Title:	Kantara Identity Assurance Framework: Operational Service Assessment Criteria (SAC) & Statement of Criteria Applicability (SoCA)
Document id:	KIAF-1420
Version:	2.0
Document type:	Recommendation
Publication Date:	2020-10-15
Effective Date:	2021-02-01
Status:	Final
Approval Authority:	IAWG
IAWG	https://kantarainitiative.org/confluence/display/IAWG/Participant+Roster
IPR:	Patent and Copyright Option: Reciprocal Royalty Free with Opt-Out to Reasonable and Non-Discriminatory terms (RAND) | © 2020

Abstract: This Specification sets forth KI's Service Assessment Criteria, generally referred-to as the 'OP_SAC', for the assessment of the operational functionality of those services which align to the 'Classical' Kantara criteria, which are based loosely on NIST SP 800-53 rev.2, be generally referred-to as the 'OP_SAC'. It is anticipated that these criteria will be reviewed 12 months after publication, for any

Though this document is structured with headers, footers etc. for document management purposes, the OP_SAC worksheet itself 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-1420 Commonly-Applicable Service Assessment Criteria (OP_SAC)

Version	*Date*	*Status*	*Summary of changes*
Note re. version numbers:		*Changes which the IAWG considers to be Non-Material shall be incremented by '0.1', whereas changes considered to be MATERIAL shall be raised to the next whole number.*	
v2.0	10/15/20	Final - Material changes - released for application	Re-expression in Spreadsheet format with addition of explicit SoCA and SoC columns.

For version v1.0, refer to the Word version of KIAF-1420.

This Worksheet realization includes changes to eliminate historical artefacts, such as use of 'omitted' where changes have lead to the removal of text, and 'normalization' of criteria tags to have greater commonality with those used an all other SACs. Essentially, a 'clean start' for these criteria.

OP_SAC SAC / SoCA v2.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
Part A - Credential Operating Environment																	
		Credential Policy and Practices															
			Credential Policy and Practice Statement	✓				OPA#0010			Document and apply both the Credential Policy against which it issues credentials and the corresponding Credential Practices it applies in their management. At a minimum, the Credential Policy and Practice Statement must specify:		✓	✓			This is a MANDATORY criterion
			Credential Policy and Practice Statement	✓				OPA#0010	a)		if applicable, any OIDs related to the Practice and Policy Statement;		✓	✓			
			Credential Policy and Practice Statement	✓				OPA#0010	b)		how users may subscribe to the service/apply for credentials and how users' credentials will be delivered to them;		✓	✓			
			Credential Policy and Practice Statement	✓				OPA#0010	c)		how Subjects acknowledge receipt of tokens and credentials, what obligations they accept in so doing (including whether they consent to publication of their details in credential status directories) and the measures the CSP takes to initialize and personalize the credentials;		✓	✓			
			Credential Policy and Practice Statement	✓				OPA#0010	d)		how credentials may be renewed, modified, revoked, and suspended, including how requestors are authenticated or their identity re-proven;		✓	✓			
			Credential Policy and Practice Statement	✓				OPA#0010	e)		what actions a Subject must take to terminate a subscription;		✓	✓			
			Credential Policy and Practice Statement	✓				OPA#0010	f)		how records are retained and archived.		✓	✓			
			Credential Policy reference					OPA#0015			Include in its Service Definition, either directly or by accessible reference, the policy against which it issues credentials.		✓	✓			This is a MANDATORY criterion
			Certificate Policy / Certification Practice Statement	✓				OPA#0020			Include in its Service Definition its full Certificate Policy and may include the corresponding Certification and Practice Statement. The Certificate Policy and Certification Practice Statement must conform to IETF RFC 3647 (2003-11) in their content and scope or be demonstrably consistent with the content or scope of that RFC. At a minimum, the Certificate Policy must specify:				✓		This is a MANDATORY criterion Publication of the CSP is optional since in some cases its release may present a risk to the service. CSPs are therefore allowed to exercise their discretion in this matter.
			Certificate Policy / Certification Practice Statement	✓				OPA#0020	a)		applicable OIDs for each certificate type issued;				✓		
			Certificate Policy / Certification Practice Statement	✓				OPA#0020	b)		how users may subscribe to the service/apply for certificates, and how certificates will be issued to them;				✓		
			Certificate Policy / Certification Practice Statement	✓				OPA#0020	c)		if users present their own keys, how they will be required to demonstrate possession of the private key;				✓		
			Certificate Policy / Certification Practice Statement	✓				OPA#0020	d)		if users' keys are generated for them, how the private keys will be delivered to them;				✓		
			Certificate Policy / Certification Practice Statement	✓				OPA#0020	e)		how Subjects acknowledge receipt of tokens and credentials and what obligations they accept in so doing (including whether they consent to publication of their details in certificate status directories);				✓		
			Certificate Policy / Certification Practice Statement	✓				OPA#0020	f)		how certificates may be renewed, re-keyed, modified, revoked, and suspended, including how requestors are authenticated or their identity proven;				✓		
			Certificate Policy / Certification Practice Statement	✓				OPA#0020	g)		what actions a Subject must take to terminate their subscription.				✓		
			Management Authority	✓				OPA#0030			Have a nominated management body with authority and responsibility for approving the Credential Policy and Practice Statement and for its implementation.		✓				This is a MANDATORY criterion

OP_SAC SAC / SoCA v2.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
			Management Authority	✓				OPA#0030			Have a nominated **or appointed high-level management body** with authority and responsibility for approving the **Certificate Policy and Certification Practice Statement, including ultimate responsibility for their proper implementation.**			✓	✓		This is a MANDATORY criterion
			Discretionary Access Control	✓				OPA#0040			**Apply discretionary access controls that limit access to trusted administrators and to those applications that require access.**				✓		
		Security Controls															
			Protocol threat risk assessment and controls	✓				OPA#0050			Account for at least the following protocol threats and apply appropriate controls:	✓					The following list is not be considered to be a complete list of threats to be addressed by the risk assessment, the scope of which should be determined and justified by the CSP. Organizations should consider potential protocol threats identified in other sources, e.g. ISO/IEC 29115:2013 "Information technology -- Security techniques – Entity authentication assurance framework". Kantara IAF-5415 provides a mapping between IS29115 and the SAC.
			Protocol threat risk assessment and controls	✓				OPA#0050	a)		password guessing, such that there are at least 14 bits of entropy to resist an on-line guessing attack against a selected user/password;	✓					
			Protocol threat risk assessment and controls	✓				OPA#0050	b)		message replay.	✓					
			Protocol threat risk assessment and controls	✓				OPA#0050			Account for at least the following protocol threats in its risk assessment and apply controls that reduce them to acceptable risk levels:		✓				See LoA1 Guidance
			Protocol threat risk assessment and controls	✓				OPA#0050	a)		password guessing, such that there are at least 14 bits of entropy to resist an on-line guessing attack against a selected user/password;		✓				
			Protocol threat risk assessment and controls	✓				OPA#0050	b)		message replay.		✓				
			Protocol threat risk assessment and controls	✓				OPA#0050	**c)**		**eavesdropping, showing that it is impractical;**		✓				
			Protocol threat risk assessment and controls	✓				OPA#0050	**d)**		**no stipulation;**		✓				
			Protocol threat risk assessment and controls	✓				OPA#0050	**e)**		**man-in-the-middle attack;**		✓				
			Protocol threat risk assessment and controls	✓				OPA#0050	**f)**		**session hijacking;**		✓				
			Protocol threat risk assessment and controls	✓				OPA#0050	**g)**		**phishing and other fraudulent attacks, showing that they are impractical.**		✓				
			Protocol threat risk assessment and controls	✓				OPA#0050			Account for at least the following protocol threats in its risk assessment and apply controls that reduce them to acceptable risk levels:			✓			See LoA1 Guidance
			Protocol threat risk assessment and controls	✓				OPA#0050	**a)**		password guessing, such that there are at least 24 bits of entropy to resist an on-line guessing attack against a selected user/password;			✓			
			Protocol threat risk assessment and controls	✓				OPA#0050	b)		message replay, **showing that it is impractical;**			✓			
			Protocol threat risk assessment and controls	✓				OPA#0050	c)		eavesdropping, showing that it is impractical;			✓			
			Protocol threat risk assessment and controls	✓				OPA#0050	**d)**		**relying party (verifier) impersonation, showing that it is impractical;**			✓			
			Protocol threat risk assessment and controls	✓				OPA#0050	e)		man-in-the-middle attack;			✓			

OP_SAC SAC / SoCA v2.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
			Protocol threat risk assessment and controls	✓				OPA#0050	f)		session hijacking, **showing that it is impractical.**			✓			
			Protocol threat risk assessment and controls	✓				OPA#0050	g)		phishing and other fraudulent attacks, showing that they are impractical.			✓			
			Protocol threat risk assessment and controls	✓				OPA#0050			Account for at least the following protocol threats in its risk assessment and apply controls that reduce them to acceptable risk levels:				✓		See LoA1 Guidance
			Protocol threat risk assessment and controls	✓				OPA#0050	**a)**		password guessing, **showing that there is sufficient entropy;**				✓		
			Protocol threat risk assessment and controls	✓				OPA#0050	b)		message replay, showing that it is impractical;				✓		
			Protocol threat risk assessment and controls	✓				OPA#0050	c)		eavesdropping, showing that it is impractical;				✓		
			Protocol threat risk assessment and controls	✓				OPA#0050	d)		relying party (verifier) impersonation, showing that it is impractical;				✓		
			Protocol threat risk assessment and controls	✓				OPA#0050	**e)**		man-in-the-middle attack**, showing that it is impractical;**				✓		
			Protocol threat risk assessment and controls	✓				OPA#0050	f)		session hijacking, showing that it is impractical.				✓		
			Protocol threat risk assessment and controls	✓				OPA#0050	g)		phishing and other fraudulent attacks, showing that they are impractical.				✓		
			Authentication protocols	✓				OPA#0060			**Apply only authentication protocols which, through a comparative risk assessment which takes into account the target Assurance Level, are shown to have resistance to attack at least as strong as that provided by commonly-recognized protocols such as:**		✓				Whilst many authentication protocols are well-established and may be mandated or strongly-recommended by specific jurisdictions or sectors (e.g. standards published by national SDOs or applicable to government-specific usage) this criterion gives flexibility to advanced and innovative authentication protocols for which adequate strength can be shown to be provided by the protocol applied with the specific service.
			Authentication protocols	✓				OPA#0060	**a)**		**tunneling;**		✓				
			Authentication protocols	✓				OPA#0060	**b)**		**zero knowledge-based;**		✓				
			Authentication protocols	✓				OPA#0060	**c)**		**signed SAML.**		✓				
			Authentication protocols	✓				OPA#0060			**For non-PKI credentials,** apply only authentication protocols which, through a comparative risk assessment which takes into account the target Assurance Level, are shown to have resistance to attack at least as strong as that provided by commonly-recognized protocols such as:			✓			See LoA2 Guidance
			Authentication protocols	✓				OPA#0060	a)		tunneling;			✓			
			Authentication protocols	✓				OPA#0060	b)		zero knowledge-based;			✓			
			Authentication protocols	✓				OPA#0060	c)		signed SAML [Omitted].			✓			
			One-time passwords	✓				OPA#0070			**Use only one-time passwords which:**		✓				
			One-time passwords	✓				OPA#0070	**a)**		**are generated using an approved block-cipher or hash function to combine a symmetric key, stored on the device, with a nonce; or**		✓				
			One-time passwords	✓				OPA#0070	**b)**		**derive the nonce from a date and time, or a counter, which is generated on the device; or**		✓				
			One-time passwords	✓				OPA#0070	**c)**		**have a limited lifetime, in the order of minutes.**		✓				

OP_SAC SAC / SoCA v2.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
			System threat risk assessment and controls	✓				OPA#0080			Account for the following system threats and apply appropriate controls:	✓	✓	✓	✓		This is a MANDATORY criterion The following list is not be considered to be a complete list of threats to be addressed by the risk assessment, the scope of which should be determined and justified by the CSP. The risk assessment should address these threats from any perspective in which they might adversely affect the operation of the service, whether they be from within the organization (e.g. in its development environment, the hosting environment) or without (e.g. network attacks, hackers).
			System threat risk assessment and controls	✓				OPA#0080	a)		the introduction of malicious code;	✓	✓	✓	✓		
			System threat risk assessment and controls	✓				OPA#0080	b)		compromised authentication arising from insider action;	✓	✓	✓	✓		
			System threat risk assessment and controls	✓				OPA#0080	c)		out-of-band attacks by other users and system operators (e.g., the ubiquitous shoulder-surfing);	✓	✓	✓	✓		
			System threat risk assessment and controls	✓				OPA#0080	d)		spoofing of system elements/applications;	✓	✓	✓	✓		
			System threat risk assessment and controls	✓				OPA#0080	e)		malfeasance on the part of Subscribers and Subjects.	✓	✓	✓	✓		
			System threat risk assessment and controls	✓				OPA#0080	**f)**		**intrusions leading to information theft.**		✓	✓	✓		
			System threat risk assessment and controls	✓				OPA#0080			**The above list shall not be considered to be a complete list of threats to be addressed by the risk assessment.**			✓	✓		
			Specified Service's Key Management	✓				OPA#0090			**Specify and observe procedures and processes for the generation, storage, and destruction of its own cryptographic keys used for securing the specific service's assertions and other publicized information. At a minimum, these should address:**		✓	✓	✓		
			Specified Service's Key Management	✓				OPA#0090	a)		**the physical security of the environment;**		✓	✓	✓		
			Specified Service's Key Management	✓				OPA#0090	b)		**access control procedures limiting access to the minimum number of authorized personnel;**		✓	✓	✓		
			Specified Service's Key Management	✓				OPA#0090	c)		**public-key publication mechanisms;**		✓	✓	✓		
			Specified Service's Key Management	✓				OPA#0090	d)		**application of controls deemed necessary as a result of the service's risk assessment;**		✓	✓	✓		
			Specified Service's Key Management	✓				OPA#0090	e)		**destruction of expired or compromised private keys in a manner that prohibits their retrieval, or their archival in a manner which prohibits their reuse;**		✓	✓	✓		
			Specified Service's Key Management	✓				OPA#0090	f)		**applicable cryptographic module security requirements, quoting [IS19790] or equivalent, as established by a recognized national technical authority.**		✓	✓	✓		
		Storage of Long-term Secrets															
			Stored Secret Encryption (shared secrets)	✓				OPA#0100			**Encrypt such shared secret files so that:**			✓			
			Stored Secret Encryption (shared secrets)	✓				OPA#0100	**a)**		**the encryption key for the shared secret file is encrypted under a key held in an [IS19790]Level 2 or higher validated hardware or software cryptographic module or any [IS19790] Level 3 or 4 cryptographic module, or equivalent, as established by a recognized national technical authority;**			✓			
			Stored Secret Encryption (shared secrets)	✓				OPA#0100	**b)**		**the shared secret file is decrypted only as immediately required for an authentication operation;**			✓			

