Title: Identity Assurance Framework: NIST SP 800-63C Service Assessment Criteria (SAC) & Statement of Criteria Applicability (SoCA)
Document id: KIAF-1450
Version: 1.0
Document type: Recommendation
Publication Date: 2020-10-15
Effective Date: 2021-02-01
Status: Final
Approval Authority: IAWG
Sponsor: ID.me

IAWG Sub-group Participants
Ken DAGG (Individual contributor)
Mark HAPNER (Resilient Networks)
James JUNG (Slandala)
Richard WILSHER (Zygma Inc.)
Nathan FAUT (KPMG)
Andrew HUGHES (IDEMIA)
Martin SMITH (Individual contributor)

IPR: Patent and Copyright Option: Reciprocal Royalty Free with Opt-Out to Reasonable and Non-

Abstract: This document sets forth KI's Service Assessment Criteria for assessments against the requirements of NIST's SP 800-63C as published 2017-12-01 (with errata) at FAL2 & FAL3, to be generally referred-to as the '63C_SAC'. It is anticipated that these criteria will be reviewed 12

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

Revision history: See Revision History

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

Version	*Date*	*Status*
v1.0	10/15/20	Final - first release

NIST SP 800-63C - NORMATIVE clause references and requirement(s)				Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				FAL		CRITERION APPLICABILITY (SoCA)	Guidance	ASSESSOR'S FINDING (SoC)
§(H)	(L1)	Clause title	Requirement	CSP	RP	FA	US Fed Agcy	63C tag	index		KI_criterion	2	3	read this comment	Note - guidance will be added as KI-IAWG members develop it in response to usage & experience	
4.0		Federation Assurance Levels	All assertions SHALL be used with a federation protocol as described in Section 4.	✓	✓	✓		63C#0010			Assertions which federation participants create or consume SHALL meet the requirements expressed in criteria 63C#0020 to 63C#0240 inclusive.	✓	✓		Given the lack of granularity of this criterion it is expected that it would have a finding determined only after the assessment was largely concluded and might be qualified, depending whether more specific criteria have themselves received qualification (e.g. Minor Nonconformities).	
4.0		Federation Assurance Levels	All assertions SHALL comply with the detailed requirements in Section 6.	✓	✓			63C#0020			Assertions which federation participants create or consume SHALL meet the requirements expressed in criteria 63C#0430 to 63C#0640 inclusive.	✓	✓		Given the lack of granularity of this criterion it is expected that it would have a finding determined only after the assessment was largely concluded and might be qualified, depending whether more specific criteria have themselves received qualification (e.g. Minor Nonconformities).	
4.0		Federation Assurance Levels	All assertions SHALL be presented using one of the methods described in Section 7.	✓	✓			63C#0030			The assertions which federation participants create or consume SHALL meet the requirements expressed in criteria 63C#0650 to 63C#0780 inclusive.	✓	✓		Given the lack of granularity of this criterion it is expected that it would have a finding determined only after then assessment was largely concluded and might be qualified, depending whether more specific criteria have themselves received qualification (e.g. Minor Nonconformities).	
			Kantara-specific criterion to broadly enforce this requirement rather than state it repeatedly as is found in the source requirements.	✓	✓	✓	✓	63C#0040			Federation participants SHALL at all times use cryptographic functions which are approved by a recognized authority.	✓	✓			
4.0		Federation Assurance Levels	[Assertions] presented through a proxy SHALL be represented by the lowest level used during the proxied transaction. *NB - this substitution agreed with NIST, 2020-02-12. Erratum to SP 800-63 stated to be in preparation*	✓	✓	✓		63C#0050			When acting as a Proxy, federation participants SHALL only present assertions at the lowest assurance level of any transactional elements	✓	✓			
4.0		Federation Assurance Levels	If the RP is using a front-channel presentation mechanism, as defined in Section 7.2 (e.g., the OpenID Connect Implicit Client profile or the SAML Web SSO profile), it SHALL require FAL2 or greater in order to protect the information in the assertion from disclosure to the browser or other parties in the transaction other than the intended RP.		✓			63C#0060			The RP SHALL, when using a front-channel presentation mechanism, require FAL2 or FAL3 transactional mechanisms in a manner which conforms to 63C#0690 - '#0710 inclusive.	✓	✓			
4.0		Federation Assurance Levels	Additionally, the IdP SHALL employ appropriately-tailored security controls (to include control enhancements) from the moderate or high baseline of security controls defined in SP 800-53 or equivalent federal (e.g., FEDRAMP) or industry standard.	✓				63C#0070			The CSP's risk assessments SHALL include actions to select controls from NIST SP 800-53's moderate or high baseline of security controls or other controls defined by any equivalent Federal or industry standard.	✓	✓			
4.1		Key Management	At any FAL, the IdP SHALL ensure that an RP is unable to impersonate the IdP at another RP by protecting the assertion with a signature and key using approved cryptography.	✓				63C#0080			The CSP SHALL protect the assertions it generates with a signature and key using approved cryptography.	✓	✓			

