISO/IEC 30107-1.	✓				63B#1500	*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	The biometric system SHOULD implement PAD. Testing of the biometric system to be deployed SHOULD demonstrate 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.					n/a								
5.2.3		Use of Biometrics	Testing of presentation attack resistance SHALL be in accordance with Clause 12 of ISO/IEC 30107-3.	✓				63B#1500	*c)*		*perform testing of presentation attack resistance in accordance with §12 of ISO/IEC 30107-3.*	✓	✓			
5.2.3		Use of Biometrics	The PAD decision MAY be made either locally on the claimant's device or by a central verifier.					n/a								
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.	✓				63B#1510			*The CSP SHALL implement rate-limiting measures on failed authentication attempts as follows:*	✓	✓			
5.2.3		Use of Biometrics		✓				63B#1510	*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		Use of Biometrics		✓				63B#1510	*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:	✓				63B#1520			*If either limit set in 63B#1510 is reached the CSP SHALL:*	✓	✓			

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
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 attempt, 2 minutes before the second following attempt), or	✓				63B#1520	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.	✓				63B#1520	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.	✓				63B#1530			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.	✓	✓			
5.2.3		Use of Biometrics	Acceptable methods for making this determination include, but are not limited to:					n/a								
5.2.3		Use of Biometrics	Authentication of the sensor or endpoint.					n/a								
5.2.3		Use of Biometrics	Certification by an approved accreditation authority.					n/a								
5.2.3		Use of Biometrics	· Runtime interrogation of signed metadata (e.g., attestation) as described in Section 5.2.4.					n/a								
5.2.3		Use of Biometrics	Biometric comparison can be performed locally on claimant's device or at a central verifier. Since the potential for attacks on a larger scale is greater at central verifiers, local comparison is preferred.					n/a								
5.2.3		Use of Biometrics	If comparison is performed centrally:	✓				63B#1540			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 identified using approved cryptography.	✓				63B#1540	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.	✓				63B#1540	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.	✓				63B#1540	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.	✓				63B#1540	d)		transmit all biometric data over an authenticated protected channel.	✓	✓			
5.2.3		Use of Biometrics	Biometric samples collected in the authentication process MAY be used to train comparison algorithms or — with user consent — for other research purposes.					n/a								
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.	✓				63B#1550			The CSP SHALL zeroize the biometric sample (including any associated biometric data) immediately after any training or research data has been derived.	✓	✓			

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
5.2.3		Use of Biometrics	Biometrics are also used in some cases to prevent repudiation of enrollment and to verify that the same individual participates in all phases of the enrollment process as described in SP 800-63A.					n/a								
5.2.4		Attestation	An attestation is information conveyed to the verifier regarding a directly-connected authenticator or the endpoint involved in an authentication operation. Information conveyed by attestation MAY include, but is not limited to:					n/a								
5.2.4		Attestation	· The provenance (e.g., manufacturer or supplier certification), health, and integrity of the authenticator and endpoint.					n/a								
5.2.4		Attestation	· Security features of the authenticator.					n/a								
5.2.4		Attestation	· Security and performance characteristics of biometric sensor(s).					n/a								
5.2.4		Attestation	· Sensor modality.					n/a								
5.2.4		Attestation	If this attestation is signed, it SHALL be signed using a digital signature that provides at least the minimum security strength specified in the latest revision of SP 800-131A (112 bits as of the date of this publication).	✓				63B#1560			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.	✓	✓			
5.2.4		Attestation	Attestation information MAY be used as part of a verifier's risk-based authentication decision.					n/a								
5.2.5		Verifier Impersonation Resistance	*... informative preamble (excised) ...*					n/a								
5.2.5		Verifier Impersonation Resistance	A verifier impersonation-resistant authentication protocol SHALL establish an authenticated protected channel with the verifier.	✓				63B#1570			**The CSP SHALL establish an authenticated protected channel between itself and the verifier by use of a verifier impersonation-resistant authentication protocol**		✓			
5.2.5		Verifier Impersonation Resistance	It SHALL then strongly and irreversibly bind a channel identifier that was negotiated in establishing the authenticated protected channel to the authenticator output (e.g., by signing the two values together using a private key controlled by the claimant for which the public key is known to the verifier).	✓				63B#1580			**The CSP SHALL strongly and irreversibly bind to the authenticator output a channel identifier which was negotiated during the establishment of the authenticated protected channel**		✓			
5.2.5		Verifier Impersonation Resistance	The verifier SHALL validate the signature or other information used to prove verifier impersonation resistance. This prevents an impostor verifier, even one that has obtained a certificate representing the actual verifier, from replaying that authentication on a different authenticated protected channel.	✓				63B#1590			**At the time of binding the channel identifier the CSP SHALL validate the information used to prove verifier impersonation-resistance.**		✓			
5.2.5		Verifier Impersonation Resistance	Approved cryptographic algorithms SHALL be used to establish verifier impersonation resistance where it is required. Keys used for this purpose SHALL provide at least the minimum security strength specified in the latest revision of SP 800-131A (112 bits as of the date of this publication).	✓				63B#1600			**The CSP SHALL establish the verifier impersonation resistant channel using approved cryptographic algorithms the keys for which meet at least the minimum security strength specified in the latest revision of SP 800-131A.**		✓			