OP_SAC SAC / SoCA v2.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
			Stored Secret Encryption (shared secrets)	✓				OPA#0100	c)		shared secrets are protected as a key within the boundary of an [IS19790] Level 2 or higher validated hardware cryptographic module or any [IS19790] Level 3 or 4 cryptographic module and are not exported from the module in plain text, or equivalent, as established by a recognized national technical authority;			✓			
			Stored Secret Encryption (shared secrets)	✓				OPA#0100	d)		shared secrets are split by an "n from m" cryptographic secret sharing method.			✓			
			Stored Secret Encryption	✓				OPA#0110			Encrypt such secret files so that:				✓		
			Stored Secret Encryption	✓				OPA#0110	a)		the encryption key for the secret file is encrypted under a key held in an [IS19790]Level 2 or higher validated hardware or software cryptographic module or any [IS19790] Level 3 or 4 cryptographic module, or equivalent, as established by a recognized national technical authority;				✓		
			Stored Secret Encryption	✓				OPA#0110	b)		the secret file is decrypted only as immediately required for an authentication operation;				✓		
			Stored Secret Encryption	✓				OPA#0110	c)		secrets are protected as a key within the boundary of an [IS19790] Level 2 or higher validated hardware cryptographic module or any [IS19790] Level 3 or 4 cryptographic module and are not exported from the module in plain text, or equivalent, as established by a recognized national technical authority;				✓		
			Stored Secret Encryption	✓				OPA#0110	d)		shared secrets are split by an "n from m" cryptographic secret storing method.				✓		
		Security-relevant Event (Audit) Records															
			Security event logs	✓				OPA#0120			Ensure that such audit records include:			✓	✓		This is a MANDATORY criterion.
			Security event logs	✓				OPA#0120	a)		the identity of the point of registration (irrespective of whether internal or outsourced);			✓	✓		
			Security event logs	✓				OPA#0120	b)		generation of the Subject's keys or the evidence that the Subject was in possession of both parts of their own key-pair;			✓	✓		
			Security event logs	✓				OPA#0120	c)		generation of the Subject's credential/certificate;			✓	✓		
			Security event logs	✓				OPA#0120	d)		dissemination of the Subject's credential/certificate;			✓	✓		
			Security event logs	✓				OPA#0120	e)		any revocation or suspension associated with the Subject's credential/certificate.			✓	✓		
		Operational infrastructure															
			Physical access control	✓				OPA#0130			Apply physical access control mechanisms to ensure that:		✓	✓	✓		
			Physical access control	✓				OPA#0130	a)		access to sensitive areas is restricted to authorized personnel;		✓	✓	✓		
			Physical access control	✓				OPA#0130	b)		all removable media and paper documents containing sensitive information as plain-text are stored in secure containers;		✓	✓	✓		
			Physical access control	✓				OPA#0130	c)		a minimum of two persons are required to enable access to any cryptographic modules;		✓	✓	✓		
			Physical access control	✓				OPA#0130	d)		there is 24/7 monitoring for unauthorized intrusions.			✓	✓		
			Logical access control	✓				OPA#0140			Employ logical access control mechanisms that ensure access to sensitive system functions and controls is restricted to authorized personnel.		✓	✓	✓		
		Secure communications															

OP_SAC SAC / SoCA v2.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
			Secure remote communications	✓				OPA#0140			If the specific service components are located remotely from and communicate over a public or unsecured network with other service components or other CSPs it services, or parties requiring access to the CSP's services, each transaction must be cryptographically protected using an encryption method approved by a recognized national technical authority or other generally-recognized authoritative body, by either:		✓	✓	✓		The reference to "parties requiring access to the CSP's services" is intended to cover SP 800-63's reference to RPs (see cross-mapped EZP 63 clause).
			Secure remote communications	✓				OPA#0140	a)		implementing mutually-authenticated protected sessions; or		✓	✓	✓		
			Secure remote communications	✓				OPA#0140	b)		time-stamped or sequenced messages signed by their source and encrypted for their recipient.		✓	✓	✓		
			Verification / Authentication confirmation messages	✓				OPA#0150			Ensure that any verification or confirmation of authentication messages, which assert either that a weakly bound credential is valid or that a strongly bound credential has not been subsequently revoked, is logically bound to the credential and that the message, the logical binding, and the credential are all transmitted within a single integrity-protected session between the service and the Verifier / Relying Party.		✓	✓	✓		
			Limited access to shared secrets	✓				OPA#0160			Ensure that:	✓	✓				
			Limited access to shared secrets	✓				OPA#0160	a)		access to shared secrets shall be subject to discretionary controls which permit access to those roles/applications needing such access;	✓	✓				
			Limited access to shared secrets	✓				OPA#0160	b)		stored shared secrets are not held in their plaintext form unless given adequate physical or logical protection;	✓	✓				
			Limited access to shared secrets	✓				OPA#0160	c)		any plaintext passwords or secrets are not transmitted across any public or unsecured network.	✓	✓				
			Limited access to shared secrets	✓				OPA#0160	d)		any long-term (i.e., not session) shared secrets are revealed only to the Subject or to the CSP's direct agents (bearing in mind (a) above).		✓				
			Limited access to shared secrets	✓				OPA#0160			In addition, these roles shall be defined and documented by the CSP in accordance with KIAF-1410 CO#0270		✓				
			Limited access to shared secrets	✓				OPA#0160			Ensure that:			✓			
			Limited access to shared secrets	✓				OPA#0160	a)		access to shared secrets shall be subject to discretionary controls which permit access to those roles/applications needing such access;			✓			
			Limited access to shared secrets	✓				OPA#0160	b)		stored shared secrets are **encrypted such that:**			✓			
			Limited access to shared secrets	✓				OPA#0160	b)	i)	the encryption key for the shared secret file is encrypted under a key held in either an [IS19790] Level 2 (or higher) validated hardware cryptographic module or any [IS19790] Level 3 or 4 validated cryptographic module, or equivalent, as established by a recognized national technical authority, and decrypted only as immediately required for an authentication operation;			✓			
			Limited access to shared secrets	✓				OPA#0160	b)	ii)	they are protected as a key within the boundary of either an [IS19790] Level 2 (or higher) validated hardware cryptographic module or any [IS19790] Level 3 or 4 validated cryptographic module, or equivalent, as established by a recognized national technical authority, and are not exported from the module in plaintext;			✓			
			Limited access to shared secrets	✓				OPA#0160	c)		no stipulation;			✓			
			Limited access to shared secrets	✓				OPA#0160	d)		any long-term (i.e., not session) shared secrets are revealed only to the Subject or to the CSP's direct agents (bearing in mind (a) above).			✓			

OP_SAC SAC / SoCA v2.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
			Limited access to shared secrets	✓				OPA#0160			In addition, these roles shall be defined and documented by the CSP in accordance with KIAF-1410 CO#0270			✓			
			Limited access to shared secrets	✓				OPA#0160			Ensure that:				✓		
			Limited access to shared secrets	✓				OPA#0160	a)		access to shared secrets shall be subject to discretionary controls which permit access to those roles/applications needing such access;				✓		
			Limited access to shared secrets	✓				OPA#0160	b)		stored shared secrets are **encrypted such that:**				✓		
			Limited access to shared secrets	✓				OPA#0160	b)	i)	the encryption key for the shared secret file is encrypted under a key held in either an [IS19790] Level 2 (or higher) validated hardware cryptographic module or any [IS19790] Level 3 or 4 validated cryptographic module, or equivalent, as established by a recognized national technical authority, and decrypted only as immediately required for an authentication operation;				✓		
			Limited access to shared secrets	✓				OPA#0160	b)	ii)	they are protected as a key within the boundary of either an [IS19790] Level 2 (or higher) validated hardware cryptographic module or any [IS19790] Level 3 or 4 validated cryptographic module, or equivalent, as established by a recognized national technical authority, and are not exported from the module in plaintext;				✓		
			Limited access to shared secrets	✓				OPA#0160	b)	iii)	**they are split by an "n from m" cryptographic secret-sharing method;**				✓		
			Limited access to shared secrets	✓				OPA#0160	c)		no stipulation;				✓		
			Limited access to shared secrets	✓				OPA#0160	d)		any long-term (i.e., not session) shared secrets are revealed only to the Subject and the CSP's direct agents (bearing in mind (a) above).				✓		
			Limited access to shared secrets	✓				OPA#0160			In addition, these roles should be defined and documented by the CSP in accordance with KIAF-1410 CO#$0270				✓		
			Logical protection of shared secrets	✓				OPA#0170			**Ensure that one of the alternative methods (below) is used to protect shared secrets:**		✓	✓			
			Logical protection of shared secrets	✓				OPA#0170	**a)**		**concatenation of the password to a salt and/or username which is then hashed with an Approved algorithm such that the computations used to conduct a dictionary or exhaustion attack on a stolen password file are not useful to attack other similar password files, or;**		✓	✓			
			Logical protection of shared secrets	✓				OPA#0170	**b)**		**encryption using an Approved algorithm and modes, and the shared secret decrypted only when immediately required for authentication, or;**		✓	✓			
			Logical protection of shared secrets	✓				OPA#0170	**c)**		**any secure method allowed to protect shared secrets at Level 3 or 4.**		✓	✓			
Part B - Credential Issuing																	
		Identity Proofing Policy															
			Unique service identity	✓				OPB#0010			Ensure that a unique identity is attributed to the specific service, such that credentials issued by it can be distinguishable from those issued by other services, including services operated by the same enterprise.	✓	✓	✓	✓		
			Unique Subject identity	✓				OPB#0020			Ensure that each applicant's identity is unique within the service's community of Subjects and uniquely associable with tokens and/or credentials issued to that identity.	✓					
			Unique Subject identity	✓				OPB#0020			Ensure that each applicant's identity is unique within the service's community of Subjects and uniquely associable with tokens and/or credentials issued to that identity.		✓	✓	✓		Cf. CM_OP-B_CRN#0020 which expresses a very similar requirement. Although presenting repetition for a single provider, if the identity-proofing functions and credential management functions are provided by separate CSPs, each needs to fulfill this requirement.

OP_SAC SAC / SoCA v2.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
			Published Proofing Policy	✓				OPB#0030			**Make available the Identity Proofing Policy under which it verifies the identity of applicants[1] in form, language, and media accessible to the declared community of users.**		✓	✓	✓		For an identity proofing service that is within the management scope of a credential management service provider, this should be the credential management service's definitive policy; for a stand-alone identity proofing service, the policy may be either that of a client who has imposed one through contract, the ID service's own policy, or a separate policy that explains how the client's policies will be complied-with.
			Adherence to Proofing Policy	✓				OPB#0040			**Perform all identity proofing strictly in accordance with its published Identity Proofing Policy.**		✓				
			Adherence to Proofing Policy	✓				OPB#0040			Perform all identity proofing strictly in accordance with its published Identity Proofing Policy, **through application of the procedures and processes set out in its Identity Proofing Practice Statement (IdPPS).**			✓	✓		
		Identity Verification															
			Identity Proofing classes	✓				OPB#0050			The enterprise or specific service:	✓	✓				
			Identity Proofing classes	✓				OPB#0050	a)		must include in its Service Definition at least one of the following classes of identity proofing service, and;	✓	✓				
			Identity Proofing classes	✓				OPB#0050	b)		may offer any additional classes of identity proofing service it chooses, subject to the nature and the entitlement of the CSP concerned;	✓	✓				
			Identity Proofing classes	✓				OPB#0050	c)		must fulfill the applicable assessment criteria according to its choice of identity proofing service, i.e. conform to at least one of the criteria sets defined in:	✓	✓				
			Identity Proofing classes	✓				OPB#0050	c)	*i)*	OPB#0070 - '#0110 inc. "In-Person Public Identity Proofing";	✓	✓				
			Identity Proofing classes	✓				OPB#0050	c)	*ii)*	OPB#0120 & '#0130 "Remote Public Identity Proofing".	✓	✓				
			Identity Proofing classes	✓				OPB#0050	c)	***iii)***	**OPB#0140 & '#0150 Current Relationship Identity Proofing**		✓				
			Identity Proofing classes	✓				OPB#0050	c)	***iv)***	**OPB#0160 - '#0180 inc., "Affiliation Identity Proofing";**		✓				
			Identity Proofing classes	✓				OPB#0050			**although, in any of the above cases, the criteria defined in OPB#0190 - '#0210 inc., may be substituted for identity proofing where the Applicant already possesses a recognized credential at Level 3 or 4.**		✓				
			Identity Proofing classes	✓				OPB#0050			The enterprise or specific service:			✓			
			Identity Proofing classes	✓				OPB#0050	a)		must include in its Service Definition at least one of the following classes of identity proofing service, and;			✓			
			Identity Proofing classes	✓				OPB#0050	b)		may offer any additional classes of identity proofing service it chooses, Subject to the nature and the entitlement of the CSP concerned;			✓			
			Identity Proofing classes	✓				OPB#0050	c)		must fulfill the applicable assessment criteria according to its choice of identity proofing service, i.e. conform to at least one of the criteria sets, at the applicable LoA, defined in:			✓			
			Identity Proofing classes	✓				OPB#0050	c)	*i)*	OPB#0070 - '#0110 inclusive - "In-Person Public Identity Verification";			✓			
			Identity Proofing classes	✓				OPB#0050	***c)***	***ii)***	**OPB#0120 & '#0130 "Remote Public Identity Verification";**			✓			
			Identity Proofing classes	✓				OPB#0050	***c)***	***iii)***	**OPB#0140 & '#0150 Current Relationship Identity Proofing**			✓			
			Identity Proofing classes	✓				OPB#0050	***c)***	***iv)***	OPB#0160 - '#0180 inc., "Affiliation Identity Verification";			✓			
			Identity Proofing classes	✓				OPB#0050			**although, in any of the above cases, the criteria defined in OPB#0190 - '#0210 inc. may be substituted for identity proofing where the Applicant already possesses a recognized credential at Level 4.**			✓			

OP_SAC SAC / SoCA v2.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
			Identity Proofing classes	✓				OPB#0050			The enterprise or specific service must offer only in-person identity proofing as defined in OPB#0070 - '#0110 inclusive. Remote verification is not allowed at this assurance level;				✓		
			Identity Verification Measures	✓				OPB#0060			For each identity proofing service offered (see above [i.e. OPB#0050]) justify the identity verification measures applied by describing how these meet or exceed the requirements of applicable policies, regulations, adopted standards and other relevant conditions in order to maintain a level of rigour consistent with the applicable Assurance Level.		✓				Although strict requirements for identity proofing and verification can be defined, a real-world approach must account for instances where there is not 100% certitude. To cope with this CSPs need to have a set of prescribed (through policy – see OP-B_ID_POL#0030) and applied measures (see OP-B_ID_POL#0040) which observe policy, identify the measures taken according to the degree of certitude determined by each step in the verification process and what additional measures are taken. The CSP must present a case which shows that their solution is sufficient to ensure that the basic requirements of the applicable AL are met or exceeded. Note that in each set of proofing service criteria below there are criteria with specific requirements for evidence checks and an additional criterion for 'secondary' checks, all of which have an interplay with these overall requirements to have a policy and practice statement and to demonstrate processes which sustain confidence that the applicable AL is being achieved. Even though a CSP may use the services of a component service for the performance of the identity-proofing within its own service, it still needs to ensure that its policy is both justified and upheld. Where another service provider is used appropriate stipulations in contracts should be established, but any internal adherence to (e.g.) 'POL#040 should be determined by the fact that the component service is already Kantara Approved.
			Identity Verification Measures	✓				OPB#0060			For each identity proofing service offered (see above [i.e. OPB#0050]) justify the identity verification measures described in its IdPPS (see OPB#0040) by describing how these meet or exceed the requirements of applicable policies, regulations, adopted standards and other relevant conditions in order to maintain a level of rigour consistent with the AL3.			✓			see loA2 guidance
			Identity Verification Measures	✓				OPB#0060			Justify the identity verification measures described in its IdPPS (see OPB#0040) by describing how these meet or exceed the requirements of applicable policies, regulations, adopted standards and other relevant conditions in order to maintain a level of rigour consistent with the AL4.				✓		see loA2 guidance.
		In-Person Public Identity Proofing															
			Required evidence (in-person)	✓				OPB#0070			Require the applicant to provide a contact telephone number or email address.	✓					
			Required evidence (in-person)	✓				OPB#0070			**Ensure that the applicant is in possession of a primary Government Picture ID document that bears a photographic image of the holder.**		✓	✓			
			Required evidence (in-person)	✓				OPB#0070			Ensure that the applicant is in possession of:				✓		
			Required evidence (in-person)	✓				OPB#0070	*a)*		a primary Government Picture ID document that bears a photographic image of the holder **and either:**				✓		
			Required evidence (in-person)	✓				OPB#0070	***a)***	***i)***	**secondary Government Picture ID or an account number issued by a regulated financial institution or;**				✓		
			Required evidence (in-person)	✓				OPB#0070	***a)***	***ii)***	**two items confirming name, and address or telephone number, such as: utility bill, professional license or membership, or other evidence of equivalent standing.**				✓		
			Evidence checks (in-person)	✓				OPB#0080			Accept self-attestation of evidence.	✓					