4.1		Key Management	[Government-operated] IdPs asserting authentication at AAL2 and all IdPs asserting authentication at AAL3 SHALL protect keys used for signing or encrypting those assertions with mechanisms validated at FIPS 140 Level 1 or higher.	✓				*63C#0090*			The CSP SHALL protect keys used for signing or encrypting AAL2 (or higher) assertions with crypto modules validated at FIPS 140 Level 1 or higher.	✓	✓		This criterion is broadly applicable (i.e. not exclusively to US Federal Agencys) since NIST personnel have commented that 'govt-operated' is essentially noise, since the SP is intended for application by governemnt agencies and systems they operate or procure.	
4.2		Runtime Decisions	The fact that parties have federated SHALL NOT be interpreted as permission to pass information.	✓	✓			*63C#0100*			Federation participants SHALL restrict their transfer of SSI in accordance with all applicable laws, regulations, contracts and policies as they apply to the relevant party	✓	✓		this criterion establishes the fundamental restrictions on sharing SII*, notwithstanding any consent which may be given by the Subject (or their authorized representative) in specific instances. * SSI, which stands for Sensitive Subject Information, is defined in KIAF-1050 Glossary & Overview.	
4.2		Runtime Decisions	All RPs in an IdP's whitelist SHALL abide by the provisions and requirements in the SP 800-63 [rev.3] suite.	✓				*63C#0110*			CSPs SHALL only include in their allowlists those RPs which provide evidence of their conformity to the requirements in the SP 800-63 [rev.3] suite.	✓	✓		Inclusion of an RP within a white list allows the CSP to make decisions on info release when generating an assertion for the RP in question. In contrast, a gray list requires run-time consent (therefore consent clauses herein are moot if the RP is white-listed)	
			Kantara-specific criterion to bring into effect the means to be able to demonstrate conformity with the preceding NIST requirement.	✓	✓			*63C#0120*			Federation participants SHALL, in accordance with the requirements of the applicable Federation Agreement, make available to all other federation participants:	✓	✓			
			Kantara-specific criterion to bring into effect the means to be able to demonstrate conformity with the preceding NIST requirement.	✓	✓			*63C#0120*	*a)*		a statement as to whether or not their service conforms fully to the requirements in the SP 800-63 [rev.3] suite which are in scope of their service; and	✓	✓		This requirement may be satisfied by a Kantara requirement that the Approval applicant submit to Kantara a SoCA where the FednAgrmnt requires formal Kantara Approval for its members. Otherwise it stands.	
			Kantara-specific criterion to bring into effect the means to be able to demonstrate conformity with the preceding NIST requirement.	✓	✓			*63C#0120*	*b)*		if the statement required in a) above is affirmative, a reference to a source of evidence of that conformity.	✓	✓		Noting that if the Fedn Agrmnt calls only for a self attestation, so be it, and likewise if it requires Kantara (or any other definable) approval.	
4.2		Runtime Decisions	IdPs SHALL make whitelists available to subscribers as described in [NIST SP 800-63C] Section 9.2.	✓				*63C#0130*			The CSP SHALL maintain a list of those RPs and the associated types of SSI which will be automatically presented to the RP if the Subject engages in a transaction with an allow-listed RP	✓	✓			
4.2		Runtime Decisions	Every RP not on a whitelist or a blacklist SHALL be placed by default in a gray area where runtime authorization decisions will be made by an authorized party, usually the subscriber.	✓				*63C#0140*			If an RP with which the CSP is conducting a transaction is neither in an allowlist nor in a denylist, the CSP SHALL require the Subject or an authorized party (as defined in the applicable Fedn Agrmnt - see 63C#0350 i)) to give a runtime SSI authorization decision/consent prior to the transaction being executed.	✓	✓			
4.2		Runtime Decisions	The IdP MAY remember a subscriber's decision to authorize a given RP, provided that the IdP SHALL allow the subscriber to revoke such remembered access at a future time.	✓				*63C#0150*			If a CSP remembers a SSI authorization decision with regard to a specific RP, the CSP SHALL allow the Subject or an authorized party (as defined in the applicable Fedn Agrmnt - see 63C#0350 i)) to revoke that decision at any time.	✓	✓			
4.2		Runtime Decisions	[If an RP maintains a whitelist] All IdPs in an RP's whitelist SHALL abide by the provisions and requirements in the 800-63 [rev.3] suite.			✓		*63C#0 160*			RPs SHALL only include in their allowlists those CSPs which provide evidence of their conformity to the requirements in the SP 800-63 [rev.3] suite.	✓	✓		Inclusion of an RP within a white list allows the CSP to make decisions on info release when generating an assertion for the RP in question. In contrast, a gray list requires run-time consent (therefore consent clauses herein are moot if the RP is white-listed)	
4.2		Runtime Decisions	Every IdP that is not on a whitelist or a blacklist SHALL be placed by default in a gray area where runtime authorization decisions will be made by an authorized party, usually the subscriber		✓			*63C#0170*			If a CSP with which the RP is conducting a transaction is neither in an allowlist nor in a denylist, the RP SHALL proceed with the transaction only after gaining a runtime SSI authorization decision/consent from the Subject or an authorized party (as defined in the applicable Fedn Agrmnt - see 63C#0350 i)) prior to the transaction being executed.	✓	✓		See #0130	

4.2		Runtime Decisions	[If the RP remembers a subscriber's decision to authorize a given IdP] the RP SHALL allow the subscriber to revoke such remembered access at a future time.		✓			*63C#0180*			If an RP remembers the Subject's or an authorized party's (as defined in the applicable Fedn Agrmnt - see 63C#0350 i)) SSI authorization decision with regard to a specific CSP, the CSP SHALL allow the Subject or the authorized party to revoke that decision at any time.	✓	✓			
4.2		Runtime Decisions	A subscriber's information SHALL NOT be transmitted between IdP and RP for any purpose other than those described in Section 5.2, even when those parties are whitelisted.	✓	✓			*63C#0190*			Federation participants SHALL NOT transmit a Subject's SSI unless it is expressly for one of the following purposes:	✓	✓			
4.2		Runtime Decisions		✓	✓			*63C#0190*	*a)*		identity proofing, in accordance with the applicable Fed Agrmnt);	✓	✓			
4.2		Runtime Decisions		✓	✓			*63C#0190*	*b)*		identity authentication, in accordance with the applicable CrP (see in accordance with 63A#9999 and/or 63B#9999);	✓	✓			
4.2		Runtime Decisions		✓	✓			*63C#0190*	*c)*		attribute assertions, in accordance with the applicable CrP (see in accordance with 63A#9999 and/or 63B#9999);	✓	✓			
4.2		Runtime Decisions		✓	✓			*63C#0190*	*d)*		related fraud mitigation;	✓	✓			
4.2		Runtime Decisions		✓	✓			*63C#0190*	*e)*		to comply with applicable laws, regulations or other legal process;	✓	✓			
4.2		Runtime Decisions		✓	✓			*63C#0190*	*f)*		in response to a specific authorization.	✓	✓			
4.2		Runtime Decisions	To mitigate the risk of unauthorized exposure of sensitive information, the IdP SHALL, by default, mask sensitive information displayed to the subscriber.	✓				*63C#0200*			The CSP SHALL mask any SSI displayed to the Subject unless the Subject requests that the information be provided in clear.	✓	✓			
4.2		Runtime Decisions	The IdP SHALL provide mechanisms for the subscriber to temporarily unmask such information in order for the subscriber to view full values.	✓				*63C#0210*			The CSP SHALL limit the duration in which SSI is displayed in clear, subject to a maximum of 60 seconds or as specified in the applicable Federation Agreement.	✓	✓			
4.2		Runtime Decisions	The IdP SHALL provide effective mechanisms for redress of applicant complaints or problems.	✓				*63C#0220*			The CSP SHALL provide and publish mechanisms by which Subjects can resolve any complaints or problems.	✓	✓			
4.2		Runtime Decisions	When the subscriber is involved in a runtime decision, the subscriber SHALL receive explicit notice and be able to provide positive confirmation before any attributes about the subscriber are transmitted to any RP.	✓				*63C#0230*			The CSP SHALL ensure that, prior to any SSI attributes being transmitted to any RP, the Subject or an authorized party (as defined in the applicable Fedn Agrmnt - see 63C#0350 i)) SHALL receive explicit notice and be able to provide positive confirmation to those attributes' transmission.	✓	✓			
4.2		Runtime Decisions	If the protocol in use allows for optional attributes, the subscriber SHALL be given the option to decide whether to transmit those attributes to the RP.	✓				*63C#0240*			The CSP SHALL ensure that the notice and consent receipt processes required in 63C#0230 allow specific consent for the transmission of optional SSI.	✓	✓			
5		**Federation**															
5.1		**Federation Models**															
5.1.1		Manual Registration	In cases where an RP is not whitelisted, the IdP SHALL require runtime decisions (see Section 4.2) to be made by an authorized party (such as the subscriber) before releasing user information.	✓				*63C#0250*			If an RP with which the CSP is conducting a transaction is not in an allowlist the CSP SHALL require a runtime SSI authorization decision/consent from the Subject or an authorized party (as defined in the applicable Fedn Agrmnt - see 63C#0350 i)) prior to releasing SSI.	✓	✓			
5.1.1		Manual Registration	Protocols requiring the transfer of keying information SHALL use a secure method during the registration process to exchange keying information needed to operate the federated relationship, including any shared secrets or public keys.	✓	✓			*63C#0260*			Federation participants SHALL securely exchange any keying information (including any shared secrets or public keys) necessary to be used in federated transactions in accordance with the applicable Federation Agreement.	✓	✓			
5.1.1		Manual Registration				✓		*63C#0262*			Federation Authorities SHALL require that Federation participants securely exchange any keying information (including any shared secrets or public keys) necessary to be used in Federated transactions.	✓	✓			

