KIAF-1	Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'			IAL		CRITERION APPLICABILITY (SoCA)
§	CSP	RP	FA	US Fed Agcy	63A tag	index	KI_criterion (text in red is new this version)	2	3	read this comment
4.2	✓				63A#0010		The CSP SHALL NOT perform identity proofing to determine suitability or entitlement to gain access to services or benefits.	✓	✓	In scope - Applicable
4.2	✓				63A#0020		The CSP SHALL limit collection of PII to the minimum necessary to validate and resolve the existence of the claimed identity uniquely in a given context, and to associate the claimed identity with the Applicant providing identity evidence for appropriate identity resolution, validation, and verification.	✓	✓	In scope - Applicable
4.2	✓				63A#0030		The CSP SHALL document and publish a Privacy Notice which describes its purposes in collecting and maintaining a record of the attributes necessary for identity proofing, including whether such attributes are voluntary or mandatory to complete the identity proofing process, and the consequences for not providing the attributes.	✓	✓	In scope - Applicable
4.2	✓				63A#0040		The CSP SHALL explicitly make its Privacy Notice available to the Applicant at the time of collection of the attributes necessary for the Applicant's identity proofing.	✓	✓	In scope - Applicable
4.2	✓				63A#0050		If the CSP processes attributes which it collects and stores for purposes other than identity proofing, authentication, or attribute assertions, related fraud mitigation, or to comply with law or legal process), it SHALL:	✓	✓	In scope - Not applicable ID.me's CrP states that no such additional use shall be made
4.2	✓				63A#0050	a)	document and apply predictability and manageability measures associated with those additional processes based on the results of its privacy risk assessment; (see 63A#0160)	✓	✓	In scope - Not applicable See above
4.2	✓				63A#0050	b)	NOT make consent to processing of these additional attributes a condition of provision of the service.	✓	✓	In scope - Not applicable See above
4.2	✓				63A#0060		The CSP SHALL provide mechanisms to redress Applicant complaints or problems arising from their use of the identity proofing service.	✓	✓	In scope - Applicable
	✓				63A#0062		The CSP SHALL document and publish its redress mechanisms in a manner which is easy for Applicants to find and use.	✓	✓	In scope - Applicable
4.2	✓				63A#0070		The CSP SHALL review its redress mechanisms at least every 12 months and assess their efficacy in achieving resolution of complaints or problem , implementing corrective action when efficacy falls below defined thresholds of performance or accomplishment.	✓	✓	In scope - Applicable
4.2	✓				63A#0080		The CSP SHALL:	✓	✓	In scope - Applicable
4.2	✓				63A#0080	a)	document in a Credential Policy (CrP) its identity proofing and enrollment policy/ies;	✓	✓	In scope - Applicable
4.2	✓				63A#0080	b)	for each type of identity proofing offered (see 63A#0260), state which issuing and authoritative sources are used to prove identities;	✓	✓	In scope - Applicable
4.2	✓				63A#0080	c)	state any eligibility requirements or limitations which it applies to the scope of Applicants to its identity proofing service, subject to such limitations not breaching the restriction placed by 63A#0010;	✓	✓	In scope - Applicable
4.2	✓				63A#0080	d)	publish its CrP such that it is available to members of the intended community (e.g. Applicants, Subscribers, Relying Parties, …) before they are required to commit to signing-up to being a subject of the policy.	✓	✓	In scope - Applicable
4.2	✓				63A#0090		The CSP SHALL document in its Credentialing Practices Statement (CrPS) the practices which it implements to fulfil its CrP intentions.	✓	✓	In scope - Applicable
4.2	✓				63A#0100		The CSP's CrPS SHALL reflect the structure of its CrP and SHALL include control information detailing how the CSP handles proofing errors or other circumstances that result in an Applicant not being successfully enrolled.	✓	✓	In scope - Applicable
4.2	✓				63A#0110		The CSP SHALL document both its risk management process (at least in the context of its identity proofing policy and practices) and the outcomes of applying that process.	✓	✓	In scope - Applicable
	✓				63A#0120		The CSP SHALL conduct its risk management process at least once every six months and whenever there is a material change to its CrP, and SHALL include assessment of privacy and security risks, accounting for:	✓	✓	In scope - Applicable
4.2	✓				63A#0120	a)	Any steps that it will take to verify the identity of the Applicant beyond any mandatory requirements specified herein;	✓	✓	In scope - Applicable