OP_SAC SAC / SoCA v2.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
			Evidence checks (in-person)	✓				OPB#0080			Have in place and apply processes which ensure that the presented document:		✓				
			Evidence checks (in-person)	✓				OPB#0080	a)		appears to be a genuine document properly issued by the claimed issuing authority and valid at the time of application;		✓				
			Evidence checks (in-person)	✓				OPB#0080	b)		bears a photographic image of the holder that matches that of the applicant;		✓				
			Evidence checks (in-person)	✓				OPB#0080	c)		provides all reasonable certainty that the identity exists and that it uniquely identifies the applicant.		✓				
			Evidence checks (in-person)	✓				OPB#0080			Have in place and apply processes which ensure that the presented document:			✓			
			Evidence checks (in-person)	✓				OPB#0080	a)		appears to be a genuine document properly issued by the claimed issuing authority and valid at the time of application;			✓			
			Evidence checks (in-person)	✓				OPB#0080	b)		bears a photographic image of the holder that matches that of the applicant;			✓			
			Evidence checks (in-person)	✓				OPB#0080	c)		is electronically verified by a record check with the specified issuing authority or through similar databases that:			✓			
			Evidence checks (in-person)	✓				OPB#0080	c)	i)	establishes the existence of such records with matching name and reference numbers;			✓			
			Evidence checks (in-person)	✓				OPB#0080	c)	ii)	corroborates date (year, month and day) of birth, current address of record, and other personal information sufficient to ensure a unique identity;			✓			
			Evidence checks (in-person)	✓				OPB#0080	d)		provides all reasonable certainty that the identity exists and that it uniquely identifies the applicant.			✓			
			Evidence checks – primary ID	✓				OPB#0090			Ensure that the presented document: a)				✓		
			Evidence checks – primary ID	✓				OPB#0090	a)		appears to be a genuine document properly issued by the claimed issuing authority and valid at the time of application;				✓		
			Evidence checks – primary ID	✓				OPB#0090	b)		bears a photographic image of the holder which matches that of the applicant;				✓		
			Evidence checks – primary ID	✓				OPB#0090	c)		is electronically verified by a record check with the specified issuing authority or through similar databases that:				✓		
			Evidence checks – primary ID	✓				OPB#0090	c)	i)	establishes the existence of such records with matching name and reference numbers;				✓		
			Evidence checks – primary ID	✓				OPB#0090	c)	ii)	corroborates date (year, month and day) of birth, current address of record, and other personal information sufficient to ensure a unique identity;				✓		
			Evidence checks – primary ID	✓				OPB#0090	d)		provides all reasonable certainty, at AL4, that the identity exists and that it uniquely identifies the applicant.				✓		
			Evidence checks – secondary ID	✓				OPB#0100			Ensure that the presented document meets the following conditions:				✓		
			Evidence checks – secondary ID	✓				OPB#0100	a)		If it is secondary Government Picture ID:				✓		
			Evidence checks – secondary ID	✓				OPB#0100	a)	i)	appears to be a genuine document properly issued by the claimed issuing authority and valid at the time of application;				✓		
			Evidence checks – secondary ID	✓				OPB#0100	a)	ii)	bears a photographic image of the holder which matches that of the applicant;				✓		

OP_SAC SAC / SoCA v2.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
			Evidence checks – secondary ID	✓				OPB#0100	a)	iii)	states an address at which the applicant can be contacted.				✓		
			Evidence checks – secondary ID	✓				OPB#0100	b)		If it is a financial institution account number, is verified by a record check with the specified issuing authority or through similar databases that:				✓		
			Evidence checks – secondary ID	✓				OPB#0100	b)	i)	establishes the existence of such records with matching name and reference numbers;				✓		
			Evidence checks – secondary ID	✓				OPB#0100	b)	ii)	corroborates date (year, month and day) of birth, current address of record, and other personal information sufficient to ensure a unique identity.				✓		
			Evidence checks – secondary ID	✓				OPB#0100	c)		If it is two utility bills or equivalent documents:				✓		
			Evidence checks – secondary ID	✓				OPB#0100	c)	i)	each appears to be a genuine document properly issued by the claimed issuing authority;				✓		
			Evidence checks – secondary ID	✓				OPB#0100	c)	ii)	corroborates current address of record or telephone number sufficient to ensure a unique identity.				✓		
			Applicant knowledge checks	✓				OPB#0110			Where the applicant is unable to satisfy any of the above requirements, that the applicant can provide a unique identifier, such as a Social Security Number (SSN), that matches the claimed identity.				✓		
		Remote Public Identity Verification															
			Required evidence (remote)	✓				OPB#0120			Require the applicant to provide a contact telephone number or email address.	✓					
			Required evidence (remote)	✓				OPB#0120			Ensure that the applicant submits the references of and attests to current possession of a primary Government ID document, and one of:		✓				
			Required evidence (remote)	✓				OPB#0120	a)		a second Government ID;		✓				
			Required evidence (remote)	✓				OPB#0120	b)		an employee or student ID number;		✓				
			Required evidence (remote)	✓				OPB#0120	c)		a financial account number (e.g., checking account, savings account, loan or credit card);		✓				
			Required evidence (remote)	✓				OPB#0120	d)		a utility service account number (e.g., electricity, gas, or water) for an address matching that in the primary document; or		✓				
			Required evidence (remote)	✓				OPB#0120	e)		a telephone service account.		✓				
			Required evidence (remote)	✓				OPB#0120			Ensure that the applicant provides additional verifiable personal information that at a minimum must include:		✓				
			Required evidence (remote)	✓				OPB#0120	f)		a name that matches the referenced ID;		✓				
			Required evidence (remote)	✓				OPB#0120	g)		date (year, month and day) of birth and;		✓				
			Required evidence (remote)	✓				OPB#0120	h)		current address;		✓				
			Required evidence (remote)	✓				OPB#0120	i)		for a telephone service account, the demonstrable ability to send or receive messages at the phone number.		✓				
			Required evidence (remote)	✓				OPB#0120			Additional information may be requested so as to ensure a unique identity, and alternative information may be sought where the enterprise can show that it leads to at least the same degree of certitude when verified.		✓				
			Required evidence (remote)	✓				OPB#0120			Ensure that the applicant submits the references of and attests to current possession of a primary Government ID document, and one of:			✓			
			Required evidence (remote)	✓				OPB#0120	a)		a second Government ID;			✓			
			Required evidence (remote)	✓				OPB#0120	b)		an employee or student ID number;			✓			
			Required evidence (remote)	✓				OPB#0120	c)		a financial account number (e.g., checking account, savings account, loan or credit card);			✓			
			Required evidence (remote)	✓				OPB#0120	d)		a utility service account number (e.g., electricity, gas, or water) for an address matching that in the primary document;			✓			
			Required evidence (remote)	✓				OPB#0120	e)		No stipuation.			✓			

OP_SAC SAC / SoCA v2.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
			Required evidence (remote)	✓				OPB#0120			Ensure that the applicant provides additional verifiable personal information that at a minimum must include:			✓			
			Required evidence (remote)	✓				OPB#0120	f)		a name that matches the referenced ID;			✓			
			Required evidence (remote)	✓				OPB#0120	g)		date (year, month and day) of birth and;			✓			
			Required evidence (remote)	✓				OPB#0120	h)		current address;			✓			
			Required evidence (remote)	✓				OPB#0120	i)		for a telephone service account, the demonstrable ability to send or receive messages at the phone number.			✓			
			Required evidence (remote)	✓				OPB#0120			Additional information may be requested so as to ensure a unique identity, and alternative information may be sought where the enterprise can show that it leads to at least the same degree of certitude when verified.			✓			
			Evidence checks (remote)	✓				OPB#0130			Verify the provided information by either:	✓					
			Evidence checks (remote)	✓				OPB#0130	a)		confirming the request by calling the number;	✓					
			Evidence checks (remote)	✓				OPB#0130	b)		successfully sending a confirmatory email and receiving a positive acknowledgement.	✓					
			Evidence checks (remote)	✓				OPB#0130			**Perform inspection and analysis of records against the provided identity references with the specified issuing authorities/institutions or through similar databases, according to the inspection rules set by the issuing authorities:**		✓				
			Evidence checks (remote)	✓				OPB#0130	**a)**		**the existence of such records with matching name and reference numbers;**		✓				
			Evidence checks (remote)	✓				OPB#0130	**b)**		**corroboration of date (year, month and day) of birth, current contact information of record, and other personal information sufficient to ensure a unique identity;**		✓				
			Evidence checks (remote)	✓				OPB#0130	**c)**		**for a utility account, dynamic verification of personal information previously provided by or likely to be known only by the applicant;**		✓				
			Evidence checks (remote)	✓				OPB#0130	**d)**		**for a telephone service account, confirmation that the phone number supplied by the applicant is associated in Records with the Applicant's name and address of record and by having the applicant demonstrate that they are able to send or receive messages at the phone number.**		✓				
			Evidence checks (remote)	✓				OPB#0130			**Confirm contact information of record by at least one of the following means, ensuring that any secret sent over an unprotected channel shall be reset upon first use and shall be valid for a maximum lifetime of seven days:**		✓				
			Evidence checks (remote)	✓				OPB#0130	**e)**		**RA sends notice to an address of record confirmed in the records check and receives a mailed or telephonic reply from applicant;**		✓				
			Evidence checks (remote)	✓				OPB#0130	**f)**		**RA issues credentials in a manner that confirms the address of record supplied by the applicant, for example by requiring applicant to enter on-line some information from a notice sent to the applicant;**		✓				
			Evidence checks (remote)	✓				OPB#0130	**g)**		**RA issues credentials in a manner that confirms ability of the applicant to receive telephone communications at telephone number or email at email address associated with the applicant in records;**		✓				
			Evidence checks (remote)	✓				OPB#0130	**h)**		**Not Stipulated.**		✓				

OP_SAC SAC / SoCA v2.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
			Evidence checks (remote)	✓				OPB#0130			**Additional checks may be performed so as to establish the uniqueness of the claimed identity (see OPB#0220). Alternative checks may be performed where the enterprise can show that they lead to a comparable degree of certitude (see OPB#0220).**		✓				
			Evidence checks (remote)	✓				OPB#0130			**Electronically verify by a record check** against the provided identity references with the specified issuing authorities/institutions or through similar databases, according to the inspection rules set by the issuing authorities:			✓			
			Evidence checks (remote)	✓				OPB#0130	a)		the existence of such records with matching name and reference numbers;			✓			
			Evidence checks (remote)	✓				OPB#0130	b)		corroboration of date (year, month and day) of birth, current contact information of record, and other personal information sufficient to ensure a unique identity;			✓			
			Evidence checks (remote)	✓				OPB#0130	c)		for a utility account, dynamic verification of personal information previously provided by or likely to be known only by the applicant;			✓			
			Evidence checks (remote)	✓				OPB#0130	d)		for a telephone service account, confirmation that the phone number supplied by the applicant is associated in Records with the Applicant's name and address of record and by having the applicant demonstrate that they are able to send or receive messages at the phone number.			✓			
			Evidence checks (remote)	✓				OPB#0130			Confirm contact information of record by at least one of the following means, ensuring that any secret sent over an unprotected channel shall be reset upon first use and shall be valid for a maximum lifetime of seven days:			✓			
			Evidence checks (remote)	✓				OPB#0130	e)		RA sends notice to an address of record confirmed in the records check and receives a mailed or telephonic reply from applicant;			✓			
			Evidence checks (remote)	✓				OPB#0130	f)		RA issues credentials in a manner that confirms the address of record supplied by the applicant, for example by requiring applicant to enter on-line some information from a notice sent to the applicant;			✓			
			Evidence checks (remote)	✓				OPB#0130	g)		RA issues credentials in a manner that confirms ability of the applicant to receive telephone communications at telephone number or email at email address associated with the applicant in records.			✓			
			Evidence checks (remote)	✓				OPB#0130	h)		No stipulation.			✓			
			Evidence checks (remote)	✓				OPB#0130			Additional checks may be performed so as to establish the uniqueness of the claimed identity (see OPB#0220). Alternative checks may be performed where the enterprise can show that they lead to a comparable degree of certitude (see OPB#0220).			✓			
		Current Relationship Identity Proofing															
			Required evidence (current)	✓				OPB#0140			**Ensure that it has previously exchanged with the applicant a shared secret (e.g., a PIN or password) that meets AL2 (or higher) entropy requirements).**		✓				Refer to NIST SP 800-63 "Appendix A: Estimating Entropy and Strength" or similar recognized sources of such information.
			Required evidence (current)	✓				OPB#0140			Ensure that it has previously exchanged with the applicant a shared secret (e.g., a PIN or password) that meets AL**3** (or higher) entropy requirements).			✓			See AL2 guidance.
			Evidence Checks (current)	✓				OPB#0150			**Ensure that it has:**		✓				
			Evidence Checks (current)	✓				OPB#0150	**a)**		**only issued the shared secret after originally establishing the applicant's identity:**		✓				

OP_SAC SAC / SoCA v2.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
			Evidence Checks (current)	✓				OPB#0150	a)	i)	with a degree of rigor equivalent to that required under either the AL2 (or higher) requirements for in-person or remote public verification; or		✓				
			Evidence Checks (current)	✓				OPB#0150	a)	ii)	by complying with regulatory requirements effective within the applicable jurisdiction which set forth explicit proofing requirements which include a prior in-person appearance by the applicant and are defined as meeting AL2 (or higher) requirements;		✓				
			Evidence Checks (current)	✓				OPB#0150	b)		an ongoing business relationship sufficient to satisfy the enterprise of the applicant's continued personal possession of the shared secret.		✓				
			Evidence Checks (current)	✓				OPB#0150			Ensure that it has:			✓			
			Evidence Checks (current)	✓				OPB#0150	a)		only issued the shared secret after originally establishing the applicant's identity:			✓			
			Evidence Checks (current)	✓				OPB#0150	a)	i)	with a degree of rigor equivalent to that required under either the AL3 (or higher) requirements for in-person or remote public verification; or			✓			
			Evidence Checks (current)	✓				OPB#0150	a)	ii)	by complying with regulatory requirements effective within the applicable jurisdiction which set forth explicit proofing requirements which include a prior in-person appearance by the applicant and are defined as meeting AL3 (or higher) requirements;			✓			
			Evidence Checks (current)	✓				OPB#0150	b)		an ongoing business relationship sufficient to satisfy the enterprise of the applicant's continued personal possession of the shared secret.			✓			
		Afffiliation Identity Proofing															
			Meet preceding criteria	✓				OPB#0160			Meet all the criteria set out above, under OP#0120 & '#0130 - "Remote Public Identity Verification".		✓	✓			
			Meet preceding criteria	✓				OPB#0160			Meet all the criteria set out above, under OPB0070 - '#0110 inc. - "In-Person Public Identity Verification".				✓		
			Required evidence (affiliated)	✓				OPB#0170			Ensure that the applicant possesses:		✓	✓	✓		
			Required evidence (affiliated)	✓				OPB#0170	a)		identification from the organization with which it is claiming affiliation;		✓	✓	✓		
			Required evidence (affiliated)	✓				OPB#0170	b)		agreement from the organization that the applicant may be issued a credential indicating that an affiliation exists.		✓	✓	✓		
			Evidence checks (affiliated)	✓				OPB#0180			Have in place and apply processes which ensure that the presented documents:		✓	✓	✓		
			Evidence checks (affiliated)	✓				OPB#0180	a)		each appear to be a genuine document properly issued by the claimed issuing authorities and valid at the time of application;		✓	✓	✓		
			Evidence checks (affiliated)	✓				OPB#0180	b)		refer to an existing organization with a contact address;		✓	✓	✓		
			Evidence checks (affiliated)	✓				OPB#0180	c)		indicate that the applicant has some form of recognizable affiliation with the organization;		✓	✓	✓		
			Evidence checks (affiliated)	✓				OPB#0180	d)		appear to grant the applicant an entitlement to obtain a credential indicating an affiliation with the organization.		✓	✓	✓		
		Issuing Derived Credentials															
			Authenticate Original Credential	✓				OPB#0190			Prior to issuing any derived credential the original credential on which the identity-proofing relies must be proven to be in the possession and under the control of the Applicant.	✓					This is the equivalent of recording the details of identity-proofing documents provided during (e.g.) face-face id-proofing. It is not required that the original credential be issued by a Kantara-Approved CSP.
			Authenticate Original Credential	✓				OPB#0190			Prior to issuing any derived credential the original credential on which the identity-proofing relies must be:		✓				