5.1.1		Manual Registration	Any symmetric keys used in this [federated] relationship SHALL be unique to a pair of federation participants.	✓	✓			*63C#0270*			Symmetric keys used within a Federation SHALL be unique to each pair of participants.	✓	✓			
5.1.1		Manual Registration	Federation relationships SHALL establish parameters regarding expected and acceptable IALs and AALs in connection with the federated relationship.					*63C#0280*			See 63C#0350 i)	✓	✓			
5.1.2		Dynamic Registration	IdPs that support dynamic registration SHALL make their configuration information (such as dynamic registration endpoints) available in such a way as to minimize system administrator involvement.	✓				*63C#0290*			If the CSP supports dynamic registration it SHALL:	✓	✓			
5.1.2		Dynamic Registration		✓				*63C#0290*	*a)*		publish to the extent necessary its configuration information;	✓	✓			
5.1.2		Dynamic Registration		✓				*63C#0290*	*b)*		publish via an authoritative source that can be verified by all parties requiring access;	✓	✓			
5.1.2		Dynamic Registration		✓				*63C#0290*	*c)*		comply with the applicable specification protocol.	✓	✓			
5.1.2		Dynamic Registration	Protocols requiring the transfer of keying information SHALL use a secure method during the registration process to exchange keying information needed to operate the federated relationship, including any shared secrets or public keys.					*superseded*			See 63C#0260				NIST has commented that there is no differentiation to be made in these requirements at the level of granularity at which 63C is set.	
5.1.2		Dynamic Registration	Any symmetric keys used in this [federated] relationship SHALL be unique to a pair of federation participants.					*superseded*			See 63C#0270					
5.1.2		Dynamic Registration	IdPs SHALL require runtime decisions (see Section 4.2) to be made by an authorized party (such as the subscriber) before releasing user information.	✓				*63C#0300*			The CSP SHALL require the Subject or an authorized party (as defined in the applicable Fedn Agrmnt - see 63C#0350 i)) to give a runtime SSI authorization decision/consent prior to the transfer of any SSI.	✓	✓			
5.1.3		Federation Authorities	Federation authorities SHALL individually vet each participant in the federation to determine whether they adhere to their expected security, identity, and privacy standards.			✓		*63C#0310*			The Federation Authority SHALL ensure that each Federation participant has been approved in accordance with the provisions of the Federation Agreement defined in 63C#0350 b), such approval being based upon an assessment performed by either:	✓	✓		This excludes the possibility for self-assessment by federation participants. The FedAgrmnt should define the period of re-assessment and what level of sufficiency of conformance is to be achieved.	
5.1.3		Federation Authorities				✓		*63C#0310*	*a)*		the Federation Authority itself; OR	✓	✓			
5.1.3		Federation Authorities				✓		*63C#0310*	*b)*		an independent framework or independent assessor designated by the Federation Authority as being competent to perform and manage such approvals.	✓	✓			
			Kantara-specific criterion to bring into effect the need to have a documented Fedn Agrmnt	✓	✓	✓		*no tag required - explains applicability of following criteria (as referenced)*			The use of " (✓) " in criteria 63C#0320 - '#0350 inclusive is intended to indicate that, if a Federation Authority (FA) is in existence then, irresepctive of whether or not they are subject to Kantara Approval, they must provide a Federation Agreement to the other parties such that they can be assessed against concrete Federation requirements, but that in the absence of an FA, the parties in the federation must organize the creation of a Federation Agreement between themselves. The Applicants' S3A should make it clear which is the case and therefore, in each case, whether or not these criteria apply to them.	✓	✓			

			Kantara-specific criterion to bring into effect the need to have a documented Fedn Agrmnt	(✓)	(✓)	✓		*63C#0320*			Federation participants SHALL inter-operate in accordance with a documented Federation Agreement which SHALL define the obligations upon participants within the applicable Federation.	✓	✓		This criterion is specifc to Kantara - it serves to create the notion of the Fedn Agrmnt which is refered-to elsewhere. The Fedn Agrmnt is a 'coneptual document', i.e. its purpose may be fulfilled by one or more documents which need not bear the explicit name. They may also be owned by different parties so long as there is a clear broad understanding that the collective set of documents shall be adhered-to by all participants.	
5.1.3		Federation Authorities	Federation Authorities SHALL establish parameters regarding expected and acceptable IALs, AALs, and FALs in connection with the federated relationships they enable.	(✓)	(✓)	✓		*63C#0330*			The Federation Agreement SHALL, as a minimum, address:	✓	✓		The wording of this criterion (in its two parts) is intended to indicate the summation of areas which should be considered whilst using 'weasel' words to allow the FA (and others?) to show that they considered what was '**necessary**'.	
5.1.3		Federation Authorities		(✓)	(✓)	✓		*63C#0330*	*a)*		parameters regarding expected and acceptable IALs, AALs, and FALs;	✓	✓			
5.1.3		Federation Authorities (nb - this clause re-sequenced for the convenience of criteria creation)	Vetting of IdPs and RPs SHALL establish, as a minimum, that:	(✓)	(✓)	✓		*63C#0330*	*b)*		required assertion and protocol characteristics, which SHALL as a minimum address:	✓	✓		Derived directly from -63C Assumes that 'RP and IdP' are functional descriptions as much as specific entities, and therefore proxies/brokers are intrinsically included.	
5.1.3	1	Federation Authorities	1. Assertions generated by IdPs adhere to the requirements in Section 6	(✓)	(✓)	✓		*63C#0330*	*b)*	*i)*	generation of assertions in accordance with 63C#0430 to 63C#0640 inclusive;	✓	✓			
5.1.3	2	Federation Authorities	2. RPs adhere to IdP requirements for handling subscriber attribute data, such as retention, aggregation, and disclosure to third parties	(✓)	(✓)	✓		*63C#0330*	*b)*	*ii)*	RP adherence to CSP requirements concerning the handling of SSI;	✓	✓			
5.1.3	3	Federation Authorities	3. RP and IdP systems use approved profiles of federation protocols.	(✓)	(✓)	✓		*63C#0330*	*b)*	*iii)*	adherence to Federation protocols.	✓	✓			
				(✓)	(✓)	✓		*63C#0330*			and SHALL be assigned a unique identifier which accounts for the relevant date and/or version of issue of the Agreement.	✓	✓		The unique identifier should preferably be electronically parsable (e.g. a uri, oid or other unique form) or otherwise a definitive text string	
5.1.3	3	Federation Authorities	Federation authorities approve IdPs to operate at certain IALs, AALs, and FALs. This information is used by relying parties, as shown in the right side of Figure 5-4, to determine which identity providers meet their requirements.	(✓)	(✓)	✓		*63C#0340*			Federation Authorities SHALL:	✓	✓			
5.1.3	3	Federation Authorities		(✓)	(✓)	✓		*63C#0340*	*a)*		make available an up-to-date list of those CSPs in the federation which it has succesfully vetted; and	✓	✓			
5.1.3	3	Federation Authorities		(✓)	(✓)	✓		*63C#0340*	*b)*		provide in that list (see a), above) information pertaining to the CSP's services and IAL/AAL/FAL(s) at which they can operate within the federation.	✓	✓			
5.1.3		Federation Authorities	*Kantara-specific criterion to create consistency in the format and structure of Fedn Agrmnts*	(✓)	(✓)	✓		*63C#0350*			The Federation Agreement SHALL, as a minimum, address the need for:	✓	✓		The wording of this criterion is intended to indicate areas which should be considered whilst not absolutley mandating the inclusion of specific requirements in these areas.	
			Kantara-specific criterion to create consistency in the format and structure of Fedn Agrmnts	(✓)	(✓)	✓		*63C#0350*	*a)*		applicable terms and conditions;	✓	✓			
			Kantara-specific criterion to create consistency in the format and structure of Fedn Agrmnts	(✓)	(✓)	✓		*63C#0350*	*b)*		requirements for the scope and periodicity of Approvals, which SHALL as a minimum address:	✓	✓			
			Kantara-specific criterion to create consistency in the format and structure of Fedn Agrmnts	(✓)	(✓)	✓		*63C#0350*	*b)*	*i)*	initial approval to allow participation within the Federation;	✓	✓			
			Kantara-specific criterion to create consistency in the format and structure of Fedn Agrmnts	(✓)	(✓)	✓		*63C#0350*	*b)*	*ii)*	the periodicity of ongoing renewal or surveillance evaluations to enable retention of approval, which shall not be more than 36 months apart;	✓	✓		This could default to the requirements of Kantara's Approval Framework (SAH) if KI is to be the agreed basis of Approvals	