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
5.2.5		Verifier Impersonation Resistance	One example of a verifier impersonation-resistant authentication protocol is client-authenticated TLS, because the client signs the authenticator output along with earlier messages from the protocol that are unique to the particular TLS connection being negotiated.					n/a								
5.2.5		Verifier Impersonation Resistance	Authenticators that involve the manual entry of an authenticator output, such as out-of-band and OTP authenticators, SHALL NOT be considered verifier impersonation-resistant because the manual entry does not bind the authenticator output to the specific session being authenticated. In a MitM attack, an impostor verifier could replay the OTP authenticator output to the verifier and successfully authenticate.	✓				63B#1610			The CSP SHALL NOT accept as verifier impersonation-resistant authenticators those that involve the manual entry of an authenticator output.		✓			
5.2.6		Verifier-CSP Communications	In situations where the verifier and CSP are separate entities (as shown by the dotted line in SP 800-63-3 Figure 4-1), communications between the verifier and CSP SHALL occur through a mutually-authenticated secure channel (such as a client-authenticated TLS connection) using approved cryptography.	✓				63B#1620			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.	✓	✓			
		Verifier-Compromise Resistance	... informative preamble (excised) ...					n/a								
5.2.7		Verifier-Compromise Resistance	To be considered verifier compromise resistant, public keys stored by the verifier SHALL ...	✓				63B#1630			For verifier's public keys to be considered verifier compromise resistant, the CSP SHALL only store such keys when they:	✓	✓		This ensures that the keys are considered as being 'verifier compromise resistent'	
5.2.7		Verifier-Compromise Resistance	be associated with the use of approved cryptographic algorithms and ...	✓				63B#1630	a)		use approved cryptographic algorithms;	✓	✓			
5.2.7		Verifier-Compromise Resistance	... SHALL have at least the minimum security strength specified in the latest revision of SP 800-131A (112 bits as of the date of this publication).	✓				63B#1630	b)		provide at least the minimum security strength specified in the latest revision of SP 800-131A.	✓	✓			
5.2.7		Verifier-Compromise Resistance	Other verifier compromise resistant secrets SHALL ...	✓				63B#1640			For verifier's secrets other than public key to be considered verifier compromise resistant, the CSP SHALL only only store such secrets when they:	✓	✓			
5.2.7		Verifier-Compromise Resistance	... use approved hash algorithms and ...	✓				63B#1640	a)		use approved hashing algorithms;	✓	✓			
5.2.7		Verifier-Compromise Resistance	... the underlying secrets SHALL have at least the minimum security strength specified in the latest revision of SP 800-131A (112 bits as of the date of this publication).	✓				63B#1640	b)		provide at least the minimum security strength specified in the latest revision of SP 800-131A.	✓	✓			
5.2.7		Verifier-Compromise Resistance	Secrets (e.g., memorized secrets) having lower complexity SHALL NOT be considered verifier compromise resistant when hashed because of the potential to defeat the hashing process through dictionary lookup or exhaustive search.					n/a			Superseded by the two criteria above				Covered by the above criterion - this NIST 'requirement' is effectively a comment on the rationale for the preceding clauses and cannot be ignored if they are met in full.	
5.2.8		Replay Resistance	Entirely informative					n/a								
5.2.9		Authentication Intent	... informative preamble (excised) ...					n/a								

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
5.2.9		Authentication Intent	Authentication intent SHALL be established by the authenticator itself, although multi-factor cryptographic devices MAY establish intent by reentry of the other authentication factor on the endpoint with which the authenticator is used.	✓				63B#1650			The CSP SHALL use only those authenticators which demonstrate authentication intent.	✓	✓			
5.2.9		Authentication Intent	Authentication intent MAY be established in a number of ways. Authentication processes that require the subject's intervention (e.g., a claimant entering an authenticator output from an OTP device) establish intent. Cryptographic devices that require user action (e.g., pushing a button or reinsertion) for each authentication or reauthentication operation are also establish intent.					n/a								
5.2.9		Authentication Intent	Depending on the modality, presentation of a biometric may or may not establish authentication intent. Presentation of a fingerprint would normally establish intent, while observation of the claimant's face using a camera normally would not by itself. Behavioral biometrics similarly are less likely to establish authentication intent because they do not always require a specific action on the claimant's part.					n/a								
5.2.10		Restricted Authenticators	The use of a RESTRICTED authenticator requires that the implementing organization assess, understand, and accept the risks associated with that RESTRICTED authenticator and acknowledge that risk will likely increase over time. It is the responsibility of the organization to determine the level of acceptable risk for their system(s) and associated data and to define any methods for mitigating excessive risks.					n/a								
5.2.10		Restricted Authenticators	If at any time the organization determines that the risk to any party is unacceptable, then that authenticator SHALL NOT be used.	✓				63B#1660			If the CSP employs RESTRICTED authenticators then the associated risks shall be considered in its risk assessments.	✓	✓			
5.2.10		Restricted Authenticators	Furthermore, the risk of an authentication error is typically borne by multiple parties, including the implementing organization, organizations that rely on the authentication decision, and the subscriber.					n/a								
5.2.10		Restricted Authenticators	Because the subscriber may be exposed to additional risk when an organization accepts a RESTRICTED authenticator and that the subscriber may have a limited understanding of and ability to control that risk, the CSP SHALL:	✓				63B#1670			If the CSP employs RESTRICTED authenticators then it SHALL:	✓	✓			
5.2.10		Restricted Authenticators	1. Offer subscribers at least one alternate authenticator that is not RESTRICTED and can be used to authenticate at the required AAL.	✓				63B#1670	a)		require at least one alternate authenticator that is not RESTRICTED;	✓	✓			

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
5.2.10		Restricted Authenticators	2. Provide meaningful notice to subscribers regarding the security risks of the RESTRICTED authenticator and availability of alternative(s) that are not RESTRICTED.	✓				63B#1670	b)		provide meaningful notice to subscribers regarding the security risks of the RESTRICTED authenticator and availability of alternative(s) that are not RESTRICTED;	✓	✓			
5.2.10		Restricted Authenticators	3. Address any additional risk to subscribers in its risk assessment.					n/a			See 63B#1660					
5.2.10		Restricted Authenticators	4. Develop a migration plan for the possibility that the RESTRICTED authenticator is no longer acceptable at some point in the future and include this migration plan in its digital identity acceptance statement.				✓	63B#1680			The CSP SHALL, in a digital identity acceptance statement (DIAS), develop a migration plan to account for the possibility that the RESTRICTED authenticator is no longer acceptable at some point in the future.	✓	✓			
6		Authenticator Lifecycle Management						n/a								
6.1		Authenticator Binding	... informative preamble (excised) ...					n/a								
6.1		Authenticator Binding	Authenticators SHALL be bound to subscriber accounts by either:	✓				63B#1690			The CSP SHALL bind authenticators to Subject accounts by either:	✓	✓			
6.1		Authenticator Binding	· Issuance by the CSP as part of enrollment; or	✓				63B#1690	a)		issuing them at the time of enrollment; OR	✓	✓			
6.1		Authenticator Binding	· Associating a subscriber-provided authenticator that is acceptable to the CSP.	✓				63B#1690	b)		associating a subscriber-provided authenticator that is acceptable to the CSP.	✓	✓			
6.1		Authenticator Binding	These guidelines refer to the *binding* rather than the issuance of an authenticator [so]? as to accommodate both options.					n/a								
6.1		Authenticator Binding	Throughout the digital identity lifecycle, CSPs SHALL maintain a record of all authenticators that are or have been associated with each identity.	✓				63B#1700			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.	✓	✓			
6.1		Authenticator Binding	The CSP or verifier SHALL maintain the information required for throttling authentication attempts when required, as described in Section 5.2.2.	✓				63B#1710			The CSP SHALL maintain information required for throttling authentication attempts when required (see 63B#1450 & '#1460).	✓	✓			
6.1		Authenticator Binding	The CSP SHALL also verify the type of user-provided authenticator (e.g., single-factor cryptographic device vs. multi-factor cryptographic device) so verifiers can determine compliance with requirements at each AAL.	✓				63B#1720			The CSP SHALL determine the type of user-provided authenticator and make that determination available to Verifiers to fulfill AAL2 requirements.	✓	✓			
6.1		Authenticator Binding	The record created by the CSP SHALL contain the date and time the authenticator was bound to the account.	✓				63B#1730			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:	✓	✓			
6.1		Authenticator Binding	The record SHOULD include ...					n/a								
6.1		Authenticator Binding	... information about the source of the binding (e.g., IP address, device identifier) of any device associated with the enrollment.					n/a								
6.1		Authenticator Binding	If available, the record SHOULD also contain information about the source of unsuccessful authentications attempted with the authenticator.					n/a								