OP_SAC SAC / SoCA v2.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
			Authenticate Original Credential	✓				OPB#0190	**a)**		**authenticated by a source trusted by the CSP as being valid and un-revoked;**		✓				
			Authenticate Original Credential	✓				OPB#0190	**b)**		**issued at Assurance Level 3 or 4;**		✓				
			Authenticate Original Credential	✓				OPB#0190	**c)**		**issued in the same name as that which the Applicant is claiming;**		✓				
			Authenticate Original Credential	✓				OPB#0190	d)		proven to be in the possession and under the control of the Applicant.		✓				
			Authenticate Original Credential	✓				OPB#0190			Prior to issuing any derived credential the original credential on which the identity-proofing relies must be:			✓			
			Authenticate Original Credential	✓				OPB#0190	a)		authenticated by a source trusted by the CSP as being valid and un-revoked;			✓			
			Authenticate Original Credential	✓				OPB#0190	**b)**		**issued at Assurance Level 4;**			✓			
			Authenticate Original Credential	✓				OPB#0190	c)		issued in the same name as that which the Applicant is claiming;			✓			
			Authenticate Original Credential	✓				OPB#0190	d)		proven to be in the possession and under the control of the Applicant.			✓			
			Authenticate Original Credential	✓				OPB#0190			Prior to issuing any derived credential the original credential on which the identity-proofing relies must be:				✓		
			Authenticate Original Credential	✓				OPB#0190	a)		authenticated by a source trusted by the CSP as being valid and un-revoked;				✓		
			Authenticate Original Credential	✓				OPB#0190	b)		issued at Assurance Level 4;				✓		
			Authenticate Original Credential	✓				OPB#0190	c)		issued in the same name as that which the Applicant is claiming;				✓		
			Authenticate Original Credential	✓				OPB#0190	d)		proven to be in the possession and under the control of the Applicant, **who shall be physically present.**				✓		
			Record Original Credential	✓				OPB#0200			**Record the details of the original credential.**		✓				
			Record Original Credential	✓				OPB#0200			**Before issuing the derived credential ensure that:**			✓			
			Record Original Credential	✓				OPB#0200	**a)**		**for in-person issuance, the claimant is the Applicant;**			✓			
			Record Original Credential	✓				OPB#0200	**b)**		**for remote issuance, token activation requires proof of possession of both the derived token and the original Level 4 token.**			✓			
			Record Original Credential	✓				OPB#0200			**Record the details of the original credential, the biometric sample related to the original credential and the biometric sample captured when authenticating the Applicant.**				✓		
			Issue Derived Credential	✓				OPB#0210			**Before issuing the derived credential ensure that:**		✓				
			Issue Derived Credential	✓				OPB#0210	**a)**		**for in-person issuance, the claimant is the Applicant;**		✓				
			Issue Derived Credential	✓				OPB#0210	**b)**		**for remote issuance, token activation requires proof of possession of both the derived token and the original Level 3 or Level 4 token.**		✓				
			Issue Derived Credential	✓				OPB#0210			Before issuing the derived credential ensure that:			✓			
			Issue Derived Credential	✓				OPB#0210	a)		for in-person issuance, the claimant is the Applicant;			✓			
			Issue Derived Credential	✓				OPB#0210	b)		for remote issuance, token activation requires proof of possession of both the derived token and the original **Level 4** token.			✓			
			Issue Derived Credential	✓				OPB#0210			**Only issue the derived credential in-person after performing biometric authentication of the Applicant.**				✓		
		Secondary Identity Verification															
			Secondary checks	✓				OPB#0220			In each proofing class which the service supports, there must be in place additional measures (e.g., require additional documentary evidence, delay completion while out-of-band checks are undertaken) to deal with:	✓					

OP_SAC SAC / SoCA v2.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
			Secondary checks	✓				OPB#0220	a)		any reasonably anomalous circumstances that can be reasonably anticipated (e.g., a legitimate and recent change of address that has yet to be established as the address of record);	✓					
			Secondary checks	✓				OPB#0220	b)		any use of processes and/or technologies which may not fully meet the preceding applicable requirements but which are deemed to be comparable and thus able to support AL1.	✓					
			Secondary checks	✓				OPB#0220			In each proofing class which the service supports, there must be in place additional measures (e.g., require additional documentary evidence, delay completion while out-of-band checks are undertaken) to deal with:		✓				
			Secondary checks	✓				OPB#0220	a)		any reasonably anomalous circumstances that can be reasonably anticipated (e.g., a legitimate and recent change of address that has yet to be established as the address of record);		✓				
			Secondary checks	✓				OPB#0220	b)		any use of processes and/or technologies which may not fully meet the preceding applicable requirements but which are deemed to be comparable and thus able to support **AL2.**		✓				
			Secondary checks	✓				OPB#0220			In each proofing class which the service supports, there must be in place additional measures (e.g., require additional documentary evidence, delay completion while out-of-band checks are undertaken) to deal with:			✓			
			Secondary checks	✓				OPB#0220	a)		any reasonably anomalous circumstances that can be reasonably anticipated (e.g., a legitimate and recent change of address that has yet to be established as the address of record);			✓			
			Secondary checks	✓				OPB#0220	b)		any use of processes and/or technologies which may not fully meet the preceding applicable requirements but which are deemed to be comparable and thus able to support **AL3.**			✓			
			Secondary checks	✓				OPB#0220			**In each proofing class which the service supports, there must be in place additional measures (e.g., require additional documentary evidence, delay completion while out-of-band checks are undertaken) to deal with any anomalous circumstances that can reasonably be anticipated (e.g., a legitimate and recent change of address that has yet to be established as the address of record).**				✓		
		Identity-proofing Records															
			Verification Records for Personal Applicants	✓				OPB#0230			**Log, taking account of all applicable legislative and policy obligations, a record of the facts of the verification process, including a reference relating to the verification processes, the date and time of verification and the identity of the registrar (person, or entity if remote or automatic) performing the proofing functions.**		✓	✓			The facts of the verification process should include the specific record information (source, unique reference, value/content) used in establishing the applicant's identity, and will be determined by the specific processes used and documents accepted by the CSP. The CSP need not retain these records itself if it uses a third-party service which retains such records securely and to which the CSP has access when required, in which case it must retain a record of the identity of the third-party service providing the verification service or the location at which the (in-house) verification was performed.
			Verification Records for Personal Applicants	✓				OPB#0230			Log, taking account of all applicable legislative and policy obligations, a record of the facts of the verification process and the identity of the registrar (person, or entity if remote or automatic) performing the proofing functions, including a reference relating to the verification processes and the date and time of verification **issued by a trusted time-source**.				✓		See AL2 guidance.

OP_SAC SAC / SoCA v2.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
			Verification Records for Affiliated Applicants	✓				OPB#0240			In addition to the foregoing, log, taking account of all applicable legislative and policy obligations, a record of the additional facts of the verification process.		✓	✓	✓	In scope - Not applicable	Although there is no specific stipulation as to what should be recorded the list below suggests identity information which would typically be captured, with increasing levels of assurance requiring greater amounts of information andsd stronger verification of it. : a) the Subject's full name; b) the Subject's dob (ccyy-mm-dd) c) the Subject's current address of record; d) the Subject's current telephone or email address of record; e) the Subscriber's authorization for issuing the Subject a credential; f) type, issuing authority, and reference number(s) of all documents checked in the identity proofing process; g) a biometric record of each required representative of the affiliating organization (e.g., a photograph, fingerprint, voice recording), as determined by that organization's governance rules/charter.
			Provide Subject identity records	✓				OPB#0250			If required, provide to qualifying parties a unique identity for each Subscriber and their associated tokens and credentials to the extent permitted by applicable legislation and/or agreed by the Subscriber.	✓					The qualifier 'if required' is intended to account for circumstances where conditions such as whether a contract or a federation policy permits or is required or jurisdiction / legal injunction demand such provision. A qualifying party is any party to which provision of such info can justified according to circumstance: by contract/policy; with Subject's agreement; with due authority (Court Order, e.g.). The CSP needs to make the case, according to their service's characteristics and operating environment.
			Provide Subject identity records	✓				OPB#0250			**If required, provide to qualifying parties records of identity proofing to the extent permitted by applicable legislation and/or agreed by the Subscriber.**		✓	✓	✓		See AL1 guidance.
			Record Retention	✓				OPB#0260			**Either retain, securely, the record of the verification process for the duration of the Subject account plus a further period sufficient to allow fulfillment of any period required legally, contractually or by any other form of binding agreement or obligation, or submit same record to a client CSP that has undertaken to retain the record for the requisite period or longer.**		✓	✓	✓		
			Revision to Subject Information	✓				OPB#0270			Provide a means for Subjects to amend their stored information after registration.	✓					The necessity for re-issuance will be determined by, inter alia, policy, the technology and practices in use, the nature of change (e.g. registration data not bound into the credential) and the nature of the proofing processes.
			Revision to Subject Information	✓				OPB#0270			Provide a means for Subjects to securely amend their stored information after registration, **either by re-proving their identity, as in the initial registration process, or by using their credentials to authenticate their revision. Successful revision must instigate the re-issuance of the credential when the data being revised are bound into the credential.**		✓	✓			See AL1 guidance.
			Revision to Subject Information	✓				OPB#0270			Provide a means for Subscribers and Subjects to securely amend their stored information after registration, either by re-proving their identity as in the initial registration process or by using their credentials to authenticate their revision. Successful revision must**, where necessary, instigate the re-issuance of the credential.**				✓		See AL1 guidance.
			Authenticate Subject Information Change	✓				OPB#0280			Permit only changes which are supported by appropriate and sufficient authentication of the legitimacy of change according, to its type.	✓	✓	✓			
		Credential Creation															

OP_SAC SAC / SoCA v2.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
			Authenticated Request	✓				OPB#0290			Only accept a request to generate a credential and bind it to an identity if the source of the request can be authenticated as being authorized to perform identity proofing at AL1 or higher.	✓					
			Authenticated Request	✓				OPB#0290			Only accept a request to generate a credential and bind it to an identity if the source of the request can be authenticated, **i.e., Registration Authority**, as being authorized to perform identity proofing at **AL2** or higher.		✓				
			Authenticated Request	✓				OPB#0290			Only accept a request to generate a credential and bind it to an identity if the source of the request, i.e., Registration Authority, can be authenticated as being authorized to perform identity proofing at **AL3** or higher.			✓			
			Authenticated Request	✓				OPB#0290			Only accept a request to generate a credential and bind it to an identity if the source of the request, i.e., Registration Authority, can be authenticated as being authorized to perform identity proofing at **AL4**.				✓		
			Unique identity	✓				OPB#0300			**Ensure that the identity which relates to a specific applicant is unique within the specified service, including identities previously used and that are now cancelled, other than its re-assignment to the same applicant.**		✓	✓	✓		This requirement is intended to prevent identities that may exist in a Relying Party's access control list from possibly representing a different physical person. Cf. OP-B_CM_POL#0020 which expresses a very similar requirement. Although presenting repetition for a single provider, if the identity-proofing functions and credential management functions are provided by separate CSPs, each needs to fulfill this requirement.
			Credential uniqueness	✓				OPB#0310			Allow the Subject to select a credential (e.g., UserID) that is verified to be unique within the specified service's community and assigned uniquely to a single identity Subject. Default names shall not be permitted. {source [5415] KI.10.3.2.1#04}	✓	✓	✓	✓		
			Convey credential	✓				OPB#0320			Be capable of conveying the unique identity information associated with a credential to Verifiers and Relying Parties.	✓	✓	✓	✓		
			Token strength	✓				OPB#0330			Ensure that the single-factor token associated with the credential has one of the following sets of characteristics:	✓					
			Token strength	✓				OPB#0330	a)		For a memorized secret, apply a rule-set such that there shall be a minimum of 14 bits of entropy in the pin or pass-phrase. Default values shall not be permitted;	✓					
			Token strength	✓				OPB#0330	b)		For a knowledge-based question, apply a rule-set such that there shall be:	✓					
			Token strength	✓				OPB#0330	b)	i)	a minimum of 14 bits of entropy in the pin or pass-phrase OR;	✓					
			Token strength	✓				OPB#0330	b)	ii)	a set of knowledge-based questions created by the user OR;	✓					
			Token strength	✓				OPB#0330	b)	iii)	a set of knowledge-based questions selected by the user from a service-generated list of at least five questions. Null or empty answers in any case above shall not be permitted.	✓					
			Token strength	✓				OPB#0330			Ensure that the single-factor token associated with the credential has one of the following sets of characteristics:		✓				
			Token strength	✓				OPB#0330	a)		For a memorized secret, apply a rule-set such that there shall be a minimum of **24** bits of entropy in the pin or pass-phrase. Default values shall not be permitted;		✓				
			Token strength	✓				OPB#0330	b)		For a knowledge-based question, apply a rule-set such that there shall be:		✓				
			Token strength	✓				OPB#0330	b)	i)	a minimum of **20** bits of entropy in the pin or pass-phrase OR;		✓				
			Token strength	✓				OPB#0330	b)	ii)	a set of knowledge-based questions created by the user OR;		✓				