			Kantara-specific criterion to create consistency in the format and structure of Fedn Agrmnts	(✓)	(✓)	✓		*63C#0350*	*b)*	*iii)*	specific security, identity, and privacy standards to be conformed-to;	✓	✓			
			Kantara-specific criterion to create consistency in the format and structure of Fedn Agrmnts	(✓)	(✓)	✓		*63C#0350*	*b)*	*iv)*	how participation within the Federation can be terminated or will be revoked;	✓	✓		As b) ii)	
			Kantara-specific criterion to create consistency in the format and structure of Fedn Agrmnts	(✓)	(✓)	✓		*63C#0350*	*b)*	*v)*	any specific testing requirements which must be fulfilled (and their periodicity if more frequent than the period specified in (ii) above);	✓	✓			
			Kantara-specific criterion to create consistency in the format and structure of Fedn Agrmnts	(✓)	(✓)	✓		*63C#0350*	*b)*	*vi)*	how non-conformities are to be handled;	✓	✓		As b) ii)	
			Kantara-specific criterion to create consistency in the format and structure of Fedn Agrmnts	(✓)	(✓)	✓		*63C#0350*	*b)*	*vii)*	obligations upon the assessed party should its service be subjected to change or modification which results in a material change to the scope of its approval.	✓	✓			
			Kantara-specific criterion to create consistency in the format and structure of Fedn Agrmnts	(✓)	(✓)	✓		*63C#0350*	*c)*		Policy statements;	✓	✓			
			Kantara-specific criterion to create consistency in the format and structure of Fedn Agrmnts	(✓)	(✓)	✓		*63C#0350*	*d)*		Processes and working relationships;	✓	✓			
			Kantara-specific criterion to create consistency in the format and structure of Fedn Agrmnts	(✓)	(✓)	✓		*63C#0350*	*e)*		assertion profiles, protocols and associated meta-data;	✓	✓			
			Kantara-specific criterion to create consistency in the format and structure of Fedn Agrmnts	(✓)	(✓)	✓		*63C#0350*	*f)*		for which attributes references can be requested rather than full attributes,	✓	✓			
			Kantara-specific criterion to create consistency in the format and structure of Fedn Agrmnts	(✓)	(✓)	✓		*63C#0350*	*g)*		configuration data.	✓	✓			
			Kantara-specific criterion to create consistency in the format and structure of Fedn Agrmnts	(✓)	(✓)	✓		*63C#0350*	*h)*		which entities are recognized as having authority to grant approval for cryptographic functions (see 63C#0040).	✓	✓			
			Kantara-specific criterion to create consistency in the format and structure of Fedn Agrmnts	(✓)	(✓)	✓		*63C#0350*	*i)*		which parties are authorized to act of behalf of Subjects, and how their authority is established.	✓	✓			
			Kantara-specific criterion to create consistency in the format and structure of Fedn Agrmnts	(✓)	(✓)	✓		*63C#0350*	*j)*		parameters regarding expected and acceptable IALs and AALs to be used in Federated transactions.	✓	✓			
5.1.4		Proxied Federation	[A]all normative requirements that apply to IdPs and RPs SHALL apply to proxies in their respective roles [as an IdP on one side and an RP on the other].					*superseded*			This is achieved by Applicants indicating which of the parties in columns D, E, F & G apply to their specific service					
5.2		Privacy Requirements		✓	✓			*63C#0360*			Each federation participant SHALL conduct a Privacy Risk Assessment, based on Federal or industry standards, which addresses privacy risks appropriate to the Assurance Level being met.	✓	✓			
5.2		Privacy Requirements	If an IdP discloses information on subscriber activities at an RP to any party, or processes the subscriber's information for any purpose other than identity proofing, authentication, or attribute assertions (collectively "identity service"), related fraud mitigation, to comply with law or legal process, or in the case of a specific user request, to transmit the information, the IdP SHALL implement measures to maintain predictability and manageability commensurate with the privacy risk arising from the	✓	✓			*63C#0370*			Each federation participant's Privacy Risk Assessment SHALL addresses privacy risks associated with:	✓	✓			
5.2		Privacy Requirements		✓	✓			*63C#0370*	*a)*		disclosure of information on subscriber activities at an RP;	✓	✓		There is the assumption here that a CSP might be able to commit such exposures, depending on the nature of and visibility into the activities of the RP	
5.2		Privacy Requirements		✓	✓			*63C#0370*	*b)*		processing SSI for any purposes other than those described in 63C#0190 a) to f) inclusive;	✓	✓			
5.2		Privacy Requirements			✓			*63C#0370*	*c)*		the acceptability of the risks to SSI associated with sharing a pairwise pseudonymous identifier with other RPs;	✓	✓		This derives from 63C#0660 and applies solely to RPs, and not to CSPs	
5.2		Privacy Requirements			✓			*63C#0370*	*d)*		which SSI to request in an assertion.	✓	✓		This derives from 63C#0690 and applies solely to RPs, and not to CSPs	
5.2		Privacy Requirements		✓	✓			*63C#0380*			Each federation participant SHALL implement measures to maintain predictability and manageability commensurate with the outcomes of the Privacy Risk Assessment performed under 63C#0360 & #0370	✓	✓			