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
6.1		Authenticator Binding	When any new authenticator is bound to a subscriber account, the CSP SHALL ensure that the binding protocol and the protocol for provisioning the associated key(s) are done at a level of security commensurate with the AAL at which the authenticator will be used.	✓				63B#1740			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.	✓	✓			
6.1		Authenticator Binding	For example, protocols for key provisioning SHALL use authenticated protected channels or be performed in person to protect against man-in-the-middle attacks.					n/a								
6.1		Authenticator Binding	Binding of multifactor authenticators SHALL require multifactor authentication or equivalent (e.g., association with the session in which identity proofing has been just completed) be used in order to bind the authenticator.	✓				63B#1750			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.	✓	✓			
6.1		Authenticator Binding	The same conditions apply when a key pair is generated by the authenticator and the public key is sent to the CSP.					n/a			Included within 63B#1750					
6.1.1		Binding at Enrollment	The following requirements apply when an authenticator is bound to an identity as a result of a successful identity proofing transaction, as described in SP 800-63A. Since Executive Order 13681 [EO 13681] requires the use of multi-factor authentication for the release of any personal data, it is important that authenticators be bound to subscriber accounts at enrollment, enabling access to personal data, including that established by identity proofing.					n/a			Though not normatively-stated, accommodated within the following criterion.					
6.1.1		Binding at Enrollment	The CSP SHALL bind ...	✓				63B#1760			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:	✓	✓			
6.1.1		Binding at Enrollment	... at least one, and SHOULD bind at least two, physical (*something you have*) authenticators to the subscriber's online identity, ...	✓				63B#1760	a)		at least one physical (something [the Subject] has) authenticator; AND	✓	✓			
6.1.1		Binding at Enrollment	... in addition to a memorized secret or one or more biometrics. Binding of multiple authenticators is preferred in order to recover from the loss or theft of the subscriber's primary authenticator.	✓				63B#1760	b)		a memorized secret or at least one biometric.	✓	✓			
6.1.1		Binding at Enrollment	While all identifying information is self-asserted at IAL1, preservation of online material or an online reputation makes it undesirable to lose control of an account due to the loss of an authenticator. The second authenticator makes it possible to securely recover from an authenticator loss. For this reason, a CSP SHOULD bind at least two physical authenticators to the subscriber's credential at IAL1 as well.					n/a								
6.1.1		Binding at Enrollment	At IAL2 and above, identifying information is associated with the digital identity and the subscriber has undergone an identity proofing process as described in SP 800-63A. As a result, ...					n/a								

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
6.1.1		Binding at Enrollment	... authenticators at the same AAL as the desired IAL SHALL be bound to the account.	✓				63B#1770			The CSP SHALL ensure that authenticators bound to the Subject's online identity are AAL2 or higher.	✓	✓			
6.1.1		Binding at Enrollment	For example, if the subscriber has successfully completed proofing at IAL2, then AAL2 or AAL3 authenticators are appropriate to bind to the IAL2 identity.					n/a								
6.1.1		Binding at Enrollment	While a CSP MAY bind an AAL1 authenticator to an IAL2 identity, if the subscriber is authenticated at AAL1, ...					n/a								
6.1.1		Binding at Enrollment	... the CSP SHALL NOT expose personal information, even if self-asserted, to the subscriber.	✓				63B#1780			The CSP SHALL NOT expose personal information to the subscriber, even if self-asserted, unless AAL2 authentication has been accomplished.	✓	✓			
6.1.1		Binding at Enrollment	As stated in the previous paragraph, the availability of additional authenticators provides backup methods for authentication if an authenticator is damaged, lost, or stolen.					n/a								
6.1.1		Binding at Enrollment	If enrollment and binding cannot be completed in a single physical encounter or electronic transaction (i.e., within a single protected session), the following methods SHALL be used to ensure that the same party acts as the applicant throughout the processes:	✓				63B#1790			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:	✓	✓			
6.1.1		Binding at Enrollment	For remote transactions:	✓				63B#1790	a)		For remote transactions the CSP SHALL:	✓	✓			
6.1.1		Binding at Enrollment	1. The applicant SHALL identify themselves in each new binding transaction by presenting a temporary secret which was either ...	✓				63B#1790	a)	i)	require the Applicant to identify themselves in each new binding transaction by presenting a temporary secret which was either:	✓	✓			
6.1.1		Binding at Enrollment	... established during a prior transaction, or ...	✓				63B#1790	a)	i)	established during a prior transaction; or	✓	✓			
6.1.1		Binding at Enrollment	... sent to the applicant's phone number, email address, or postal address of record.	✓				63B#1790	a)	i)	sent to the Applicant's phone number, email address, or postal address of record.	✓	✓			
6.1.1		Binding at Enrollment	2. Long-term authenticator secrets SHALL only be issued to the applicant within a protected session.	✓				63B#1790	a)	ii)	Only issue long-term authenticator secrets to the Applicant within a protected session.	✓	✓			
6.1.1		Binding at Enrollment	For in-person transactions:	✓				63B#1790	b)		For in-person transactions the CSP SHALL:	✓	✓			
6.1.1		Binding at Enrollment	1. The applicant SHALL identify themselves in person by either	✓				63B#1790	b)	i)	require the Applicant to identify themselves in person by either:	✓	✓			
6.1.1		Binding at Enrollment	... using a secret as described in remote transaction (1) above, or ...	✓				63B#1790	b)	i)	using a secret as described in remote transaction a) i) above; OR	✓	✓			
6.1.1		Binding at Enrollment	... through use of a biometric that was recorded during a prior encounter.	✓				63B#1790	b)	i)	through use of a biometric that was recorded during a prior encounter.	✓	✓			
6.1.1		Binding at Enrollment	2. Temporary secrets SHALL NOT be reused.	✓				63B#1790	b)	ii)	only accepting a temporary secret once;	✓	✓			
6.1.1		Binding at Enrollment	3. If the CSP issues long-term authenticator secrets during a physical transaction, then they SHALL be loaded locally onto a physical device that is issued in person to the applicant or delivered in a manner that confirms the address of record.	✓				63B#1790	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.	✓	✓			
6.1.2		Post-Enrollment Binding						n/a								