OP_SAC SAC / SoCA v2.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
			Token strength	✓				OPB#0330	b)	iii)	a set of knowledge-based questions selected by the user from a service-generated list of at least **seven** questions. Null or empty answers in any case above shall not be permitted.		✓				
			Token strength	✓				OPB#0330	**c)**		**For a look-up token, apply a rule-set such that there shall be a minimum of 20 bits of entropy in the secret phrase(s);**		✓				
			Token strength	✓				OPB#0330	**d)**		**For an out-of-band token, ensure that the token is uniquely addressable and supports communication over a channel that is separate from the primary channel for e-authentication;**		✓				
			Token strength	✓				OPB#0330	**e)**		**For a one-time-password device, generate one-time passwords using an approved block cipher or hash function to combine a nonce and a symmetric key;**		✓				
			Token strength	✓				OPB#0330	**f)**		**Use a cryptographic device validated at [IS19790] Level 1 or higher or equivalent, as established by a recognized national technical authority.**		✓				
			Token strength	✓				OPB#0330			**_Not_ use PIN/password tokens.**			✓	✓		
			One-time password strength	✓				OPB#0340			**Only allow password tokens that have a resistance to online guessing attack against a selected user/password of at least 1 in 2^{14} (16,384), accounting for state-of-the-art attack strategies, and at least 10 bits of min-entropy.**		✓				
			One-time password strength	✓				OPB#0340			Only allow one-time password tokens that:			✓			
			One-time password strength	✓				OPB#0340	**a)**		**depend on a symmetric key stored on a personal hardware device validated against [IS19790] Level 1 or higher, or equivalent, as established by a recognized national technical authority;**			✓			
			One-time password strength	✓				OPB#0340	**b)**		**permit at least 106 possible password values;**			✓			
			One-time password strength	✓				OPB#0340	**c)**		**require password or biometric activation by the Subject.**			✓			
			One-time password strength	✓				OPB#0340			**_Not_ use one-time password tokens.**				✓		
			One-time password lifetime	✓				OPB#0340			**Set the minimum valid lifetime for the one-time password to a value commensurate with service usage and in no case greater than fifteen minutes.**		✓				
			Software cryptographic token strength	✓				OPB#0350			**Ensure that software cryptographic keys stored on general-purpose devices are protected by a key and cryptographic protocol that are validated against [IS19790] Level 1, or equivalent, as established by a recognized national technical authority.**		✓				
			Software cryptographic token strength	✓				OPB#0350			Ensure that software cryptographic keys stored on general-purpose devices:			✓			
			Software cryptographic token strength	✓				OPB#0350	**a)**		**are protected by a key and cryptographic protocol that are validated against [IS19790] Level 1, or equivalent, as established by a recognized national technical authority;**			✓			
			Software cryptographic token strength	✓				OPB#0350	**b)**		**require password or biometric activation by the Subject or employ a password protocol when being used for authentication;**			✓			
			Software cryptographic token strength	✓				OPB#0350	**c)**		**erase any unencrypted copy of the authentication key after each authentication.**			✓			
			Software cryptographic token strength	✓				OPB#0350			**_Not_ use software cryptographic tokens.**				✓		
			Hardware token strength	✓				OPB#0360			**Ensure that hardware tokens used to store cryptographic keys:**		✓				
			Hardware token strength	✓				OPB#0360	**a)**		**employ a cryptographic module that is validated against [IS19790] Level 1 or higher, or equivalent, as established by a recognized national technical authority;**		✓				

OP_SAC SAC / SoCA v2.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
			Hardware token strength	✓				OPB#0360	b)		are locked prior to their delivery, once personalization processes have been completed.		✓				
			Hardware token strength	✓				OPB#0360			Ensure that hardware tokens used to store cryptographic keys:			✓			
			Hardware token strength	✓				OPB#0360	a)		employ a cryptographic module that is validated against [IS19790] Level 1 or higher, or equivalent, as established by a recognized national technical authority;			✓			
			Hardware token strength	✓				OPB#0360	b)		require password or biometric activation by the Subject or also employ a password when being used for authentication;			✓			
			Hardware token strength	✓				OPB#0360	c)		erase any unencrypted copy of the authentication key after each authentication;			✓			
			Hardware token strength	✓				OPB#0360	d)		are locked prior to their delivery, once personalization processes have been completed.			✓			
			One-time password hardware token strength	✓				OPB#0361			Ensure that hardware tokens used to store cryptographic keys:				✓		This criterion's tag is iknсremented only by '1' since it is essentially thwe same purpose and function as #0360 but at level 4. Hpowever, it also has a different title and hence the tag is incremented to provide a unique match title to tag.
			One-time password hardware token strength	✓				OPB#0361	a)		employ a cryptographic module that is validated against [IS19790] Level 1 or higher, or equivalent, as established by a recognized national technical authority;				✓		
			One-time password hardware token strength	✓				OPB#0361	b)		require password or biometric activation by the Subject;				✓		
			One-time password hardware token strength	✓				OPB#0361	c)		Generate a one-time password using an algorithm recognized by a national technical authority;				✓		
			One-time password hardware token strength	✓				OPB#0361	d)		are locked prior to their delivery, once personalization processes have been completed.				✓		
			Multi-factor hardware cryptographic token strength	✓				OPB#0370			Ensure that hardware tokens used to store cryptographic keys:				✓		
			Multi-factor hardware cryptographic token strength	✓				OPB#0370	a)		employ a cryptographic module that is validated against [IS19790] Level 2 or higher, or equivalent, as determined by a recognized national technical authority;				✓		
			Multi-factor hardware cryptographic token strength	✓				OPB#0370	b)		are validated against [IS19790] Level 3 or higher, or equivalent, as determined by a recognized national technical authority, for their physical security;				✓		
			Multi-factor hardware cryptographic token strength	✓				OPB#0370	c)		require password, PIN or biometric activation by the Subject when being used for authentication;				✓		
			Multi-factor hardware cryptographic token strength	✓				OPB#0370	d)		do not permit the export of authentication keys;				✓		
			Multi-factor hardware cryptographic token strength	✓				OPB#0370	e)		are locked prior to their delivery, once personalization processes have been completed. {source [5415] KI.10.2.2.1#07}				✓		
			Binding	✓				OPB#0380			Ensure that the Subject is uniquely bound to the credential and remains so until the credential is securely delivered to the Subject.		✓				
			Binding of key	✓				OPB#0381			If the specified service generates the Subject's key pair, that the key generation process securely and uniquely binds that process to the certificate generation and maintains at all times the secrecy of the private key, until it is accepted by the Subject.			✓	✓		
			Hardware Inventory Control	✓				OPB#0390			Prior to issuance, if a credential, or the means to produce credentials, is held on a hardware device, the hardware device shall be kept physically secure and the inventory tracked.			✓	✓		

OP_SAC SAC / SoCA v2.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
			Nature of Subject	✓				OPB#0400			Record the nature of the Subject of the credential (which must correspond to the manner of identity proofing performed), i.e., physical person, a named person acting on behalf of a corporation or other legal entity, corporation or legal entity, or corporate machine entity, in a manner that can be unequivocally associated with the credential and the identity that it asserts.		✓	✓			
			Nature of Subject	✓				OPB#0400			Record the nature of the Subject of the credential, **i.e., private person,** a named person acting on behalf of a corporation or other legal entity, corporation or legal entity, or corporate machine entity, in a manner that can be unequivocally associated with the credential and the identity that it asserts.				✓		
			Pseudonym's Real Identity	✓				OPB#0410			If the credential is based upon a pseudonym this must be indicated in the credential and a record of the real identity retained.		✓				
		Subject Key Pair Generation															
			Key generation by Specified Service	✓				OPB#0420			If the specified service generates the Subject's keys:			✓	✓		
			Key generation by Specified Service	✓				OPB#0420	a)		use an [IS19790] compliant algorithm, or equivalent, as established by a recognized national technical authority, that is recognized as being fit for the purposes of the service;			✓	✓		
			Key generation by Specified Service	✓				OPB#0420	b)		only create keys of a key length and for use with an [IS19790] compliant public key algorithm, or equivalent, as established by a recognized national technical authority, recognized as being fit for the purposes of the service;			✓	✓		
			Key generation by Specified Service	✓				OPB#0420	c)		generate and store the keys securely until delivery to and acceptance by the Subject;			✓	✓		
			Key generation by Specified Service	✓				OPB#0420	d)		deliver the Subject's private key in a manner that ensures that the privacy of the key is not compromised and only the Subject has access to the private key.			✓	✓		
			Key generation by Subject	✓				OPB#0430			If the Subject generates and presents its own keys, obtain the Subject's written confirmation that it has:			✓	✓		
			Key generation by Subject	✓				OPB#0430	a)		used an [IS19790] compliant algorithm, or equivalent, as established by a recognized national technical authority, that is recognized as being fit for the purposes of the service;			✓	✓		
			Key generation by Subject	✓				OPB#0430	b)		created keys of a key length and for use with an [IS19790] compliant public key algorithm, or equivalent, as established by a recognized national technical authority, recognized as being fit for the purposes of the service.			✓	✓		
		Credential Delivery															
			Notify Subject of Credential Issuance	✓				OPB#0440			Notify the Subject of the credential's issuance and, if necessary, confirm the Subject's contact information by:		✓				The nature of issuance could mean that the Subject is fully aware and therefore no notification is necessary. If any other such circumstances prevailed, the CSP should identify them.
			Notify Subject of Credential Issuance	✓				OPB#0440	a)		sending notice to the address of record confirmed during identity proofing or;		✓				
			Notify Subject of Credential Issuance	✓				OPB#0440	b)		issuing the credential(s) in a manner that confirms the address of record supplied by the applicant during identity proofing or;		✓				
			Notify Subject of Credential Issuance	✓				OPB#0440	c)		issuing the credential(s) in a manner that confirms the ability of the applicant to receive telephone communications at a fixed-line telephone number or postal address supplied by the applicant during identity proofing.		✓				
			Notify Subject of Credential Issuance	✓				OPB#0440			Notify the Subject of the credential's issuance and, if necessary, confirm the Subject's contact information by:			✓			See LoA2 guidance.

OP_SAC SAC / SoCA v2.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
			Notify Subject of Credential Issuance	✓				OPB#0440	a)		sending notice to the address of record confirmed during identity proofing **and either;**			✓			
			Notify Subject of Credential Issuance	✓				OPB#0440	a)	i)	**issuing the credential(s) in a manner that confirms the address of record supplied by the applicant during identity proofing, or;**			✓			
			Notify Subject of Credential Issuance	✓				OPB#0440	a)	ii)	**issuing the credential(s) in a manner that confirms the ability of the applicant to receive telephone communications at a phone number supplied by the applicant during identity proofing, while recording the applicant's voice.**			✓			
			Notify Subject of Credential Issuance	✓				OPB#0440			**Notify the Subject of the credential's issuance and, if necessary, confirm the Subject's contact information by:**				✓		See LoA2 guidance.
			Notify Subject of Credential Issuance	✓				OPB#0440	a)		sending notice to the address of record confirmed during identity proofing;				✓		
			Notify Subject of Credential Issuance	✓				OPB#0440	b)		**unless the Subject presented with a private key, issuing the hardware token to the Subject in a manner that confirms the address of record supplied by the applicant during identity proofing;**				✓		
			Notify Subject of Credential Issuance	✓				OPB#0440	c)		**issuing the certificate to the Subject over a separate channel in a manner that confirms either the address of record or the email address supplied by the applicant during identity proofing.**				✓		
			Confirm Applicant's identity (in person)	✓				OPB#0450			**Prior to delivering the credential, require the Applicant to identify themselves in person in any new transaction (beyond the first transaction or encounter) by either:**		✓				
			Confirm Applicant's identity (in person)	✓				OPB#0450	a)		**using a temporary secret which was established during a prior transaction or encounter, or sent to the Applicant's phone number, email address, or physical address of record, or;**		✓				
			Confirm Applicant's identity (in person)	✓				OPB#0450	b)		**matching a biometric sample against a reference sample that was recorded during a prior encounter.**		✓				
			Confirm Applicant's identity (in person)	✓				OPB#0450			Prior to delivering the credential, require the Applicant to identify themselves in person in any new transaction (beyond the first transaction or encounter) by either:			✓			
			Confirm Applicant's identity (in person)	✓				OPB#0450	a)		using a temporary secret which was established during **the** prior transaction or encounter **(whilst ensuring that such temporary secrets are used only once)**, or sent to the Applicant's phone number, email address, or physical address of record, or;			✓			
			Confirm Applicant's identity (in person)	✓				OPB#0450	b)		matching a biometric sample against a reference sample that was recorded during a prior encounter.			✓			
			Confirm Applicant's identity (in person)	✓				OPB#0450			Prior to delivering the credential, require the Applicant to identify themselves in person in any new transaction (beyond the first transaction or encounter) through the use of a biometric that was recorded during **the first** encounter.				✓		
			Confirm Applicant's identity (remotely)	✓				OPB#0460			**Prior to activating the credential, require the Applicant to identify themselves in any new electronic transaction (beyond the first transaction or encounter) by presenting a temporary secret which was established during a prior transaction or encounter, or sent to the Applicant's phone number, email address, or physical address of record.**		✓	✓			Activation typically requires that the credential be delivered to the Applicant/Subject before activation occurs.
			Protected Issuance of Permanent Secrets (in person)	✓				OPB#0470			**Only issue permanent secrets if the CSP has loaded the secret itself onto the physical device, which was either:**			✓	✓		
			Protected Issuance of Permanent Secrets (in person)	✓				OPB#0470	a)		**issued in-person to the Applicant, or;**			✓	✓		

OP_SAC SAC / SoCA v2.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
			Protected Issuance of Permanent Secrets (in person)	✓				OPB#0470	b)		delivered in a manner that confirms the address of record.			✓	✓		
			Protected Issuance of Permanent Secrets (remotely)	✓				OPB#0480			Only issue permanent secrets within a protected session.			✓			
			Subject's acknowledgement	✓				OPB#0490			Receive acknowledgement of receipt of the credential before it is activated and its directory status record is published (and thereby the subscription becomes active or re-activated, depending upon the circumstances of issue).			✓			
			Subject's acknowledgement	✓				OPB#0480			Receive acknowledgement of receipt of the **hardware token** before it is activated and the **corresponding certificate and** its directory status record are published (and thereby the subscription becomes active or re-activated, depending upon the circumstances of issue).				✓		
			Activation window	✓				OPB#0490			Require activation of the credential within a time period specified in the Credential Policy			✓			
			Activation window	✓				OPB#0490			Require activation of the credential within a time period specified in the **Certificate Policy**.				✓		
Part C - Credential Renewal and Re-issuing																	
		Renewal/Re-issuance Procedures															
			Changeable PIN/Password	✓				OPC#0010			Permit Subjects to change their PINs/passwords.	✓					
			Changeable PIN/Password	✓				OPC#0010			Permit Subjects to change their passwords, but employ reasonable practices with respect to password resets and repeated password failures.		✓				
			Changeable PIN/Password	✓				OPC#0010			Permit Subjects to change the passwords **used to activate their credentials.**			✓	✓		
			Proof-of-possession on Renewal/Re-issuance	✓				OPC#0020			Subjects wishing to change their passwords must demonstrate that they are in possession of the unexpired current token prior to the CSP proceeding to renew or re-issue it. {source [5415] KI.10.2.2.1#29}	✓	✓	✓	✓		
			Renewal/Re-issuance limitations	✓				OPC#0030	**a)**		**not renew but may re-issue Passwords;**		✓				Renewal is considered as an extension of usability, whereas re-issuance requires a change.
			Renewal/Re-issuance limitations	✓				OPC#0030	**b)**		**neither renew nor re-issue expired tokens;**		✓				
			Renewal/Re-issuance limitations	✓				OPC#0030	**c)**		**neither set to default nor re-use any token secrets;**		✓				
			Renewal/Re-issuance limitations	✓				OPC#0030	**d)**		**conduct all renewal / re-issuance interactions with the Subject over a protected channel such as SSL/TLS.**		✓				
			Renewal/Re-issuance limitations	✓				OPC#0030	**a)**		**No stipulation;**			✓			See AL2 guidance.
			Renewal/Re-issuance limitations	✓				OPC#0030	b)		neither renew nor re-issue expired tokens;			✓			
			Renewal/Re-issuance limitations	✓				OPC#0030	**c)**		**No stipulation;**			✓			
			Renewal/Re-issuance limitations	✓				OPC#0030	d)		conduct all renewal / re-issuance interactions with the Subject over a protected channel such as SSL/TLS.			✓			
			Renewal/Re-issuance limitations	✓				OPC#0030	a)		No stipulation;				✓		
			Renewal/Re-issuance limitations	✓				OPC#0030	b)		neither renew nor re-issue expired tokens;				✓		
			Renewal/Re-issuance limitations	✓				OPC#0030	c)		No stipulation;				✓		
			Renewal/Re-issuance limitations	✓				OPC#0030	d)		**cryptographically authenticate all sensitive** renewal / re-issuance interactions with the Subject **using keys bound to the authentication process.**				✓		
			Authentication key life	✓				OPC#0040			**Expire after 24 hours all temporary or short-term keys derived during the authentication process.**				✓		