5.2		Privacy Requirements	When an IdP uses consent measures, the IdP SHALL NOT make consent for the additional processing a condition of the identity service.	✓				*63C#0390*			The CSP SHALL NOT make access to its services conditional upon the Applicant's provision of consent regarding SSI beyond that necessary to satisfy the applicable CrP and Privacy Policy.	✓	✓			
5.2		Privacy Requirements	The following requirements apply specifically to federal agencies:				✓	*63C#0400*			Federal Agencies SHALL:	✓	✓			
5.2		Privacy Requirements	1. The agency SHALL consult with their Senior Agency Official for Privacy (SAOP) to conduct an analysis determining whether the requirements of the Privacy Act are triggered by the agency that is acting as an IdP, by the agency that is acting as an RP, or both (see Section 9.4).				✓	*63C#0400*	*a)*		in consultation with the Agency's Senior Agency Official for Privacy, conduct an analysis determining whether the requirements of the Privacy Act are triggered, according to the agency's CSP and/or RP role(s).	✓	✓			
5.2		Privacy Requirements	2. The agency SHALL publish or identify coverage by a System of Records Notice (SORN) as applicable.				✓	*63C#0400*	*b)*		according to the outcome of the analysis in a) above, publish or identify coverage by a System of Records Notice, as applicable;	✓	✓			
5.2		Privacy Requirements	3. The agency SHALL consult with their SAOP to conduct an analysis determining whether the requirements of the E-Government Act are triggered by the agency that is acting as an IdP, the agency that is acting as an RP, or both.				✓	*63C#0400*	*c)*		in consultation with the Agency's Senior Agency Official for Privacy, conduct an analysis determining whether the requirements of the E-Government Act are triggered, according to the agency's CSP and/or RP role(s);	✓	✓			
5.2		Privacy Requirements	4. The agency SHALL publish or identify coverage by a Privacy Impact Assessment (PIA) as applicable.				✓	*63C#0400*	*d)*		according to the outcome of the analysis in c) above, publish or identify coverage by a Privacy Impact Assessment, as applicable.	✓	✓			
5.3		Reauthentication and Session Requirements in Federated Environments	The IdP SHALL communicate any information it has regarding the time of the latest authentication event at the IdP ... [*non-normative text snipped*]	✓				*63C#0410*			The CSP SHALL communicate to any requesting allowlisted RP the timestamp of the latest successful authentication event relating to the Subject.	✓	✓			
5.3		Reauthentication and Session Requirements in Federated Environments	The RP SHALL NOT assume that the subscriber has an active session at the IdP past the establishment of the federated log in.		✓			*63C#0420*			The RP SHALL make and make known to relevant parties its own determination as to whether to implement 'Single Sign-out'.	✓	✓			
5.3		Reauthentication and Session Requirements in Federated Environments	The IdP SHALL NOT assume that termination of the subscriber's session at the IdP will propagate to any sessions that subscriber would have at downstream RPs.					*n/a*			No criterion required					
6		**Assertions**															
6		Assertions	All assertions SHALL include the following assertion metadata:	✓				*63C#0430*			All assertions generated by the CSP SHALL include, at least, the following assertion metadata:	✓	✓			
6	1	Assertions	1. Subject: An identifier for the party that the assertion is about (i.e., the subscriber).	✓				*63C#0430*	*a)*		a unique identifier (within the domain of its service) for the Subject to which the assertion relates;	✓	✓			
6	2	Assertions	2. Issuer: An identifier for the IdP that issued the assertion.	✓				*63C#0430*	*b)*		a unique identifier for the CSP issuing the assertion;	✓	✓			
6	3	Assertions	3. Audience: An identifier for the party intended to consume the assertion (i.e., the RP).	✓				*63C#0430*	*c)*		a unique identifier for the RP by whom the assertion is intended to be consumed;	✓	✓			
6	4	Assertions	4. Issuance: A timestamp indicating when the IdP issued the assertion.	✓				*63C#0430*	*d)*		a timestamp indicating when the IdP generated the assertion;	✓	✓			

6	5	Assertions	5. Expiration: A timestamp indicating when the assertion expires and SHALL no longer be accepted as valid by the RP (i.e., the expiration of the assertion and not the expiration of the session at the RP).	✓				*63C#0430*	*e)*		an indication of the period of validity or the expiration time of the assertion, post issuance;	✓	✓			
6	6	Assertions	6. Identifier: A value uniquely identifying this assertion, used to prevent attackers from replaying prior assertions.	✓				*63C#0430*	*f)*		a unique identifier for the specific assertion;	✓	✓			
6	7	Assertions	7. Signature: Digital signature or message authentication code (MAC), including key identifier or public key associated with the IdP, for the entire assertion.	✓				*63C#0430*	*g)*		a cryptographic authentication signature, covering the entirety of the assertion (including any fields in addition to these required herewith) with the associated key identifier;	✓	✓			
6	8	Assertions	8. Authentication Time: A timestamp indicating when the IdP last verified the presence of the subscriber at the IdP through a primary authentication event (if available).	✓				*63C#0430*	*h)*		a timestamp for the latest successful authentication event relating to the Subject of the assertion;	✓	✓			
			Kantara-specific criterion to create a complementary criterion, to phrase appropriately the requirements for CSPs (Kantara-speak) and RPs	✓				*63C#0430*	*i)*		the assurance level of the authentication event.	✓	✓			
6		Assertions	Assertions SHOULD specify the AAL when an authentication event is being asserted and IAL when identity proofed attributes (or references based thereon) are being asserted. If not specified, the RP SHALL NOT assign any specific IAL or AAL to the assertion		✓			*63C#0440*			If an assertion contains no specification as to the applicable Assurance Level the RP SHALL NOT assign any specific IAL and/or AAL to the assertion	✓	✓			
6		Assertions	An RP SHALL treat subject identifiers as not inherently globally unique. Instead, the value of the assertion's subject identifier is usually in a namespace under the assertion issuer's control.		✓			*63C#0450*			The RP SHALL only consider the identifier for the Subject to which the assertion relates as being unique within the context of the issuing CSP.	✓	✓			
6		Assertions	The ability to successfully fetch such additional attributes SHALL NOT be treated as equivalent to processing the assertion.		✓			*63C#0460*			The RP SHALL require receipt of an assertion indicating that the Subject has been successfully authenticated prior to effecting any resultant transaction.	✓	✓			
6		Assertions	[A]n assertion SHALL NOT be used past the expiration time contained therein.		✓			*63C#0470*			The RP SHALL NOT rely upon an assertion once its period of validity has expired;	✓	✓			
6		Assertions	Assertion lifetimes SHALL NOT be used to limit the session at the RP.		✓			*63C#0480*			The RP SHALL NOT, once having accepted an assertion, use the assertion's expiration as a reason for limiting or extending the Subject's session's duration at the RP.	✓	✓			
6.1		Assertion Binding															
6.1.1		Bearer Assertions															
6.1.1		Bearer Assertions	When processing holder-of-key assertions:		✓			*63C#0490*			When processing holder-of-key assertions the RP SHALL:		✓			
6.1.2	1	Holder-of-Key Assertions	1. The subscriber SHALL prove possession of that key to the RP, in addition to presentation of the assertion itself.		✓			*63C#0490*	*a)*		require the Subject to prove possession the key;		✓			