4.2	✓				63A#0120	b)	The PII which the CSP shall collect and store (per its CrP), including any biometrics, images, scans, or other copies of the identity evidence that the CSP will maintain as a record of identity proofing; and	✓	✓	In scope - Applicable
4.2	✓				63A#0120	c)	The CSP's Retention Schedule requirements for collected PII and associated records, accounting for applicable laws, regulations, contracts, and policies.	✓	✓	In scope - Applicable
4.2	✓				63A#0130		The CSP SHALL maintain a record, including audit logs, of:	✓	✓	In scope - Applicable
4.2	✓				63A#0130	a)	the type of identity proofing performed;	✓	✓	In scope - Applicable
4.2	✓				63A#0130	b)	the types of and a unique reference to identity evidence collected from the Applicant in the proofing process;	✓	✓	In scope - Applicable
4.2	✓				63A#0130	c)	PII or other responses collected from authoritative and/or issuing sources;	✓	✓	In scope - Applicable
4.2	✓				63A#0130	d)	all steps taken to validate the identity evidence;	✓	✓	In scope - Applicable
4.2	✓				63A#0130	e)	all steps taken to verify the identity of the Applicant;	✓	✓	In scope - Applicable
4.2	✓				63A#0130	f)	the outcome of each step, culminating in the final proofing result.	✓	✓	In scope - Applicable
4.2	✓				63A#0140		The CSP SHALL protect all PII collected as part of the enrollment process, including validation and verification sources used, to ensure its confidentiality, integrity, and attribution of the information source.	✓	✓	In scope - Applicable
4.2	✓				63A#0150		The CSP shall use authenticated protected channels during the entire proofing transaction, including exchanges with third parties.	✓	✓	In scope - Applicable
4.2	✓				63A#0160		If the CSP uses fraud mitigation measures, it SHALL include these measures in its privacy risk assessment for these mitigation measures.	✓	✓	In scope - Applicable
4.2	✓				63A#0170		The CSP SHALL define the practices in place for fully disposing of or destroying any sensitive data including PII, or its protection from unauthorized access for the duration of retention. Specific details of these practices must be made available.	✓	✓	In scope - Applicable
4.4 (IAL2)					n/a					
4.4.1.1 (IAL2)					n/a		See 63A#0020			
4.4.1.2 (IAL2)	✓				63A#0180		The CSP SHALL collect from the Applicant at least the following strength of evidence, as determined by the further requirements in Table 5-1:	✓		In scope - Applicable

4.4.1.2 (IAL2)	✓					63A#0180	a)		One piece of STRONG evidence **IF** the evidence's issuing source, during its identity proofing event, confirmed the claimed identity by collecting two or more forms of SUPERIOR or STRONG evidence **AND** the CSP validates the evidence directly with the issuing source; **OR**	✓		In scope - Not applicable No SUPERIOR forms of evidence claimed
4.4.1.2 (IAL2)	✓					63A#0180	b)		Two pieces of STRONG evidence; OR	✓		In scope - Applicable
4.4.1.2 (IAL2)	✓					63A#0180	c)		One piece of STRONG evidence plus two pieces of FAIR evidence.	✓		In scope - Applicable
4.4.1.2 (IAL2)	✓					63A#0190			The CSP SHALL document its justification, for each form of evidence it recognises and collects in fulfilling its CrP and these criteria, of how the strength of the evidence it collects satisfies the qualities identified in Table 5-1 [see worksheet 63A_TS-1].	✓		In scope - Applicable
4.4.1.3 (IAL2)	✓					63A#0200			The CSP SHALL, at a minimum, validate identity evidence at the same strength as that at which the evidence was collected.	✓	✓	In scope - Applicable
	✓					63A#0210			The CSP SHALL document its justification, for each form of evidence it recognises and collects in fulfilling its CrP and these criteria, of how the strength of validation of the evidence it collects satisfies the qualities identified in Table 5-2 [see worksheet 63A_TS-2].	✓	✓	In scope - Applicable
4.4.1.3 (IAL2)	✓					63A#0220			The CSP SHALL document its policies, guidelines, and requirements for the training of personnel validating evidence	✓	✓	In scope - Applicable
												In scope - Applicable
4.4.1.4 (IAL2)	✓					63A#0230			The CSP SHALL, at a minimum, verify the Applicant's binding to the identity evidence at a strength of STRONG;	✓		In scope - Applicable
4.4.1.4 (IAL2)	✓					63A#0240			Knowledge-based verification (KBV) SHALL NOT be used for Supervised (In-person or Remote) identity verification.	✓		In scope - Applicable
4.4.1.4 (IAL2)	✓					63A#0250			The CSP SHALL document its justification, for each form of evidence it recognises in fulfilling its CrP and these criteria, of how the strength of verification of the evidence it collects meets, at a minimum, the STRONG qualities identified in Table 5-3 [see worksheet 63A_TS-3].	✓		In scope - Applicable