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
6.1.2.1		Binding of an Additional Authenticator at Existing AAL	With the exception of memorized secrets, CSPs and verifiers SHOULD encourage subscribers to maintain at least two valid authenticators of each factor that they will be using. For example, a subscriber who usually uses an OTP device as a physical authenticator MAY also be issued a number of look-up secret authenticators, or register a device for out-of-band authentication, in case the physical authenticator is lost, stolen, or damaged. See Section 6.1.2.3 for more information on replacement of memorized secret authenticators.					n/a								
6.1.2.1		Binding of an Additional Authenticator at Existing AAL	Accordingly, CSPs SHOULD permit the binding of additional authenticators to a subscriber's account.					n/a								
6.1.2.1		Binding of an Additional Authenticator at Existing AAL	Before adding the new authenticator, the CSP SHALL first require the subscriber to authenticate at the AAL (or a higher AAL) at which the new authenticator will be used.	✓				63B#1800			Prior to issuing the Subject with new/additional AAL2 authenticators the CSP SHALL first authenticate the Subject at AAL2.	✓	✓			
6.1.2.1		Binding of an Additional Authenticator at Existing AAL	When an authenticator is added, the CSP SHOULD send a notification to the subscriber via a mechanism that is independent of the transaction binding the new authenticator (e.g., email to an address previously associated with the subscriber). The CSP MAY limit the number of authenticators that may be bound in this manner.					n/a								
6.1.2.2		Adding an Additional Factor to a Single-Factor Account	If the subscriber's account has only one authentication factor bound to it (i.e., at IAL1/AAL1) and an additional authenticator of a different authentication factor is to be added, the subscriber MAY request that the account be upgraded to AAL2. The IAL would remain at IAL1.					n/a								
6.1.2.2		Adding an Additional Factor to a Single-Factor Account	Before binding the new authenticator, the CSP SHALL require the subscriber to authenticate at AAL1.					n/a								
6.1.2.2		Adding an Additional Factor to a Single-Factor Account	The CSP SHOULD send a notification of the event to the subscriber via a mechanism independent of the transaction binding the new authenticator (e.g., email to an address previously associated with the subscriber).					n/a								
6.1.2.3		Replacement of a Lost Authentication Factor	If a subscriber loses all authenticators of a factor necessary to complete multi-factor authentication and has been identity proofed at IAL2 or IAL3,	✓				63B#1810			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:	✓	✓			
6.1.2.3		Replacement of a Lost Authentication Factor	that subscriber SHALL repeat the identity proofing process described in SP 800-63A.	✓				63B#1810	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 SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
6.1.2.3		Replacement of a Lost Authentication Factor	An abbreviated proofing process, confirming the binding of the claimant to previously-supplied evidence, MAY be used if the CSP has retained the evidence from the original proofing process pursuant to a privacy risk assessment as described in SP 800-63A Section 4.2.					n/a								
6.1.2.3		Replacement of a Lost Authentication Factor	The CSP SHALL require the claimant to authenticate using an authenticator of the remaining factor, if any, to confirm binding to the existing identity.	✓				63B#1810	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.	✓	✓			
6.1.2.3		Replacement of a Lost Authentication Factor	Reestablishment of authentication factors at IAL3 SHALL ...	✓				63B#1820			The CSP SHALL re-establish authentication factors by:		✓			
6.1.2.3		Replacement of a Lost Authentication Factor	... be done in person, or through a supervised remote process as described in SP 800-63A Section 5.3.3.2,	✓				63B#1820	a)		using a Supervised (In-Person or Remote) process; AND		✓			
6.1.2.3		Replacement of a Lost Authentication Factor	... and SHALL verify the biometric collected during the original proofing process.	✓				63B#1820	b)		verifying the biometric collected during the original proofing process.		✓			
6.1.2.3		Replacement of a Lost Authentication Factor	The CSP SHOULD send a notification of the event to the subscriber. This MAY be the same notice as is required as part of the proofing process.					n/a								
6.1.2.3		Replacement of a Lost Authentication Factor	Replacement of a lost (i.e., forgotten) memorized secret is problematic because it is very common. Additional "backup" memorized secrets do not mitigate this because they are just as likely to also have been forgotten. If a biometric is bound to the account, the biometric and associated physical authenticator SHOULD be used to establish a new memorized secret.					n/a								
6.1.2.3		Replacement of a Lost Authentication Factor	As an alternative to the above re-proofing process when there is no biometric bound to the account, the CSP MAY bind a new memorized secret with authentication using two physical authenticators, along with a confirmation code that ...					n/a								
6.1.2.3		Replacement of a Lost Authentication Factor	... has been sent to one of the subscriber's addresses of record.					n/a								
6.1.2.3		Replacement of a Lost Authentication Factor	The confirmation code SHALL consist of at least 6 random alphanumeric characters generated by an approved random bit generator [SP 800-90Ar1].	✓				63B#1830			The CSP SHALL, if it supports re-proofing through binding memorized secrets using two physical authenticators, use conformation codes that consist of at least 6 random alphanumeric characters generated by an approved random-bit generator [SP 800-90Ar1].	✓	✓			
6.1.2.3		Replacement of a Lost Authentication Factor		✓				63B#1840			The CSP SHALL only issue confirmation codes that have the following validities:	✓	✓			
6.1.2.3		Replacement of a Lost Authentication Factor	Those sent to a postal address of record SHALL be valid for a maximum of 7 days ...	✓				63B#1840	a)		7 days, when sent to a postal address of record within the contiguous United States; OR	✓	✓			
6.1.2.3		Replacement of a Lost Authentication Factor	... but MAY be made valid up to 21 days via an exception process to accommodate addresses outside the direct reach of the U.S. Postal Service.	✓				63B#1840	b)		21 days, when sent to a postal address of record outside the direct reach of the U.S. Postal Service; OR	✓	✓			
6.1.2.3		Replacement of a Lost Authentication Factor	Confirmation codes sent by means other than physical mail SHALL be valid for a maximum of 10 minutes.	✓				63B#1840	c)		10 minutes, when sent by any means other than physical mail.	✓	✓			