6.1.2	2	Holder-of-Key Assertions	2. An assertion containing a reference to a key held by the subscriber for which key possession has not been proven SHALL be considered a bearer assertion by the RP.		✓			*63C#0490*	*b)*		treat a reference to a key held by the Subject for which key possession has not been proven as a bearer assertion;		✓			
6.1.2	3	Holder-of-Key Assertions	3. Reference to a given key SHALL be trusted at the same level as all other information within the assertion.		✓			*63C#0490*	*c)*		treat the key reference with the same level of assurance as the assertion;		✓			
6.1.2	4	Holder-of-Key Assertions	4. The assertion SHALL NOT include an unencrypted private or symmetric key to be used with holder-of-key presentation.	✓				*63C#0500*			The CSP SHALL NOT create assertions which include unencrypted private or symmetric keys to be used with holder-of-key presentations.		✓			
6.2		Assertion Protection	[A]ssertions SHALL include a set of protections to prevent attackers from manufacturing valid assertions or reusing captured assertions at disparate RPs.	✓	✓			*63C#0510*			Federation participants SHALL implement within assertions it generates measures to prevent attackers from manufacturing valid assertions or reusing captured assertions at RPs for which the assertion was not intended.	✓	✓			
6.2.1		Assertion Identifier	Assertions SHALL be sufficiently unique to permit unique identification by the target RP.	✓				*superseded*			Covered by #0430 a) & b), #0450					
6.2.2		Signed Assertion	Assertions SHALL be cryptographically signed by the issuer (IdP).	✓				*superseded*			Covered by #0430 g)					
6.2.2		Signed Assertion	This signature SHALL cover the entire assertion, including its identifier, issuer, audience, subject, and expiration.	✓				*superseded*			Covered by #0430 g)					
6.2.2		Signed Assertion	The RP SHALL validate the digital signature or MAC of each such assertion based on the issuer's key.		✓			*63C#0520*			The RP SHALL only process assertions for which it is able to validate the cryptographic signature using the issuer's key.	✓	✓			
6.2.2		Signed Assertion	The assertion signature SHALL either be …	✓				*superseded*			Covered by 63C#0430 g)					
6.2.2		Signed Assertion	… a digital signature using asymmetric keys or …					n/a			No criterion required					
6.2.2		Signed Assertion	… a MAC using a symmetric key shared between the RP and issuer.					n/a			No criterion required					
6.2.2		Signed Assertion	Shared symmetric keys used for this purpose by the IdP SHALL be independent for each RP to which they send assertions,	✓				*63C#0530*			The CSP SHALL manage its symmetric signing keys such that each is shared exclusively with only one discrete RP.	✓	✓			
6.2.2		Signed Assertion	Approved cryptography SHALL be used.	✓	✓			*63C#0540*			Each federation participant SHALL only use cryptography approved by a national technical authority or other generally-recognized authoritative body.	✓	✓			
6.2.3		Encrypted Assertion	The IdP SHALL encrypt the contents of the assertion using either the RP's public key or a shared symmetric key	✓				*superseded*			Covered by 63C#0430 g)					
6.2.3		Encrypted Assertion	Shared symmetric keys used for this purpose by the IdP SHALL be independent for each RP to which they send assertions	✓				*superseded*			Covered by #0530					
6.2.3		Encrypted Assertion	All encryption of assertions SHALL use approved cryptography.	✓				*superseded*			Covered by #0540					
6.2.3		Encrypted Assertion	When assertions are passed through third parties, such as a browser, the actual assertion SHALL be encrypted	✓				*63C#0550*			The CSP SHALL encrypt any assertions which it generates and which are passed through third parties.	✓	✓			
6.2.3		Encrypted Assertion	An assertion passed directly between IdP and RP SHALL be either …	✓				*63C#0560*			If the CSP passes an assertion directly to the RP for which it was intended the assertion SHALL be either:	✓	✓			
6.2.3		Encrypted Assertion	… encrypted OR …	✓				*63C#0560*	*a)*		encrypted; OR	✓	✓			
6.2.3		Encrypted Assertion	… sent over an authenticated protected channel.	✓				*63C#0560*	*b)*		sent over a mutually-authenticated protected channel.	✓	✓			