OP_SAC SAC / SoCA v2.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
			Record Retention	✓				OPC#0050			Retain, securely, the record of any renewal/re-issuance process for the duration of the Subscriber's account plus a further period sufficient to allow fulfillment of any period required legally, contractually or by any other form of binding agreement or obligation, or submit same record to a client CSP that has undertaken to retain the record for the requisite period or longer.		✓	✓	✓		
Part D - Credential Revocation																	
		Revocation Procedures															
			Revocation procedures	✓				OPD#0010	a)		State the conditions under which revocation of an issued credential may occur;		✓	✓	✓		
			Revocation procedures	✓				OPD#0010	b)		State the processes by which a revocation request may be submitted;		✓	✓	✓		
			Revocation procedures	✓				OPD#0010	c)		State the persons and organizations from which a revocation request will be accepted;		✓	✓	✓		
			Revocation procedures	✓				OPD#0010	d)		State the validation steps that will be applied to ensure the validity (identity) of the Revocant, and;		✓	✓	✓		
			Revocation procedures	✓				OPD#0010	e)		State the response time between a revocation request being accepted and the publication of revised certificate status.		✓	✓	✓		
			Secure status notification	✓				OPD#0020			Ensure that published credential status notification information can be relied upon in terms of the enterprise of its origin (i.e., its authenticity) and its correctness (i.e., its integrity).		✓	✓	✓		
			Revocation publication	✓				OPD#0030			Unless the credential will expire automatically within 72 hours: Ensure that published credential status notification is revised within 72 hours of the receipt of a valid revocation request, such that any subsequent attempts to use that credential in an authentication shall be unsuccessful.		✓				
			Revocation publication	✓				OPD#0030			Ensure that published credential status notification is revised within 24 hours of the receipt of a valid revocation request, such that any subsequent attempts to use that credential in an authentication shall be unsuccessful. The nature of the revocation mechanism shall be in accord with the technologies supported by the service.			✓			
			Revocation publication	✓				OPD#0030			Ensure that published credential status notification is revised within 18 hours of the receipt of a valid revocation request, such that any subsequent attempts to use that credential in an authentication shall be unsuccessful. The nature of the revocation mechanism shall be in accordance with the technologies supported by the service.				✓		
			Verify Revocation Identity	✓				OPD#0040			Establish that the identity for which a revocation request is received is one that was issued by the specified service.		✓	✓	✓		
			Notification of Revoked Credential	✓				OPD#0050			When a verification / authentication request results in notification of a revoked credential one of the following measures shall be taken:		✓				
			Notification of Revoked Credential					OPD#0050	a)		the confirmation message shall be time-stamped, or;		✓				
			Notification of Revoked Credential					OPD#0050	b)		the session keys shall expire with an expiration time no longer than that of the applicable revocation list, or;		✓				
			Notification of Revoked Credential					OPD#0050	c)		the time-stamped message, binding, and credential shall all be signed by the service.		✓				

OP_SAC SAC / SoCA v2.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
			Revocation Records	✓				OPD#0060			Retain a record of any revocation of a credential that is related to a specific identity previously verified, solely in connection to the stated credential. At a minimum, records of revocation must include:		✓	✓	✓		
			Revocation Records	✓				OPD#0060	a)		the Revocant's full name;		✓	✓	✓		
			Revocation Records	✓				OPD#0060	b)		the Revocant's authority to revoke (e.g., Subscriber, the Subject themselves, someone acting with the Subscriber's or the Subject's power of attorney, the credential issuer, law enforcement, or other legal due process);		✓	✓	✓		
			Revocation Records	✓				OPD#0060	c)		the Credential Issuer's identity (if not directly responsible for the identity proofing service);		✓	✓	✓		
			Revocation Records	✓				OPD#0060	d)		the identity associated with the credential (whether the Subject's name or a pseudonym);		✓	✓	✓		
			Revocation Records	✓				OPD#0060	e)		the reason for revocation.		✓	✓	✓		
			Record Retention	✓				OPD#0070			Retain securely, the record of the revocation process for a period which is the maximum of:		✓	✓			
			Record Retention	✓				OPD#0070	a)		the records retention policy required by OPA#0010; and		✓	✓			
			Record Retention	✓				OPD#0070	b)		applicable legislation, regulation, contract or standards.		✓	✓			
			Record Retention	✓				OPD#0070			Retain securely, the record of the revocation process for a period which is the maximum of:				✓		
			Record Retention	✓				OPD#0070	a)		the records retention policy required by OPA#0020; and				✓		
			Record Retention	✓				OPD#0070	b)		applicable legislation, regulation, contract or standards.				✓		
		Verify Revocant's Identity															
			Verify revocation identity	✓				OPD#0080			Establish that the credential for which a revocation request is received is one that was initially issued by the specified service, applying the same process and criteria as would apply to an original identity proofing.		✓				
			Verify revocation identity	✓				OPD#0080			Establish that the credential for which a revocation request is received is one that was initially issued by the specified service, applying the same process and criteria as would be applied to an original identity proofing, **ensuring that the Subject of the credential is uniquely identified.**			✓	✓		
			Revocation reason	✓				OPD#0090			Establish the reason for the revocation request as being sound and well founded, in combination with verification of the Revocant, according to OPD#0100 - '#0120 inc. as apply to the specific Level of Assurance		✓	✓	✓		
			Verify Subscriber as Revocant	✓				OPD#0100			When the Subscriber or Subject seeks revocation of the Subject's credential, the enterprise must:		✓				
			Verify Subscriber as Revocant	✓				OPD#0100	a)		if in person, require presentation of a primary Government Picture ID document that shall be electronically verified by a record check against the provided identity with the specified issuing authority's records;		✓				
			Verify Subscriber as Revocant	✓				OPD#0100	b)		if remote:		✓				
			Verify Subscriber as Revocant	✓				OPD#0100	b)	i)	electronically verify a signature against records (if available), confirmed with a call to a telephone number of record, or;		✓				
			Verify Subscriber as Revocant	✓				OPD#0100	b)	ii)	authenticate an electronic request as being from the same Subscriber or Subject, supported by a credential at Assurance Level 2 or higher.		✓				
			Verify Subscriber as Revocant	✓				OPD#0100			When the Subscriber or Subject seeks revocation of the Subject's credential, the enterprise must:			✓			

OP_SAC SAC / SoCA v2.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
			Verify Subscriber as Revocant	✓				OPD#0100	a)		if in person, require presentation of a primary Government Picture ID document that shall be electronically verified by a record check against the provided identity with the specified issuing authority's records;			✓			
			Verify Subscriber as Revocant	✓				OPD#0100	b)		if remote:			✓			
			Verify Subscriber as Revocant	✓				OPD#0100	b)	i)	electronically verify a signature against records (if available), confirmed with a call to a telephone number of record, or;			✓			
			Verify Subscriber as Revocant	✓				OPD#0100	b)	ii)	authenticate an electronic request as being from the same Subscriber or Subject, supported by a credential at Assurance Level **3** or higher.			✓			
			Verify Subscriber as Revocant	✓				OPD#0100			When the Subscriber or Subject seeks revocation of the Subject's credential, the enterprise must:				✓		
			Verify Subscriber as Revocant	✓				OPD#0100	a)		if in person, require presentation of a primary Government Picture ID document that shall be verified by a record check against the provided identity with the specified issuing authority's records;				✓		
			Verify Subscriber as Revocant	✓				OPD#0100	b)		if remote:				✓		
			Verify Subscriber as Revocant	✓				OPD#0100	b)	i)	electronically verify a signature against records (if available), confirmed with a call to a telephone number of record, or;				✓		
			Verify Subscriber as Revocant	✓				OPD#0100	b)	ii)	authenticate an electronic request as being from the same Subscriber or Subject, supported by a **different** credential at Assurance Level **4** or higher.				✓		
			CSP as Revocant	✓				OPD#0110			**Where a CSP seeks revocation of a Subject's credential, the enterprise must establish that the request is either:**		✓	✓	✓		
			CSP as Revocant	✓				OPD#0110	**a)**		**from the specified service itself, with authorization as determined by established procedures, or;**		✓	✓	✓		
			CSP as Revocant	✓				OPD#0110	**b)**		**from the client Credential Issuer, by authentication of a formalized request over the established secure communications network.**		✓	✓	✓		
			Verify Legal Representative as Revocant	✓				OPD#0120			**Where the request for revocation is made by a law enforcement officer or presentation of a legal document, the enterprise must:**		✓				
			Verify Legal Representative as Revocant	✓				OPD#0120	**a)**		**if in-person, verify the identity of the person presenting the request;**		✓				
			Verify Legal Representative as Revocant	✓				OPD#0120	**b)**		**if remote:**		✓				
			Verify Legal Representative as Revocant	✓				OPD#0120	**b)**	**i)**	**in paper/facsimile form, verify the origin of the legal document by a database check or by telephone with the issuing authority, or;**		✓				
			Verify Legal Representative as Revocant	✓				OPD#0120	**b)**	**ii)**	**as an electronic request, authenticate it as being from a recognized legal office, supported by a credential at Assurance Level 2 or higher.**		✓				
			Verify Legal Representative as Revocant	✓				OPD#0120			Where the request for revocation is made by a law enforcement officer or presentation of a legal document, the enterprise must:			✓			
			Verify Legal Representative as Revocant	✓				OPD#0120	a)		if in-person, verify the identity of the person presenting the request;			✓			
			Verify Legal Representative as Revocant	✓				OPD#0120	b)		if remote:			✓			
			Verify Legal Representative as Revocant	✓				OPD#0120	b)	i)	in paper/facsimile form, verify the origin of the legal document by a database check or by telephone with the issuing authority, or;			✓			
			Verify Legal Representative as Revocant	✓				OPD#0120	b)	ii)	as an electronic request, authenticate it as being from a recognized legal office, supported by a credential at Assurance Level **3** or higher.			✓			

OP_SAC SAC / SoCA v2.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
			Verify Legal Representative as Revocant	✓				OPD#0120			Where the request for revocation is made by a law enforcement officer or presentation of a legal document, the enterprise must:				✓		
			Verify Legal Representative as Revocant	✓				OPD#0120	a)		if in-person, verify the identity of the person presenting the request;				✓		
			Verify Legal Representative as Revocant	✓				OPD#0120	b)		if remote:				✓		
			Verify Legal Representative as Revocant	✓				OPD#0120	b)	i)	in paper/facsimile form, verify the origin of the legal document by a database check or by telephone with the issuing authority, or;				✓		
			Verify Legal Representative as Revocant	✓				OPD#0120	b)	ii)	as an electronic request, authenticate it as being from a recognized legal office, supported by a **different** credential at Assurance Level **4** or higher.				✓		
		Re-keying a credential															
			Verify Requestor as Subscriber	✓				OPD#0130			**Where the Subject seeks a re-key for the Subject's own credential:**				✓		
			Verify Requestor as Subscriber	✓				OPD#0130	**a)**		**if in-person, require presentation of a primary Government Picture ID document that shall be verified by a record check against the provided identity with the specified issuing authority's records;**				✓		
			Verify Requestor as Subscriber	✓				OPD#0130	**b)**		**if remote:**				✓		
			Verify Requestor as Subscriber	✓				OPD#0130	**b)**	**i)**	**verify a signature against records (if available), confirmed with a call to a telephone number of record, or;**				✓		
			Verify Requestor as Subscriber	✓				OPD#0130	**b)**	**ii)**	**authenticate an electronic request as being from the same Subject, supported by a different credential at Assurance Level 4.**				✓		
			Re-key requests other than Subject	✓				OPD#0140			**Re-key requests from any parties other than the Subject must not be accepted.**				✓		
		Secure Revocation Request															
			Submit Request	✓				OPD#0150			Submit a request for revocation to the Credential Issuer service (function), using a secured network communication, if necessary.	✓	✓	✓	✓		
Part E - Credential Status Management																	
		Status Maintenance															
			Maintain Status Record	✓				OPE#0010			Maintain a record of the status of all credentials issued.	✓	✓	✓	✓		
			Validation of Status Change Requests	✓				OPE#0020			**Authenticate all requestors seeking to have a change of status recorded and published and validate the requested change before considering processing the request. Such validation should include:**		✓	✓	✓		
			Validation of Status Change Requests	✓				OPE#0020	**a)**		**the requesting source as one from which the specified service expects to receive such requests;**		✓	✓	✓		
			Validation of Status Change Requests	✓				OPE#0020	**b)**		**if the request is not for a new status, the credential or identity as being one for which a status is already held.**		✓	✓	✓		
			Revision to Published Status	✓				OPE#0030			**Process authenticated requests for revised status information and have the revised information available for access within a period of 72 hours.**		✓	✓	✓		
			Status Information Availability	✓				OPE#0040			Provide, with 95% availability, a secure automated mechanism to allow relying parties to determine credential status and authenticate the Claimant's identity.	✓	✓				
			Status Information Availability	✓				OPE#0040			Provide, with **99**% availability, a secure automated mechanism to allow relying parties to determine credential status and authenticate the Claimant's identity.			✓	✓		
			Inactive Credentials	✓				OPE#0050			**Disable any credential that has not been successfully used for authentication during a period of 18 months.**		✓	✓	✓		
Part F - Credential Verification / Authentication																	

OP_SAC SAC / SoCA v2.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
		Status Maintenance															
			Validation and Assertion Security	✓				OPF#0010			Provide validation of credentials to a Relying Party using a protocol that:	✓					
			Validation and Assertion Security	✓				OPF#0010	a)		requires authentication of the specified service or of the validation source;	✓					
			Validation and Assertion Security	✓				OPF#0010	b)		ensures the integrity of the authentication assertion;	✓					
			Validation and Assertion Security	✓				OPF#0010	c)		protects assertions against manufacture, modification and substitution, and secondary authenticators from manufacture;	✓					
			Validation and Assertion Security	✓				OPF#0010			and which, specifically:	✓					
			Validation and Assertion Security	✓				OPF#0010	d)		creates assertions which are specific to a single transaction;	✓					
			Validation and Assertion Security	✓				OPF#0010	e)		where assertion references are used, generates a new reference whenever a new assertion is created;	✓					
			Validation and Assertion Security	✓				OPF#0010	f)		when an assertion is provided indirectly, either signs the assertion or sends it via a protected channel, using a strong binding mechanism between the secondary authenticator and the referenced assertion;	✓					
			Validation and Assertion Security	✓				OPF#0010	g)		requires the secondary authenticator to:	✓					
			Validation and Assertion Security	✓				OPF#0010	g)	i)	be signed when provided directly to Relying Party, or;	✓					
			Validation and Assertion Security	✓				OPF#0010	g)	ii)	have a minimum of 64 bits of entropy when provision is indirect (i.e. through the credential user).	✓					
			Validation and Assertion Security	✓				OPF#0010			Provide validation of credentials to a Relying Party using a protocol that:		✓	✓			
			Validation and Assertion Security	✓				OPF#0010	a)		requires authentication of the specified service**, itself,** or of the validation source;		✓	✓			
			Validation and Assertion Security	✓				OPF#0010	b)		ensures the integrity of the authentication assertion;		✓	✓			
			Validation and Assertion Security	✓				OPF#0010	c)		protects assertions against manufacture, modification, substitution and **disclosure**, and secondary authenticators from manufacture, **capture and replay;**		✓	✓			
			Validation and Assertion Security	✓				OPF#0010	**d)**		**uses approved cryptography techniques;**		✓	✓			
			Validation and Assertion Security	✓				OPF#0010			and which, specifically:		✓	✓			
			Validation and Assertion Security	✓				OPF#0010	e)		creates assertions which are specific to a single transaction;		✓	✓			
			Validation and Assertion Security	✓				OPF#0010	f)		where assertion references are used, generates a new reference whenever a new assertion is created;		✓	✓			
			Validation and Assertion Security	✓				OPF#0010	g)		when an assertion is provided indirectly, either signs the assertion or sends it via a protected channel, using a strong binding mechanism between the secondary authenticator and the referenced assertion;		✓	✓			
			Validation and Assertion Security	✓				OPF#0010	**h)**		**send assertions either via a channel mutually-authenticated with the Relying Party, or signed and encrypted for the Relying Party;**		✓	✓			
			Validation and Assertion Security	✓				OPF#0010	i)		requires the secondary authenticator to:		✓	✓			
			Validation and Assertion Security	✓				OPF#0010	i)	i)	be signed when provided directly to Relying Party, or;		✓	✓			
			Validation and Assertion Security	✓				OPF#0010	i)	ii)	have a minimum of 64 bits of entropy when provision is indirect (i.e. through the credential user).		✓	✓			
			Validation and Assertion Security	✓				OPF#0010	i)	**iii)**	**be transmitted to the Subject through a protected channel which is linked to the primary authentication process in such a way that session hijacking attacks are resisted;**		✓	✓			
			Validation and Assertion Security	✓				OPF#0010	i)	**iv)**	**not be subsequently transmitted over an unprotected channel or to an unauthenticated party while it remains valid.**		✓	✓			
			Validation and Assertion Security	✓				OPF#0010			Provide validation of credentials to a Relying Party using a protocol that:				✓		