NIST SP 800-63B (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'			AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index	KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
6.1.3		Binding to a Subscriber-provided Authenticator	A subscriber may already possess authenticators suitable for authentication at a particular AAL. For example, they may have a two-factor authenticator from a social network provider, considered AAL2 and IAL1, and would like to use those credentials at an RP that requires IAL2.					n/a							
6.1.3		Binding to a Subscriber-provided Authenticator	CSPs SHOULD, where practical, accommodate the use of subscriber-provided authenticators in order to relieve the burden to the subscriber of managing a large number of authenticators.					n/a							
6.1.3		Binding to a Subscriber-provided Authenticator	Binding of these authenticators SHALL be done as described in Section 6.1.2.1.	✓				63B#1850			✔	✓			
6.1.3		Binding to a Subscriber-provided Authenticator	In situations where the authenticator strength is not self-evident (e.g., between single-factor and multi-factor authenticators of a given type), the CSP SHOULD assume the use of the weaker authenticator unless it is able to establish that the stronger authenticator is in fact being used (e.g., by verification with the issuer or manufacturer of the authenticator).					n/a							
6.1.4		Renewal	The CSP SHOULD bind an updated authenticator an appropriate amount of time before an existing authenticator's expiration. The process for this SHOULD conform closely to the initial authenticator binding process (e.g., confirming address of record). Following successful use of the new authenticator, the CSP MAY revoke the authenticator that it is replacing.					n/a							
6.2		Loss, Theft, Damage, and Unauthorized Duplication	Compromised authenticators include those that have been lost, stolen, or subject to unauthorized duplication. Generally, one must assume that a lost authenticator has been stolen or compromised by someone that is not the legitimate subscriber of the authenticator. Damaged or malfunctioning authenticators are also considered compromised to guard against any possibility of extraction of the authenticator secret. One notable exception is a memorized secret that has been forgotten without other indications of having been compromised, such as having been obtained by an attacker.					n/a							
6.2		Loss, Theft, Damage, and Unauthorized Duplication	Suspension, revocation, or destruction of compromised authenticators SHOULD occur as promptly as practical following detection. Agencies SHOULD establish time limits for this process.					n/a							
6.2		Loss, Theft, Damage, and Unauthorized Duplication	To facilitate secure reporting of the loss, theft, or damage to an authenticator, the CSP SHOULD provide the subscriber with a method of authenticating to the CSP using a backup or alternate authenticator.					n/a							

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
6.2		Loss, Theft, Damage, and Unauthorized Duplication	This backup authenticator SHALL be either a memorized secret or a physical authenticator.	✓				63B#1860			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.	✓	✓			
6.2		Loss, Theft, Damage, and Unauthorized Duplication	Either MAY be used, but only one authentication factor is required to make this report. Alternatively, the subscriber MAY establish an authenticated protected channel to the CSP and verify information collected during the proofing process. The CSP MAY choose to verify an address of record (i.e., email, telephone, postal) and suspend authenticator(s) reported to have been compromised.					n/a								
6.2		Loss, Theft, Damage, and Unauthorized Duplication	The suspension SHALL be reversible if the subscriber successfully authenticates to the CSP using a valid (i.e., not suspended) authenticator and requests reactivation of an authenticator suspended in this manner.	✓				63B#1870			The CSP SHALL, if it supports suspension of authenticators reported as having been compromised, ensure that such suspension is reversible if the Subject is successfully authenticated by the CSP using an alternative valid (i.e., not suspended) authenticator, at the same or higher assurance level, and the Subject requests reactivation of the suspended authenticator.	✓	✓			
6.2		Loss, Theft, Damage, and Unauthorized Duplication	The CSP MAY set a time limit after which a suspended authenticator can no longer be reactivated.					n/a								
6.3		Expiration	CSPs MAY issue authenticators that expire.					n/a								
6.3		Expiration	If and when an authenticator expires, it SHALL NOT be usable for authentication.	✓				63B#1880			If the CSP issues authenticators which expire the CSP SHALL NOT accept authentication claims which attempt to use an expired authenticator.	✓	✓			
6.3		Expiration	When an authentication is attempted using an expired authenticator, the CSP SHOULD give an indication to the subscriber that the authentication failure is due to expiration rather than some other cause.					n/a								
6.3		Expiration	The CSP SHALL require subscribers to surrender or prove destruction of any physical authenticator containing attribute certificates signed by the CSP as soon as practical after expiration or receipt of a renewed authenticator.	✓				63B#1890			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.	✓	✓			
6.4		Revocation and Termination	Revocation of an authenticator — sometimes referred to as termination, especially in the context of PIV authenticators — refers to removal of the binding between an authenticator and a credential the CSP maintains.					n/a								
6.4		Revocation and Termination	CSPs SHALL revoke the binding of authenticators promptly when ...	✓				63B#1900			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:	✓	✓			
6.4		Revocation and Termination	... an online identity ceases to exist (e.g., subscriber's death, discovery of a fraudulent subscriber), ...	✓				63B#1900	a)		the Subject's online identity ceases to exist; OR	✓	✓			
6.4		Revocation and Termination	... when requested by the subscriber, or ...	✓				63B#1900	b)		the Subject requests revocation; OR	✓	✓			
6.4		Revocation and Termination	... when the CSP determines that the subscriber no longer meets its eligibility requirements.	✓				63B#1900	c)		the CSP determines that the Subject no longer meets its eligibility requirements; OR	✓	✓			
6.4		Revocation and Termination		✓				63B#1900	d)		the CSP is obligated to do so in response to a legal instrument.	✓	✓			