6.2.4		Audience Restriction	Assertions SHALL use audience restriction techniques to allow an RP to recognize whether or not it is the intended target of an issued assertion.	✓				*63C#0570*			The CSP SHALL employ mechanisms to ensure that assertions it generates can be restricted to being consumed only by the RP for which it was intended.	✓	✓		When a proxy acts as an RP it should be able to determine that it is the intended recipient for the purposes of passing-through the assertion	
6.2.4		Audience Restriction	All RPs SHALL check that the audience of an assertion contains an identifier for their RP to prevent the injection and replay of an assertion generated for one RP at another RP.		✓			*63C#0580*			The RP SHALL employ mechanisms to ensure that it only consumes assertions for which the issuing CSP intended it to be the recipient.	✓	✓			
		Pairwise Pseudonymous Identifiers															
6.3.1		General Requirements	When using pairwise pseudonymous subject identifiers within the assertions generated by the IdP for the RP, the IdP SHALL generate a different identifier for each RP [as described in Section 6.3.2]	✓				*superseded*			Covered by 63C#0610 - '#0640 inclusive.				Refer to §6.3.2	
6.3.1		General Requirements	[A proxy acting as an IdP] SHALL NOT disclose the mapping between the pairwise pseudonymous identifier and any other identifiers to a third party …	✓				*63C#0590*			When acting as a proxy, the CSP SHALL NOT disclose to a third party the mapping between the pairwise pseudonymous identifier and any other identifiers.	✓	✓		In this criterion third parties would be any party other than the CSP itself (1st party) and those RPs (2nd parties) with whom the pairwise identifier is explicitly shared. Note that although notionally 'pairwise' is the CSP and a single 2nd party being the applicable pair, criterion 63C#0650 allows for such identifiers to be shared with mutliple mutually-agreeable RPs. Third parties might therefore be any party outside the set of RPs (including a set of one) agreeing to share the pairwise identifier with the CSP.	
6.3.1		General Requirements	… or use the information for any purpose other than federated authentication, related fraud mitigation, to comply with law or legal process, or in the case of a specific user request for the information.	✓				*63C#0600*			When acting as a proxy, the CSP SHALL NOT use the mapping between the pairwise pseudonymous identifier and any other identifiers. for any purpose other than:	✓	✓			
6.3.1		General Requirements		✓				*63C#0600*	*a)*		federated authentication;	✓	✓			
6.3.1		General Requirements		✓				*63C#0600*	*b)*		related fraud mitigation;	✓	✓			
6.3.1		General Requirements		✓				*63C#0600*	*c)*		to comply with applicable laws, regulations or other legal process;	✓	✓			
6.3.1		General Requirements		✓				*63C#0600*	*d)*		in response to a specific user request, which SHALL be logged and recorded.	✓	✓			
6.3.2		Pairwise Pseudonymous Identifier Generation	Pairwise pseudonymous identifiers SHALL contain no identifying information about the subscriber.	✓				*63C#0610*			The CSP SHALL NOT create pairwise pseudonymous identifiers which contain any SSI	✓	✓			
6.3.2		Pairwise Pseudonymous Identifier Generation	Pairwise pseudonymous identifiers SHALL be unguessable by a party having access to some information identifying the subscriber.	✓				*63C#0620*			The CSP SHALL create pairwise pseudonymous identifiers such that any party having access to some SSI is nonetheless unable to guess their actual identity	✓	✓			
6.3.2		Pairwise Pseudonymous Identifier Generation	Normally, the identifiers SHALL only be known by and used by one pair of endpoints (e.g., IdP-RP). [However, an IdP MAY generate the same identifier for a subscriber at multiple RPs at the request of those RPs, provided: • Those RPs have a demonstrable relationship that justifies an operational need for the correlation, such as a shared security domain or shared legal ownership;	✓	✓			*63C#0630*			Federation participants SHALL ensure that pairwise pseudonymous identifiers which it creates either:	✓	✓			
6.3.2		Pairwise Pseudonymous Identifier Generation		✓	✓			*63C#0630*	*a)*		only be known and used with a single RP; or	✓	✓			
6.3.2		Pairwise Pseudonymous Identifier Generation		✓	✓			*63C#0630*	*b)*		are used with multiple RPs, each of which has:	✓	✓			
6.3.2		Pairwise Pseudonymous Identifier Generation		✓	✓			*63C#0630*	*b)*	*i)*	requested that the identifier be shared;	✓	✓			
6.3.2		Pairwise Pseudonymous Identifier Generation		✓	✓			*63C#0630*	*b)*	*ii)*	demonstrated a relationship with each other RP in a manner which conforms to the CSP's CrP; and	✓	✓			
6.3.2		Pairwise Pseudonymous Identifier Generation		✓	✓			*63C#0630*	*b)*	*iii)*	consented to being thereby correlated with the other RPs.	✓	✓			
6.3.2		Pairwise Pseudonymous Identifier Generation	The RPs SHALL conduct a privacy risk assessment to consider the privacy risks associated with requesting a common identifier.					*superseded*			Covered by 63C#0350 c)					
6.3.2		Pairwise Pseudonymous Identifier Generation	The IdP SHALL ensure that only intended RPs are correlated.	✓				*63C#0640*			The CSP SHALL, prior to sharing a pairwise pseudonymous identifier, implement measures to ensure that only intended RPs are correlated.	✓	✓			

7		Assertion Presentation														
7		Assertion Presentation	The IdP SHALL transmit only those attributes that were explicitly requested by the RP.	✓				*63C#0650*			The CSP SHALL populate an assertion with only the SSI explicitly requested by the RP and authorized by the Subject or an authorized party (as defined in the applicable Fedn Agrmnt - see 63C#0350 i))	✓	✓			
7		Assertion Presentation	RPs SHALL conduct a privacy risk assessment when determining which attributes to request.					*superseded*			Covered by 63C#0350 d)					
7.1		Back-Channel Presentation	[Back-Channel] assertion references SHALL contain no information about the subscriber and …	✓				*63C#0660*			The CSP SHALL not create assertion references which contain SSI	✓	✓			
7.1		Back-Channel Presentation	[Back-Channel] assertion references] … SHALL be resistant to tampering and fabrication by an attacker.	✓				*63C#0670*			The CSP SHALL create and transmit assertion references such that they are resistant to tampering and fabrication by an attacker.	✓	✓			
7.1		Back-Channel Presentation	[A]ssertion references SHALL:	✓				*63C#0680*			The CSP SHALL create assertion references which are:	✓	✓			
7.1	1	Back-Channel Presentation	1. be limited to use by a single RP.	✓				*63C#0680*	*a)*		limited to use by a single RP;	✓	✓			
7.1	2	Back-Channel Presentation	2. be single-use.	✓				*63C#0680*	*b)*		able to be used only a single time.	✓	✓			
7.1		Back-Channel Presentation	The RP SHALL protect itself against injection of manufactured or captured assertion references by use of cross-site scripting protection or other accepted techniques.		✓			*63C#0690*			The RP SHALL employ measures, appropriate to the Assurance Level being asserted which protect it from injection of manufactured or captured assertion references	✓	✓		Applies to both Front & Back channels	
7.1		Back-Channel Presentation	Elements within the assertion SHALL be validated by the RP, including:		✓			*63C#0700*			The RP SHALL validate an assertion by ensuring that:	✓	✓			
7.1		Back-Channel Presentation	1. Issuer verification: ensuring the assertion was issued by the IdP the RP expects it to be from.		✓			*63C#0700*	*a)*		the signature applied to the assertion can be authenticated as being that belonging to the CSP from which a response is expected					
7.1		Back-Channel Presentation	2. Signature validation: ensuring the signature of the assertion corresponds to the key related to the IdP sending the assertion.									✓	✓			
7.1		Back-Channel Presentation	3. Time validation: ensuring the expiration and issue times are within acceptable limits of the current timestamp.		✓			*63C#0700*	*b)*		its issue and expiration times are within an acceptable range of the current date/time;	✓	✓			
7.1		Back-Channel Presentation	4. Audience restriction: ensuring this RP is the intended recipient of the assertion.		✓			*63C#0700*	*c)*		the RP itself is that for which the assertion is intended.	✓	✓			
7.1		Back-Channel Presentation	Conveyance of the assertion reference from the IdP to the subscriber, as well as from the subscriber to the RP, SHALL be made over an authenticated protected channel.	✓	✓			*63C#0710*			Federation participants SHALL ensure that all transmission of assertion references [and any other communication] between themselves and between themselves and the Subject occurs over a mutually-authenticated protected channel.	✓	✓			
7.1		Back-Channel Presentation	Conveyance of the assertion reference from the RP to the IdP, as well as the assertion from the IdP to the RP, SHALL be made over an authenticated protected channel.					*superseded*			Covered by 63C#0710					
7.1		Back-Channel Presentation	When assertion references are presented, the IdP SHALL verify that the party presenting the assertion reference is the same party that requested the authentication.	✓				*63C#0720*			The CSP SHALL authenticate the source of any assertion reference as being from the same party as requested the authentication.	✓	✓			
7.2		Front-Channel Presentation	The RP SHALL protect itself against injection of manufactured or captured assertions by use of cross-site scripting protection or other accepted techniques.		✓			*63C#0730*			The RP SHALL employ measures, appropriate to the Assurance Level being asserted which protect it from injection of manufactured or captured assertion references	✓	✓		This criterion needs to be separately addressed if 63C#0730 does not include protections for the specified parties and applicable channels	
7.2		Front-Channel Presentation	Elements within the assertion SHALL be validated by the RP including:		✓			*63C#0740*			The RP SHALL validate an assertion by ensuring that:	✓	✓		This criterion needs to be separately addressed if 63C#0740 does not include protections for the specified parties and applicable channels	