OP_SAC SAC / SoCA v2.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
			Validation and Assertion Security	✓				OPF#0010	a)		requires authentication of the specified service, itself, or of the validation source;				✓		
			Validation and Assertion Security	✓				OPF#0010	b)		ensures the integrity of the authentication assertion;				✓		
			Validation and Assertion Security	✓				OPF#0010	c)		protects assertions against manufacture, modification, substitution and disclosure, and secondary authenticators from manufacture, capture and replay;				✓		
			Validation and Assertion Security	✓				OPF#0010	d)		uses approved **strong** cryptography techniques;				✓		
			Validation and Assertion Security	✓				OPF#0010			and which, specifically:				✓		
			Validation and Assertion Security	✓				OPF#0010	e)		creates assertions which are specific to a single transaction;				✓		
			Validation and Assertion Security	✓				OPF#0010	f)		where assertion references are used, generates a new reference whenever a new assertion is created;				✓		
			Validation and Assertion Security	✓				OPF#0010	g)		when an assertion is provided indirectly, either signs the assertion or sends it via a protected channel, using a strong binding mechanism between the secondary authenticator and the referenced assertion;				✓		
			Validation and Assertion Security	✓				OPF#0010	h)		send assertions either via a channel mutually-authenticated with the Relying Party, or signed and encrypted for the Relying Party;				✓		
			Validation and Assertion Security	✓				OPF#0010	i)		requires the secondary authenticator to:				✓		
			Validation and Assertion Security	✓				OPF#0010	i)	i)	be signed when provided directly to Relying Party, or;				✓		
			Validation and Assertion Security	✓				OPF#0010	i)	ii)	have a minimum of 64 bits of entropy when provision is indirect (i.e. through the credential user).				✓		
			Validation and Assertion Security	✓				OPF#0010	i)	iii)	iibe transmitted to the Subject through a protected channel which is linked to the primary authentication process in such a way that session hijacking attacks are resisted;				✓		
			Validation and Assertion Security	✓				OPF#0010	i)	iv)	not be subsequently transmitted over an unprotected channel or to an unauthenticated party while it remains valid.				✓		
			No False Authentication	✓				OPF#0020			**Employ techniques which ensure that system failures do not result in 'false positive authentication' errors.**		✓	✓	✓		
			Ensure token validity	✓				OPF#0030			**Ensure that tokens are either still valid or have been issued within the last 24 hours.**			✓	✓		The 24-hour period allows for the fact that if a freshly-issued credential is then revoked, notice of the revocation may take 24 hours to be publicised (per OP-D_CM_RVP#030).
			No Post Authentication	✓				OPF#0040			*Not* authenticate credentials that have been revoked.	✓					
			No Post Authentication	✓				OPF#0040			Not authenticate credentials that have been revoked **unless the time of the transaction for which verification is sought precedes the time of revocation of the credential.**		✓	✓	✓		The purpose in this criterion is that, if a verification is intended to refer to the status of a credential at a specific historical point in time, e.g. to determine whether the Claimant was entitled to act as a signatory in a specific capacity at the time of the transaction, this may be done. It is implicit in this thinking that both the request and the response indicate the historical nature of the query and response; otherwise the default time is 'now'. If no such service is offered then this criterion may simply be 'Inapplicable', for that reason.
			Proof of Possession	✓				OPF#0050			Use an authentication protocol that requires the claimant to prove possession and control of the authentication token.	✓	✓	✓	✓		
			Limit authentication attempts	✓				OPF#0070			Limit the number of failed authentication attempts to no more than 100 in any 30-day period.	✓					
			Limit authentication attempts	✓				OPF#0070			**Unless the token authenticator has at least 64 bits of entropy**, limit the number of failed authentication attempts to no more than 100 in any 30-day period.		✓	✓			
			Assertion Lifetime	✓				OPF#0080			Set assertions to expire such that:	✓	✓				
			Assertion Lifetime	✓				OPF#0080	a)		those used outside of the internet domain of the Verifier become invalid 5 minutes after their creation; or	✓	✓				

OP_SAC SAC / SoCA v2.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
			Assertion Lifetime	✓				OPF#0080	b)		those used within a single internet domain become invalid 12 hours after their creation (including assertions contained in or referenced by cookies).	✓	✓				
			Assertion Lifetime	✓				OPF#0080			**For non-cryptographic credentials**, generate assertions so as to indicate and effect their expiration 12 hours after their creation; **otherwise, notify the relying party of how often the revocation status sources are updated.**			✓			
			Assertion Lifetime	✓				OPF#0080			**Notify the relying party of how often the revocation status sources are updated.**				✓		
		Authenticator-generated challenges															
			Entropy level	✓				OPF#0090			**Create authentication secrets to be used during the authentication exchange (i.e. with out-of-band or cryptographic device tokens) with a degree of entropy appropriate to the token type in question.**		✓	✓	✓		
			Limit password validity	✓				OPF#0100			**Employ one-time passwords which expire within two minutes.**				✓		
		Multi-factor authentication															
			Permitted multi-factor tokens	✓				OPF#0110			**Require two tokens which, when used in combination within a single authentication exchange, are acknowledged as providing an equivalence of AL2, as determined by a recognized national technical authority.**		✓				
			Permitted multi-factor tokens	✓				OPF#0110			Require two tokens which, when used in combination within a single authentication exchange, are acknowledged as providing an equivalence of AL**3**, as determined by a recognized national technical authority.			✓			
			Permitted multi-factor tokens	✓				OPF#0110			Require two tokens which, when used in combination within a single authentication exchange, are acknowledged as providing an equivalence of AL**4**, as determined by a recognized national technical authority.				✓		
		Verifier's assertion schema															
			Approved cryptography	✓				OPF#0120			**Apply assertion protocols which use cryptographic techniques approved by a national authority or other generally-recognized authoritative body.**		✓	✓	✓		
			No browser/bearer assertions	✓				OPF#0130			**Not issue browser / bearer assertions.**				✓		
			Assertion assurance level	✓				OPF#0140			Create assertions which, either explicitly or implicitly (using a mutually-agreed mechanism), indicate the assurance level at which the initial authentication of the Subject was made.	✓	✓	✓	✓		
			Notify pseudonyms	✓				OPF#0150			**Create assertions which indicate whether the Subscriber name in the credential subject to verification is a pseudonym.**		✓				
			No pseudonyms	✓				OPF#0160			Create assertions which indicate **only verified Subscriber names** in the credential subject to verification.			✓	✓		
			Specify recipient	✓				OPF#0170			Create assertions which identify the intended recipient of the verification such that the recipient may validate that it is intended for them.		✓	✓	✓		
			No assertion manufacture/modification	✓				OPF#0180			Ensure that it is impractical to manufacture an assertion or assertion reference by using at least one of the following techniques:	✓	✓				
			No assertion manufacture/modification	✓				OPF#0180	a)		Signing the assertion;	✓	✓				
			No assertion manufacture/modification	✓				OPF#0180	b)		Encrypting the assertion using a secret key shared with the RP;	✓	✓				
			No assertion manufacture/modification	✓				OPF#0180	c)		Creating an assertion reference which has a minimum of 64 bits of entropy;	✓	✓				
			No assertion manufacture/modification	✓				OPF#0180	d)		Sending the assertion over a protected channel during a mutually-authenticated session.	✓	✓				

OP_SAC SAC / SoCA v2.0				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				LoA				CRITERION APPLICABILITY (SoCA)	Guidance
Not Used			Criterion title	CSP	RP	FA	US Fed Agcy	new tag	index		KI_criterion	1	2	3	4	read this comment	
			No assertion manufacture/modification	✓				OPF#0180			Ensure that it is impractical to manufacture an assertion or assertion reference by **Signing the assertion and** using at least one of the following techniques:			✓			
			No assertion manufacture/modification	✓				OPF#0180	a)		Signing the assertion;			✓			
			No assertion manufacture/modification	✓				OPF#0180	b)		Encrypting the assertion using a secret key shared with the RP;			✓			
			No assertion manufacture/modification	✓				OPF#0180	c)		Creating an assertion reference which has a minimum of 64 bits of entropy;			✓			
			No assertion manufacture/modification	✓				OPF#0180	d)		Sending the assertion over a protected channel during a mutually-authenticated session.			✓			
			No assertion manufacture/modification	✓				OPF#0180			Ensure that it is impractical to manufacture an assertion or assertion reference by Signing the assertion and using at least one of the following techniques:				✓		
			No assertion manufacture/modification	✓				OPF#0180	a)		**No stipulation;**				✓		
			No assertion manufacture/modification	✓				OPF#0180	b)		Encrypting the assertion using a secret key shared with the RP;				✓		
			No assertion manufacture/modification	✓				OPF#0180	c)		Creating an assertion reference which has a minimum of 64 bits of entropy;				✓		
			No assertion manufacture/modification	✓				OPF#0180	d)		Sending the assertion over a protected channel during a mutually-authenticated session.				✓		
			Assertion protections	✓				OPF#0190			**Provide protection of assertion-related data such that:**		✓	✓	✓		
			Assertion protections	✓				OPF#0190	**a)**		**both assertions and assertion references are protected against capture and re-use;**		✓	✓	✓		
			Assertion protections	✓				OPF#0190	**b)**		**assertions are also protected against redirection;**		✓	✓	✓		
			Assertion protections	✓				OPF#0190	**c)**		**assertions, assertion references and session cookies used for authentication purposes, including any which are re-directed, are protected against session hijacking, for at least the duration of their validity (see OPF#0120).**		✓	✓	✓		
			Single-use assertions	✓				OPF#0200			Limit to a single transaction the use of assertions which do not support proof of ownership.	✓	✓	✓	✓		
			Single-use assertion references	✓				OPF#0210			Limit to a single transaction the use of assertion references.	✓	✓	✓	✓		
			Bind reference to assertion	✓				OPF#0220			Provide a strong binding between the assertion reference and the corresponding assertion, based on integrity-protected (or signed) communications over which the Verifier has been authenticated.	✓	✓	✓	✓		
			SSO provisions	✓				OPF#0230			**If SSO is supported, provide a re-authentication of the Subject so long as:**			✓			The conditional nature of this criterion is dictated by the phrasing used in NIST SP 800-63 which states 'may'.
			SSO provisions	✓				OPF#0230	**a)**		**the Subject has been successfully authenticated within the last 12 hours;**			✓			
			SSO provisions	✓				OPF#0230	**b)**		**the Subject continues to be able to demonstrate that they were the party that was previously authenticated;**			✓			
			SSO provisions	✓				OPF#0230	**c)**		**it can be ensured that the Subscriber has not been inactive for more than 30 minutes.**			✓			
End of CO_SAC criteria																	

Tag cross-reference:

==>

Criterion title	*old tag*	*new tag*
Entropy level	*ALx_CM_AGC#010*	*OPF#0090*
Limit password validity	*ALx_CM_AGC#020*	*OPF#0100*
Validation and Assertion Security	*ALx_CM_ASS#010*	*OPF#0010*
No False Authentication	*ALx_CM_ASS#015*	*OPF#0020*
Ensure token validity	*ALx_CM_ASS#018*	*OPF#0030*
No Post Authentication	*ALx_CM_ASS#020*	*OPF#0040*
Proof of Possession	*ALx_CM_ASS#030*	*OPF#0050*
Limit authentication attempts	*ALx_CM_ASS#035*	*OPF#0070*
Assertion Lifetime	*ALx_CM_ASS#040*	*OPF#0080*
Credential Policy and Practice Statement	*ALx_CM_CPP#010*	*OPA#0010*
Credential Policy reference	*ALx_CM_CPP#015*	*OPA#0015*
Certificate Policy / Certification Practice Statement	*ALx_CM_CPP#020*	*OPA#0020*
Management Authority	*ALx_CM_CPP#030*	*OPA#0030*
Discretionary Access Control	*ALx_CM_CPP#040*	*OPA#0040*
Notify Subject of Credential Issuance	*ALx_CM_CRD#010*	*OPB#0440*
Confirm Applicant's identity (in person)	*ALx_CM_CRD#015*	*OPB#0450*
Confirm Applicant's identity (remotely)	*ALx_CM_CRD#016*	*OPB#0460*
Protected Issuance of Permanent Secrets (in person)	*ALx_CM_CRD#017*	*OPB#0470*
Subject's acknowledgement	*ALx_CM_CRD#020*	*OPB#0480*
Activation window	*ALx_CM_CRD#030*	*OPB#0490*
Authenticated Request	*ALx_CM_CRN#010*	*OPB#0290*
Unique identity	*ALx_CM_CRN#020*	*OPB#0300*
Credential uniqueness	*ALx_CM_CRN#030*	*OPB#0310*
Convey credential	*ALx_CM_CRN#035*	*OPB#0320*
Token strength	*ALx_CM_CRN#040*	*OPB#0330*
One-time password lifetime	*ALx_CM_CRN#055*	*OPB#0340*
Software cryptographic token strength	*ALx_CM_CRN#060*	*OPB#0350*
Hardware token strength	*ALx_CM_CRN#070*	*OPB#0360*
One-time password hardware token strength	*ALx_CM_CRN#070*	*OPB#0361*
Multi-factor hardware cryptographic token strength	*ALx_CM_CRN#075*	*OPB#0370*