NIST SP 800-63B (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'			AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
6.4		Revocation and Termination	The CSP SHALL require subscribers to surrender or certify destruction of any physical authenticator containing certified attributes signed by the CSP as soon as practical after revocation or termination takes place. This is necessary to block the use of the authenticator's certified attributes in offline situations between revocation/termination and expiration of the certification.	✓				63B#1910			The CSP SHALL require Subscribers/Subjects to surrender or certify destruction of any physical authenticator containing certified attributes signed by the CSP as soon as practical after revocation or termination takes place.	✓	✓			
6.4		Revocation and Termination	Further requirements on the termination of PIV authenticators are found in FIPS 201					n/a								
7		Session Management	A session occurs between the software that a subscriber is running — such as a browser, application, or operating system (i.e., the session subject) — and the RP or CSP that the subscriber is accessing (i.e., the session host).					n/a								
7.1.1		Browser Cookies	Browser cookies are the predominant mechanism by which a session will be created and tracked for a subscriber accessing a service.					n/a								
7.1.2		Access Tokens	An access token — such as found in OAuth — is used to allow an application to access a set of services on a subscriber's behalf following an authentication event.					n/a								
7.1.3		Device Identification	Other methods of secure device identification — including but not limited to mutual TLS, token binding, or other mechanisms — MAY be used to enact a session between a subscriber and a service.					n/a								
7.2		Reauthentication	Continuity of authenticated sessions SHALL be based upon the possession of a session secret issued by the verifier at the time of authentication and optionally refreshed during the session.	✓				63B#1920			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.	✓	✓			
7.2		Reauthentication	The nature of a session depends on the application, including:					n/a								
7.2		Reauthentication	1. A web browser session with a "session" cookie, or					n/a								
7.2		Reauthentication	2. An instance of a mobile application that retains a session secret.					n/a								
7.2		Reauthentication	Session secrets SHALL be non-persistent. That is, they SHALL NOT be retained across a restart of the associated application or a reboot of the host device.	✓				63B#1930			The CSP SHALL NOT allow session secrets (whether ~~one~~ issued initially or ~~one~~ refreshed) to persist beyond the termination of a session.	✓	✓			
7.2		Reauthentication	Periodic reauthentication of sessions SHALL be performed to confirm the continued presence of the subscriber at an authenticated session (i.e., that the subscriber has not walked away without logging out).					n/a			At AAL2, see 63B#0150 At AAL3, see 63B#0320					
7.2		Reauthentication	A session SHALL NOT be extended past the guidelines in Sections 4.1.3, 4.2.3, and 4.3.3 (depending on AAL) based on presentation of the session secret alone.					n/a			See 63B#0140					

NIST SP 800-63B (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'				AAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDINGS (SoC)
§	(...)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
7.2		Reauthentication	Prior to session expiration, the reauthentication time limit SHALL be extended by prompting the subscriber for the authentication factor(s) specified in Table 7-1.	✓				63B#1940			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.	✓	✓			
7.2		Reauthentication	When a session has been terminated, due to a time-out or other action, the user SHALL be required to establish a new session by authenticating again.	✓				63B#1950			The CSP SHALL require a new session to be started, with re-authentication of the Subject after any session termination (for whatever reason).	✓	✓			
7.2.1		Reauthentication from a Federation or Assertion	When using a federation protocol as described in SP 800-63C, Section 5 to connect the CSP and RP, special considerations apply to session management and reauthentication. The federation protocol communicates an authentication event between the CSP and the RP but establishes no session between them.					n/a								
7.2.1		Reauthentication from a Federation or Assertion	Since the CSP and RP often employ separate session management technologies, there SHALL NOT be any assumption of correlation between these sessions.	✓				63B#1960			Unless the CSP is supporting a federation protocol which permits RPs to specify an acceptable authentication age then the CSP SHALL make no assumptions of correlation between its session with the Subscriber and those of any other party.	✓	✓			
7.2.1		Reauthentication from a Federation or Assertion	Consequently, when an RP session expires and the RP requires reauthentication, it is entirely possible that the session at the CSP has not expired and that a new assertion could be generated from this session at the CSP without reauthenticating the user.					n/a								
7.2.1		Reauthentication from a Federation or Assertion	An RP requiring reauthentication through a federation protocol SHALL — if possible within the protocol — specify the maximum acceptable authentication age to the CSP, and ...					n/a								
7.2.1		Reauthentication from a Federation or Assertion	... the CSP SHALL reauthenticate the subscriber if they have not been authenticated within that time period.	✓				63B#1970			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:	✓	✓			
7.2.1		Reauthentication from a Federation or Assertion		✓				63B#1970	a)		re-authenticate the Subscriber within the RP-specified time period;	✓	✓			
7.2.1		Reauthentication from a Federation or Assertion	The CSP SHALL communicate the authentication event time to the RP to allow the RP to decide if the assertion is sufficient for reauthentication and to determine the time for the next reauthentication event.	✓				63B#1970	b)		communicate the authentication event time to the RP;	✓	✓			
	End of 63B_SAC criteria															

In scope - Applicable
In scope - Not applicable
In scope - Applicable - fulfilled by ...
Not in scope