7.2	1	Front-Channel Presentation	1. Issuer verification: ensuring the assertion was issued by the expected IdP.		✓			*63C#0740*	*a)*		it was issued by the CSP from which a response is expected;	✓	✓		This criterion needs to be separately addressed if 63C#0740 does not include protections for the specified parties and applicable channels	
7.2	2	Front-Channel Presentation	2. Signature validation: ensuring the signature of the assertion corresponds to the key related to the IdP making the assertion.		✓			*63C#0740*	*b)*		its signature can be authenticated as being that belonging to the CSP which sent the assertion;	✓	✓		This criterion needs to be separately addressed if 63C#0740 does not include protections for the specified parties and applicable channels	
7.2	3	Front-Channel Presentation	3. Time validation: ensuring the expiration and issue times are within acceptable limits of the current timestamp.		✓			*63C#0740*	*c)*		its issue and expiration times are within acceptable limits of the current date/time;	✓	✓		This criterion needs to be separately addressed if 63C#0740 does not include protections for the specified parties and applicable channels	
7.2	4	Front-Channel Presentation	4. Audience restriction: ensuring this RP is the intended recipient of the assertion.		✓			*63C#0740*	*d)*		the RP itself is that for which the assertion is intended.	✓	✓		This criterion needs to be separately addressed if 63C#0740 does not include protections for the specified parties and applicable channels	
7.2		Front-Channel Presentation	Conveyance of the assertion from the IdP to the subscriber, as well as from the subscriber to the RP, SHALL be made over an authenticated protected channel.	✓	✓			*63C#0750*			Federation participants SHALL ensure that all transmission of assertion references [and any other communication] between themselves and between themselves and the Subject occurs over a mutually-authenticated protected channel.	✓	✓		This criterion needs to be separately addressed if 63C#0750 does not include protections for the specified parties and applicable channels	
7.3		Protecting Information	Communications between the IdP and the RP SHALL be protected in transit using an authenticated protected channel.	✓	✓			*63C#0760*			Federation participants SHALL ensure that all transmission of assertion references [and any other communication] between themselves and between themselves and the Subject occurs over a mutually-authenticated protected channel.	✓	✓		This criterion needs to be separately addressed if 63C#0750 does not include protections for the specified parties and applicable channels	
7.3		Protecting Information	Communications between the subscriber and either the IdP or the RP (usually through a browser) SHALL be made using an authenticated protected channel.					*superseded*			Covered by 63C#0760					
7.3		Protecting Information	The RP SHALL, where feasible, request attribute references rather than full attribute values.		✓			*63C#0770*			The RP SHALL, where feasible, request attribute references rather than full attributes, in accordance with the Federation Agreement (see 63C#0350).	✓	✓			
7.3		Protecting Information	The IdP SHALL support attribute references.	✓				*63C#0780*			The CSP SHALL support attribute references when requested.	✓	✓			
End of 63C criteria								***End of 63C criteria***								

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

		Initials
The Kantara Glossary and Overview (KIAF-1050) is the formal reference for these definitions.		
Federation Agreement	documented provisions against which participants within a Federation have agreed to operate.	
Sensitive Subject Information	information of a personal or sensitive nature relating to a Subject. Abbrv: SSI	

Comment

#REF!

#REF!

#REF!

#REF!

#REF!

#REF!

#REF!

#REF!

Notes to the creation of Kantara 63C criteria.

63C is very explicit in assigning its normative clauses to specific roles within a Federation, these being IdPs (which these criteria treat as 'CSPs vernacular), RPs, Federation Authorities and Federal Agencies. Thus, each criterion drafted for Kantara is assigned to one or more of these role since the role of a proxy may also feature within a federation, clauses relating to Proxies is indicated by being assigned to both IdPs and RPs.

An IdP (per NIST) is synonymous with a CSP (per Kantara). The CSP may act as a proxy, in which case it shall also include within the scope of its criteria flagged as being applicable to RPs, in addition to those criteria associated with IdPs.

A CSP could serve exclusively as a proxy, in which case the applicable criteria would be 63B_SAC and 63C_SAC (and optionally CO_SAC, if not a assessment).

Alternatively, the Fedn Authy role may be filled by an entity which performs no operational/transactional functions, with the applicable criteria accordingly. Is there a case for creating a distinct (sub-)Class of Approval for this?

63C refers to a 'Federation Authority' (FA - most specifically §5.1.3) to which are assigned various responsibilities using terms such as establish relationship", whether or not they explicitly "approve" federation members, establishing "parameters regarding expected and acceptable" assu "expected security, identity, and privacy standards", and "publishing configuration data". As §5.1.1 and §5.1.3 reveal a FA may be a self-determ may be a generally-recognized authoritative body. However, 63C also makes the point that a federation may not have a Federation Authority, can neither make a normative requirement that there be one, not an it assume there will be one. Kantara's 63C criteria use the term 'Federati common phrase to encompass whatever it is the applicable Federation Authority or the federation participants choose to set forth. Clearly, fro clauses, a Federation Agreement could include policy at the highest level and/or anything working through processes, procedures, standards, pr However, Kantara has no basis based on 63C to dictate any specific a structure or form of a Federation Agreement although it wouldn't be too something if that assisted federated operations. However, for the scope of these criteria, the term 'Federation Agreement' is used to embrace defined to enable the federation to function harmoniously and criteria require only that the FednAgrmnt be documented and 'applied in full'. Federation there needs to be a generally-recognized authority for the purposes of defining the agreement, which could be a shared responsibili

HOW FAs are expected to ensure that all Federation participants meet the SP 800-63C requirements is not clear, nor is it in any way implied. A is perfectly reasonable, but in the context of writing a Kantara interpretation of that clause it raises a major question about how that can be ex obvious partial solution, with a very Kantara-specific point of view, is that the members of the Federation should each hold Kantara Approval. 'NIST 800-63 rev.3' Class of Approval (which it is assumed would undergo expansion to include FAL2), i.e. the FA would require IdPs to hold Kar is presently no means to assess and Approve RPs. Should there now be? And what about Fed agencies??

Though it might be legitimate for KI to expect the Federation participants to be Approved some way, it may be a bridge too far to recognise ON
The effect of doing so might be more detrimental (i.e. an impediment to Federations being able to meet the requirement and a rejection of KI)
a flood of applicants to Kantara's door). Therefore it seems necessary to avoid the explicit imposition of Kantara Approvals being required.