Binding	*ALx_CM_CRN#080*	*OPB#0380*
Binding of key	*ALx_CM_CRN#080*	*OPB#0381*
Hardware Inventory Control	*ALx_CM_CRN#085*	*OPB#0390*
Nature of Subject	*ALx_CM_CRN#090*	*OPB#0400*
Pseudonym's Real Identity	*ALx_CM_CRN#095*	*OPB#0410*
Maintain Status Record	*ALx_CM_CSM#010*	*OPE#0010*
Validation of Status Change Requests	*ALx_CM_CSM#020*	*OPE#0020*
Revision to Published Status	*ALx_CM_CSM#030*	*OPE#0030*
Status Information Availability	*ALx_CM_CSM#040*	*OPE#0040*
Inactive Credentials	*ALx_CM_CSM#050*	*OPE#0050*
Protocol threat risk assessment and controls	*ALx_CM_CTR#020*	*OPA#0050*
Authentication protocols	*ALx_CM_CTR#025*	*OPA#0060*
One-time passwords	*ALx_CM_CTR#028*	*OPA#0070*
System threat risk assessment and controls	*ALx_CM_CTR#030*	*OPA#0080*
Specified Service's Key Management	*ALx_CM_CTR#040*	*OPA#0090*
Revision to Subject Information	*ALx_CM_IDP#010*	*OPB#0270*
Authenticate Subject Information Change	*ALx_CM_IDP#020*	*OPB#0280*
Permitted multi-factor tokens	*ALx_CM_MFA#010*	*OPF#0110*
Physical access control	*ALx_CM_OPN#060*	*OPA#0130*
Verify Requestor as Subscriber	*ALx_CM_RKY#010*	*OPD#0130*
Re-key requests other than Subject	*ALx_CM_RKY#020*	*OPD#0140*
Changeable PIN/Password	*ALx_CM_RNR#010*	*OPC#0010*
Proof-of-possession on Renewal/Re-issuance	*ALx_CM_RNR#020*	*OPC#0020*
Renewal/Re-issuance limitations	*ALx_CM_RNR#030*	*OPC#0030*
Authentication key life	*ALx_CM_RNR#040*	*OPC#0040*
Record Retention	*ALx_CM_RNR#050*	*OPC#0050*
Revocation procedures	*ALx_CM_RVP#010*	*OPD#0010*
Secure status notification	*ALx_CM_RVP#020*	*OPD#0020*
Revocation publication	*ALx_CM_RVP#030*	*OPD#0030*
Verify Revocation Identity	*ALx_CM_RVP#040*	*OPD#0040*
Notification of Revoked Credential	*ALx_CM_RVP#045*	*OPD#0050*
Revocation Records	*ALx_CM_RVP#050*	*OPD#0060*
Record Retention	*ALx_CM_RVP#060*	*OPD#0070*

Verify revocation identity	*ALx_CM_RVR#010*	*OPD#0080*
Revocation reason	*ALx_CM_RVR#020*	*OPD#0090*
Verify Subscriber as Revocant	*ALx_CM_RVR#030*	*OPD#0100*
CSP as Revocant	*ALx_CM_RVR#040*	*OPD#0110*
Verify Legal Representative as Revocant	*ALx_CM_RVR#050*	*OPD#0120*
Secure remote communications	*ALx_CM_SCO#010*	*OPA#0140*
Verification / Authentication confirmation messages	*ALx_CM_SCO#015*	*OPA#0150*
Limited access to shared secrets	*ALx_CM_SCO#020*	*OPA#0160*
Logical protection of shared secrets	*ALx_CM_SCO#030*	*OPA#0170*
Security event logs	*ALx_CM_SER#010*	*OPA#0120*
Key generation by Specified Service	*ALx_CM_SKP#010*	*OPB#0420*
Key generation by Subject	*ALx_CM_SKP#020*	*OPB#0430*
Submit Request	*ALx_CM_SRR#010*	*OPD#0150*
Stored Secret Encryption (shared secrets)	*ALx_CM_STS#020*	*OPA#0100*
Stored Secret Encryption	*ALx_CM_STS#020*	*OPA#0110*
Approved cryptography	*ALx_CM_VAS#010*	*OPF#0120*
No browser/bearer assertions	*ALx_CM_VAS#020*	*OPF#0130*
Assertion assurance level	*ALx_CM_VAS#030*	*OPF#0140*
Notify pseudonyms	*ALx_CM_VAS#040*	*OPF#0150*
No pseudonyms	*ALx_CM_VAS#045*	*OPF#0160*
Specify recipient	*ALx_CM_VAS#050*	*OPF#0170*
No assertion manufacture/modification	*ALx_CM_VAS#060*	*OPF#0180*
Assertion protections	*ALx_CM_VAS#070*	*OPF#0190*
Single-use assertions	*ALx_CM_VAS#080*	*OPF#0200*
Single-use assertion references	*ALx_CM_VAS#090*	*OPF#0210*
Bind reference to assertion	*ALx_CM_VAS#100*	*OPF#0220*
SSO provisions	*ALx_CM_VAS#110*	*OPF#0230*
Meet preceding criteria	*ALx_ID_AFV#000*	*OPB#0160*
Required evidence (affiliated)	*ALx_ID_AFV#010*	*OPB#0170*
Evidence checks (affiliated)	*ALx_ID_AFV#020*	*OPB#0180*
Required evidence (current)	*ALx_ID_CRV#010*	*OPB#0140*
Evidence Checks (current)	*ALx_ID_CRV#020*	*OPB#0150*

Authenticate Original Credential	*ALx_ID_IDC#010*	*OPB#0190*
Record Original Credential	*ALx_ID_IDC#020*	*OPB#0200*
Issue Derived Credential	*ALx_ID_IDC#030*	*OPB#0210*
Identity Proofing classes	*ALx_ID_IDV#000*	*OPB#0050*
Identity Verification Measures	*ALx_ID_IDV#010*	*OPB#0060*
Required evidence (in-person)	*ALx_ID_IPV#010*	*OPB#0070*
Evidence checks (in-person)	*ALx_ID_IPV#020*	*OPB#0080*
Evidence checks – primary ID	*ALx_ID_IPV#030*	*OPB#0090*
Evidence checks – secondary ID	*ALx_ID_IPV#040*	*OPB#0100*
Applicant knowledge checks	*ALx_ID_IPV#050*	*OPB#0110*
Unique service identity	*ALx_ID_POL#010*	*OPB#0010*
Unique Subject identity	*ALx_ID_POL#020*	*OPB#0020*
Published Proofing Policy	*ALx_ID_POL#030*	*OPB#0030*
Adherence to Proofing Policy	*ALx_ID_POL#040*	*OPB#0040*
Required evidence (remote)	*ALx_ID_RPV#010*	*OPB#0120*
Evidence checks (remote)	*ALx_ID_RPV#020*	*OPB#0130*
Secondary checks	*ALx_ID_SCV#010*	*OPB#0220*
Verification Records for Personal Applicants	*ALx_ID_VRC#010*	*OPB#0230*
Verification Records for Affiliated Applicants	*ALx_ID_VRC#020*	*OPB#0240*
Provide Subject identity records	*ALx_ID_VRC#025*	*OPB#0250*
Record Retention	*ALx_ID_VRC#030*	*OPB#0260*
	End of CO_SAC criteria	

==>

Criterion title	*new tag*	*old tag*
Credential Policy and Practice Statement	*OPA#0010*	*ALx_CM_CPP#010*
Credential Policy reference	*OPA#0015*	*ALx_CM_CPP#015*
Certificate Policy / Certification Practice Statement	*OPA#0020*	*ALx_CM_CPP#020*
Management Authority	*OPA#0030*	*ALx_CM_CPP#030*
Discretionary Access Control	*OPA#0040*	*ALx_CM_CPP#040*
Protocol threat risk assessment and controls	*OPA#0050*	*ALx_CM_CTR#020*
Authentication protocols	*OPA#0060*	*ALx_CM_CTR#025*
One-time passwords	*OPA#0070*	*ALx_CM_CTR#028*
System threat risk assessment and controls	*OPA#0080*	*ALx_CM_CTR#030*
Specified Service's Key Management	*OPA#0090*	*ALx_CM_CTR#040*
Stored Secret Encryption (shared secrets)	*OPA#0100*	*ALx_CM_STS#020*
Stored Secret Encryption	*OPA#0110*	*ALx_CM_STS#020*
Security event logs	*OPA#0120*	*ALx_CM_SER#010*
Physical access control	*OPA#0130*	*ALx_CM_OPN#060*
Secure remote communications	*OPA#0140*	*ALx_CM_SCO#010*
Verification / Authentication confirmation messages	*OPA#0150*	*ALx_CM_SCO#015*
Limited access to shared secrets	*OPA#0160*	*ALx_CM_SCO#020*
Logical protection of shared secrets	*OPA#0170*	*ALx_CM_SCO#030*
Unique service identity	*OPB#0010*	*ALx_ID_POL#010*
Unique Subject identity	*OPB#0020*	*ALx_ID_POL#020*
Published Proofing Policy	*OPB#0030*	*ALx_ID_POL#030*
Adherence to Proofing Policy	*OPB#0040*	*ALx_ID_POL#040*
Identity Proofing classes	*OPB#0050*	*ALx_ID_IDV#000*
Identity Verification Measures	*OPB#0060*	*ALx_ID_IDV#010*
Required evidence (in-person)	*OPB#0070*	*ALx_ID_IPV#010*
Evidence checks (in-person)	*OPB#0080*	*ALx_ID_IPV#020*
Evidence checks – primary ID	*OPB#0090*	*ALx_ID_IPV#030*
Evidence checks – secondary ID	*OPB#0100*	*ALx_ID_IPV#040*
Applicant knowledge checks	*OPB#0110*	*ALx_ID_IPV#050*
Required evidence (remote)	*OPB#0120*	*ALx_ID_RPV#010*

Evidence checks (remote)	*OPB#0130*	*ALx_ID_RPV#020*
Required evidence (current)	*OPB#0140*	*ALx_ID_CRV#010*
Evidence Checks (current)	*OPB#0150*	*ALx_ID_CRV#020*
Meet preceding criteria	*OPB#0160*	*ALx_ID_AFV#000*
Required evidence (affiliated)	*OPB#0170*	*ALx_ID_AFV#010*
Evidence checks (affiliated)	*OPB#0180*	*ALx_ID_AFV#020*
Authenticate Original Credential	*OPB#0190*	*ALx_ID_IDC#010*
Record Original Credential	*OPB#0200*	*ALx_ID_IDC#020*
Issue Derived Credential	*OPB#0210*	*ALx_ID_IDC#030*
Secondary checks	*OPB#0220*	*ALx_ID_SCV#010*
Verification Records for Personal Applicants	*OPB#0230*	*ALx_ID_VRC#010*
Verification Records for Affiliated Applicants	*OPB#0240*	*ALx_ID_VRC#020*
Provide Subject identity records	*OPB#0250*	*ALx_ID_VRC#025*
Record Retention	*OPB#0260*	*ALx_ID_VRC#030*
Revision to Subject Information	*OPB#0270*	*ALx_CM_IDP#010*
Authenticate Subject Information Change	*OPB#0280*	*ALx_CM_IDP#020*
Authenticated Request	*OPB#0290*	*ALx_CM_CRN#010*
Unique identity	*OPB#0300*	*ALx_CM_CRN#020*
Credential uniqueness	*OPB#0310*	*ALx_CM_CRN#030*
Convey credential	*OPB#0320*	*ALx_CM_CRN#035*
Token strength	*OPB#0330*	*ALx_CM_CRN#040*
One-time password lifetime	*OPB#0340*	*ALx_CM_CRN#055*
Software cryptographic token strength	*OPB#0350*	*ALx_CM_CRN#060*
Hardware token strength	*OPB#0360*	*ALx_CM_CRN#070*
One-time password hardware token strength	*OPB#0361*	*ALx_CM_CRN#070*
Multi-factor hardware cryptographic token strength	*OPB#0370*	*ALx_CM_CRN#075*
Binding	*OPB#0380*	*ALx_CM_CRN#080*
Binding of key	*OPB#0381*	*ALx_CM_CRN#085*
Hardware Inventory Control	*OPB#0390*	*ALx_CM_CRN#085*
Nature of Subject	*OPB#0400*	*ALx_CM_CRN#090*
Pseudonym's Real Identity	*OPB#0410*	*ALx_CM_CRN#095*
Key generation by Specified Service	*OPB#0420*	*ALx_CM_SKP#010*
Key generation by Subject	*OPB#0430*	*ALx_CM_SKP#020*

Notify Subject of Credential Issuance	*OPB#0440*	*ALx_CM_CRD#010*
Confirm Applicant's identity (in person)	*OPB#0450*	*ALx_CM_CRD#015*
Confirm Applicant's identity (remotely)	*OPB#0460*	*ALx_CM_CRD#016*
Protected Issuance of Permanent Secrets (in person)	*OPB#0470*	*ALx_CM_CRD#017*
Subject's acknowledgement	*OPB#0480*	*ALx_CM_CRD#020*
Activation window	*OPB#0490*	*ALx_CM_CRD#030*
Changeable PIN/Password	*OPC#0010*	*ALx_CM_RNR#010*
Proof-of-possession on Renewal/Re-issuance	*OPC#0020*	*ALx_CM_RNR#020*
Renewal/Re-issuance limitations	*OPC#0030*	*ALx_CM_RNR#030*
Authentication key life	*OPC#0040*	*ALx_CM_RNR#040*
Record Retention	*OPC#0050*	*ALx_CM_RNR#050*
Revocation procedures	*OPD#0010*	*ALx_CM_RVP#010*
Secure status notification	*OPD#0020*	*ALx_CM_RVP#020*
Revocation publication	*OPD#0030*	*ALx_CM_RVP#030*
Verify Revocation Identity	*OPD#0040*	*ALx_CM_RVP#040*
Notification of Revoked Credential	*OPD#0050*	*ALx_CM_RVP#045*
Revocation Records	*OPD#0060*	*ALx_CM_RVP#050*
Record Retention	*OPD#0070*	*ALx_CM_RVP#060*
Verify revocation identity	*OPD#0080*	*ALx_CM_RVR#010*
Revocation reason	*OPD#0090*	*ALx_CM_RVR#020*
Verify Subscriber as Revocant	*OPD#0100*	*ALx_CM_RVR#030*
CSP as Revocant	*OPD#0110*	*ALx_CM_RVR#040*
Verify Legal Representative as Revocant	*OPD#0120*	*ALx_CM_RVR#050*
Verify Requestor as Subscriber	*OPD#0130*	*ALx_CM_RKY#010*
Re-key requests other than Subject	*OPD#0140*	*ALx_CM_RKY#020*
Submit Request	*OPD#0150*	*ALx_CM_SRR#010*
Maintain Status Record	*OPE#0010*	*ALx_CM_CSM#010*
Validation of Status Change Requests	*OPE#0020*	*ALx_CM_CSM#020*
Revision to Published Status	*OPE#0030*	*ALx_CM_CSM#030*
Status Information Availability	*OPE#0040*	*ALx_CM_CSM#040*
Inactive Credentials	*OPE#0050*	*ALx_CM_CSM#050*
Validation and Assertion Security	*OPF#0010*	*ALx_CM_ASS#010*

No False Authentication	*OPF#0020*	*ALx_CM_ASS#015*
Ensure token validity	*OPF#0030*	*ALx_CM_ASS#018*
No Post Authentication	*OPF#0040*	*ALx_CM_ASS#020*
Proof of Possession	*OPF#0050*	*ALx_CM_ASS#030*
Limit authentication attempts	*OPF#0070*	*ALx_CM_ASS#035*
Assertion Lifetime	*OPF#0080*	*ALx_CM_ASS#040*
Entropy level	*OPF#0090*	*ALx_CM_AGC#010*
Limit password validity	*OPF#0100*	*ALx_CM_AGC#020*
Permitted multi-factor tokens	*OPF#0110*	*ALx_CM_MFA#010*
Approved cryptography	*OPF#0120*	*ALx_CM_VAS#010*
No browser/bearer assertions	*OPF#0130*	*ALx_CM_VAS#020*
Assertion assurance level	*OPF#0140*	*ALx_CM_VAS#030*
Notify pseudonyms	*OPF#0150*	*ALx_CM_VAS#040*
No pseudonyms	*OPF#0160*	*ALx_CM_VAS#045*
Specify recipient	*OPF#0170*	*ALx_CM_VAS#050*
No assertion manufacture/modification	*OPF#0180*	*ALx_CM_VAS#060*
Assertion protections	*OPF#0190*	*ALx_CM_VAS#070*
Single-use assertions	*OPF#0200*	*ALx_CM_VAS#080*
Single-use assertion references	*OPF#0210*	*ALx_CM_VAS#090*
Bind reference to assertion	*OPF#0220*	*ALx_CM_VAS#100*
SSO provisions	*OPF#0230*	*ALx_CM_VAS#110*
		End of CO_SAC criteria