Tag cross-references

==>

old tag	new tag
63B#0010	63B#0010
63B#0010	63B#1080
63B#0020	63B#0020
63B#0030	63B#0040
63B#0030	63B#0050
63B#0040	63B#0060
63B#0050	63B#0070
63B#0060	63B#0080
63B#0070	63B#0100
63B#0080	63B#0110
63B#0090	63B#0130
63B#0100	63B#0140
63B#0110	63B#1920
63B#0120	63B#1930
63B#0130	63B#0150
63B#0150	63B#1940
63B#0160	n/a
63B#0170	63B#1950
63B#0180	63B#1960
63B#0190	63B#1970
63B#0200	63B#0160
63B#0210	63B#0180
63B#0220	63B#0190
63B#0230	63B#0350
63B#0240	63B#0360
63B#0250	63B#0370
63B#0260	63B#0380
63B#0270	63B#0390
63B#0280	63B#0410
63B#0280	63B#0420
63B#0300	63B#0430
63B#0310	63B#0440
63B#0320	63B#0450
63B#0340	63B#0460
63B#0350	63B#0470
63B#0360	63B#0480
63B#0370	63B#0490
63B#0380	63B#0500
63B#0380	63B#0500
63B#0380	63B#0500
63B#0390	63B#0510

==>

new tag	old tag
63B#0010	63B#0010
63B#0020	63B#0020
63B#0030	n/a
63B#0040	63B#0030
63B#0050	63B#0030
63B#0060	63B#0040
63B#0070	63B#0050
63B#0080	63B#0060
63B#0090	n/a
63B#0100	63B#0070
63B#0110	63B#0080
63B#0120	n/a
63B#0130	63B#0090
63B#0140	63B#0100
63B#0150	63B#0130
63B#0160	63B#0200
63B#0170	n/a
63B#0180	63B#0210
63B#0190	63B#0220
63B#0200	63B#3010
63B#0210	n/a
63B#0220	63B#3030
63B#0230	63B#3040
63B#0240	63B#3060
63B#0250	63B#3080
63B#0260	63B#3090
63B#0270	63B#3100
63B#0280	n/a
63B#0290	63B#3110
63B#0300	63B#3120
63B#0310	n/a
63B#0320	63B#3150
63B#0320	63B#3160
63B#0320	63B#3170
63B#0320	63B#3180
63B#0330	63B#3200
63B#0340	63B#3205
63B#0350	63B#0230
63B#0360	63B#0240
63B#0370	63B#0250
63B#0380	63B#0260

63B#0390	63B#0510
63B#0390	63B#0510
63B#0400	63B#0520
63B#0410	63B#0530
63B#0420	63B#0540
63B#0430	63B#0550
63B#0430	63B#0550
63B#0430	63B#0550
63B#0440	63B#0570
63B#0450	63B#0580
63B#0460	63B#0590
63B#0470	63B#0600
63B#0480	63B#0610
63B#0490	63B#0620
63B#0500	63B#0630
63B#0510	63B#0640
63B#0520	63B#0650
63B#0530	63B#0660
63B#0540	63B#0690
63B#0550	63B#0700
63B#0560	63B#0710
63B#0570	63B#0720
63B#0580	63B#0730
63B#0590	63B#0740
63B#0600	63B#0750
63B#0610	63B#0760
63B#0620	63B#0770
63B#0630	63B#0780
63B#0640	63B#0790
63B#0650	63B#0800
63B#0660	63B#0810
63B#0670	63B#0820
63B#0680	63B#0830
63B#0690	63B#0840
63B#0700	63B#0850
63B#0710	63B#0860
63B#0720	63B#0870
63B#0730	63B#0890
63B#0740	63B#0900
63B#0750	63B#0910
63B#0760	63B#0920
63B#0770	63B#0930
63B#0780	63B#0940
63B#0790	63B#0950
63B#0800	63B#0960

63B#0390	63B#0270
63B#0400	n/a
63B#0400	n/a
63B#0400	n/a
63B#0400	n/a
63B#0400	n/a
63B#0410	63B#0280
63B#0420	63B#0280
63B#0430	63B#0300
63B#0440	63B#0310
63B#0450	63B#0320
63B#0460	63B#0340
63B#0470	63B#0350
63B#0480	63B#0360
63B#0490	63B#0370
63B#0500	63B#0380
63B#0500	63B#0380
63B#0500	63B#0380
63B#0510	63B#0390
63B#0510	63B#0390
63B#0510	63B#0390
63B#0520	63B#0400
63B#0530	63B#0410
63B#0540	63B#0420
63B#0550	63B#0430
63B#0550	63B#0430
63B#0550	63B#0430
63B#0560	n/a
63B#0570	63B#0440
63B#0570	n/a
63B#0580	63B#0450
63B#0590	63B#0460
63B#0600	63B#0470
63B#0610	63B#0480
63B#0620	63B#0490
63B#0630	63B#0500
63B#0640	63B#0510
63B#0650	63B#0520
63B#0660	63B#0530
63B#0670	n/a
63B#0680	n/a
63B#0690	63B#0540
63B#0700	63B#0550
63B#0710	63B#0560
63B#0720	63B#0570

63B#0810	63B#0970
63B#0820	63B#0980
63B#0830	63B#0990
63B#0840	63B#1000
63B#0850	63B#1010
63B#0860	63B#1020
63B#0870	63B#1030
63B#0880	63B#1040
63B#0890	63B#1050
63B#0900	63B#1060
63B#0920	63B#1090
63B#0930	63B#1100
63B#0940	63B#1110
63B#0950	63B#1120
63B#0960	63B#1130
63B#0970	63B#1140
63B#0980	63B#1150
63B#0990	63B#1160
63B#1000	63B#1170
63B#1010	63B#1180
63B#1020	63B#1190
63B#1030	63B#1200
63B#1040	63B#1210
63B#1050	63B#1220
63B#1060	63B#1230
63B#1070	63B#1240
63B#1080	63B#1250
63B#1090	63B#1260
63B#1100	63B#1270
63B#1110	63B#1280
63B#1120	63B#1290
63B#1130	63B#1300
63B#1140	63B#1310
63B#1150	63B#1320
63B#1160	63B#1330
63B#1170	63B#1340
63B#1180	63B#1350
63B#1190	63B#1360
63B#1200	63B#1370
63B#1210	63B#1380
63B#1220	63B#1390
63B#1230	63B#1400
63B#1240	63B#1410
63B#1250	63B#1420
63B#1260	63B#1430

63B#0730	63B#0580
63B#0740	63B#0590
63B#0750	63B#0600
63B#0760	63B#0610
63B#0770	63B#0620
63B#0780	63B#0630
63B#0790	63B#0640
63B#0800	63B#0650
63B#0810	63B#0660
63B#0820	63B#0670
63B#0830	63B#0680
63B#0840	63B#0690
63B#0850	63B#0700
63B#0860	63B#0710
63B#0870	63B#0720
63B#0880	n/a
63B#0890	63B#0730
63B#0900	63B#0740
63B#0910	63B#0750
63B#0920	63B#0760
63B#0930	63B#0770
63B#0940	63B#0780
63B#0950	63B#0790
63B#0960	63B#0800
63B#0970	63B#0810
63B#0980	63B#0820
63B#0990	63B#0830
63B#1000	63B#0840
63B#1010	63B#0850
63B#1020	63B#0860
63B#1030	63B#0870
63B#1040	63B#0880
63B#1050	63B#0890
63B#1060	63B#0900
63B#1070	n/a
63B#1080	63B#0010
63B#1090	63B#0920
63B#1100	63B#0930
63B#1110	63B#0940
63B#1120	63B#0950
63B#1130	63B#0960
63B#1140	63B#0970
63B#1150	63B#0980
63B#1160	63B#0990
63B#1170	63B#1000

63B#1270	63B#1440
63B#1280	63B#1450
63B#1290	63B#1460
63B#1300	63B#1470
63B#1310	63B#1480
63B#1320	63B#1490
63B#1330	63B#1500
63B#1340	63B#1510
63B#1350	63B#1520
63B#1360	63B#1530
63B#1370	63B#1540
63B#1380	63B#1550
63B#1390	63B#1560
63B#1400	63B#1620
63B#1410	63B#1660
63B#1420	63B#1670
63B#1430	63B#1690
63B#1430	63B#1690
63B#1440	63B#1700
63B#1450	63B#1710
63B#1460	63B#1720
63B#1470	63B#1730
63B#1480	63B#1740
63B#1490	63B#1750
63B#1500	63B#1760
63B#1510	63B#1770
63B#1520	63B#1780
63B#1530	63B#1790
63B#1540	63B#1800
63B#1550	63B#1810
63B#1550	63B#1810
63B#1560	63B#1850
63B#1570	63B#1860
63B#1580	63B#1880
63B#1590	63B#1890
63B#1600	63B#1900
63B#1600	63B#1900
63B#3010	63B#0200
63B#3020	n/a
63B#3030	63B#0220
63B#3040	63B#0230
63B#3050	n/a
63B#3060	63B#0240
63B#3070	n/a
63B#3080	63B#0250

63B#1180	63B#1010
63B#1190	63B#1020
63B#1200	63B#1030
63B#1210	63B#1040
63B#1220	63B#1050
63B#1230	63B#1060
63B#1240	63B#1070
63B#1250	63B#1080
63B#1260	63B#1090
63B#1270	63B#1100
63B#1280	63B#1110
63B#1290	63B#1120
63B#1300	63B#1130
63B#1310	63B#1140
63B#1320	63B#1150
63B#1330	63B#1160
63B#1340	63B#1170
63B#1350	63B#1180
63B#1360	63B#1190
63B#1370	63B#1200
63B#1380	63B#1210
63B#1390	63B#1220
63B#1400	63B#1230
63B#1410	63B#1240
63B#1420	63B#1250
63B#1430	63B#1260
63B#1440	63B#1270
63B#1450	63B#1280
63B#1460	63B#1290
63B#1470	63B#1300
63B#1480	63B#1310
63B#1490	63B#1320
63B#1500	63B#1330
63B#1510	63B#1340
63B#1520	63B#1350
63B#1530	63B#1360
63B#1540	63B#1370
63B#1550	63B#1380
63B#1560	63B#1390
63B#1570	n/a
63B#1580	n/a
63B#1590	n/a
63B#1600	n/a
63B#1610	n/a
63B#1620	63B#1400

63B#3090	63B#0260
63B#3100	63B#0270
63B#3110	63B#0290
63B#3120	63B#0300
63B#3130	n/a
63B#3140	n/a
63B#3150	63B#0320
63B#3160	63B#0320
63B#3170	63B#0320
63B#3180	63B#0320
63B#3190	n/a
63B#3200	63B#0330
63B#3205	63B#0340
63B#3210	n/a
63B#3220	n/a
63B#3230	n/a
n/a	63B#0030
n/a	63B#0090
n/a	63B#0120
n/a	63B#0170
n/a	63B#0400
n/a	63B#0400
n/a	63B#0400
n/a	63B#0400
n/a	63B#0400
n/a	63B#0560
n/a	63B#0570
n/a	63B#0670
n/a	63B#0680
n/a	63B#0880
n/a	63B#1070
n/a	63B#1570
n/a	63B#1580
n/a	63B#1590
n/a	63B#1600
n/a	63B#1610
n/a	63B#1630
n/a	63B#1640
n/a	63B#1650
n/a	63B#1680
n/a	63B#1820
n/a	63B#1830
n/a	63B#1840
n/a	63B#1870
n/a	63B#1910

63B#1630	n/a
63B#1640	n/a
63B#1650	n/a
63B#1660	63B#1410
63B#1670	63B#1420
63B#1680	n/a
63B#1690	63B#1430
63B#1690	63B#1430
63B#1700	63B#1440
63B#1710	63B#1450
63B#1720	63B#1460
63B#1730	63B#1470
63B#1740	63B#1480
63B#1750	63B#1490
63B#1760	63B#1500
63B#1770	63B#1510
63B#1780	63B#1520
63B#1790	63B#1530
63B#1800	63B#1540
63B#1810	63B#1550
63B#1810	63B#1550
63B#1820	n/a
63B#1830	n/a
63B#1840	n/a
63B#1850	63B#1560
63B#1860	63B#1570
63B#1870	n/a
63B#1880	63B#1580
63B#1890	63B#1590
63B#1900	63B#1600
63B#1900	63B#1600
63B#1910	n/a
63B#1920	63B#0110
63B#1930	63B#0120
63B#1940	63B#0150
63B#1950	63B#0170
63B#1960	63B#0180
63B#1970	63B#0190
n/a	63B#0160
n/a	63B#3020
n/a	63B#3050
n/a	63B#3070
n/a	63B#3130
n/a	63B#3140
n/a	63B#3190

n/a	*63B#0210*
n/a	*63B#0280*
n/a	*63B#0310*
End of 63B_SAC criteria	

n/a	*63B#3210*
n/a	*63B#3220*
n/a	*63B#3230*
End of 63B_SAC criteria	