4.4.1.4 (IAL2)	✓								Refer to Worksheet 63A_TS-3	✓		In scope - Applicable
4.4.1.5 (IAL2)	✓					63A#0260			The CSP SHALL offer at least one of the following types of identity proofing and SHALL clearly state in its CrP which of those types it provides, describing clearly how requirements between multiple identity proofing types differ.	✓		In scope - Applicable
4.4.1.5 (IAL2)	✓					63A#0260	a)		Supervised (In-person);	✓		In scope - Applicable
4.4.1.5 (IAL2)	✓					63A#0260	b)		Supervised (Remote);	✓		In scope - Applicable
4.4.1.5 (IAL2)	✓					63A#0260	c)		Unsupervised.	✓		In scope - Applicable
4.4.1.6 (IAL2)	✓					63A#0270			The CSP SHALL validate and confirm the Applicant's address of record by relying only upon issuing source(s) or authoritative source(s).	✓	✓	In scope - Applicable
4.4.1.6 (IAL2)	✓					63A#0280			The CSP SHALL NOT accept un-validated self-asserted addresses.	✓	✓	In scope - Applicable
4.4.1.6 (IAL2)	✓					63A#0290			If the CSP performs Supervised (In-person or Remote) proofing it SHALL document the maximum validities it allows for enrollment codes and only issue codes that meet that limitation, which SHALL NOT exceed 7 days.	✓	✓	In scope - Applicable
4.4.1.6 (IAL2)						n/a			See 63A#0290			
4.4.1.6 (IAL2)	✓					63A#0300			If the CSP performs Unsupervised proofing it SHALL:	✓		In scope - Applicable
4.4.1.6 (IAL2)	✓					63A#0300	a)		send an enrollment code to a confirmed address of record for the Applicant;	✓		In scope - Applicable
4.4.1.6 (IAL2)	✓					63A#0300	b)		require the Applicant to present a valid enrollment code to complete the identity proofing process;	✓		In scope - Applicable
4.4.1.6 (IAL2)	✓					63A#0300	c)		If the enrollment code is also intended to be an authentication factor, reset the code upon first use;	✓		In scope - Not applicable The enrollment code is not used as an authenticator factor.
4.4.1.6 (IAL2)	✓					63A#0300	d)		document the maximum validities it allows for enrollment codes and only issue codes that meet the following limitations:	✓		In scope - Applicable
4.4.1.6 (IAL2)	✓					63A#0300	d)	i)	10 days, when sent to a postal address of record within the contiguous United States;	✓		In scope - Not applicable confirms email address of record, exclusively
4.4.1.6 (IAL2)	✓					63A#0300	d)	ii)	30 days, when sent to a postal address of record outside the contiguous United States;	✓		In scope - Not applicable confirms email address of record, exclusively
4.4.1.6 (IAL2)	✓					63A#0300	d)	iii)	10 minutes, when sent to a telephone number of record (SMS or voice);	✓		In scope - Not applicable confirms email address of record, exclusively
4.4.1.6 (IAL2)	✓					63A#0300	d)	iv)	24 hours, when sent to an email address of record.	✓		In scope - Applicable
4.4.1.6 (IAL2)	✓					63A#0300	e)		ensure that the enrollment code and notification of proofing are sent to different addresses of record.	✓		In scope - Applicable
4.4.1.8 (IAL2)	✓					63A#0310			The CSP SHALL employ appropriately-tailored security controls, to include control enhancements, from the moderate or high baseline of security controls, as defined in SP 800-53 or equivalent federal (e.g., FEDRAMP) or industry standards.	✓		In scope - Applicable
4.4.1.8 (IAL2)	✓					63A#0320			When fulfilling criterion 63A#0310 the CSP SHALL ensure that the minimum assurance-related controls for moderate-impact systems or equivalent are satisfied.	✓		In scope - Applicable
4.4.2	✓					63A#0330			CSPs SHALL identity-proof Trusted Referees according to the same criteria and, as a minimum, at the same IAL that are applied to normal Applicants on whose behalf they act.	✓	✓	In scope - Applicable
4.5.1 (IAL3)	✓					63A#0340			**The CSP SHALL limit collection of PII to the minimum necessary to validate and resolve the existence of the claimed identity uniquely in a given context, and to associate the claimed identity with the Applicant providing identity evidence for appropriate identity resolution, validation, and verification. (See 63A#0020)**		✓	**Not in scope** **This IAL not supported**
4.5.2 (IAL3)	✓					63A#0350			**The CSP SHALL collect from the Applicant at least the following strength of evidence, as determined by the further requirements in Table 5-1:**		✓	**Not in scope** **This IAL not supported**
4.5.2 (IAL3)	✓					63A#0350	a)		**Two pieces of SUPERIOR evidence; OR**		✓	**Not in scope** **This IAL not supported**
4.5.2 (IAL3)	✓					63A#0350	b)		**One piece of SUPERIOR evidence and one piece of STRONG evidence IF the STRONG evidence's issuing source, during its identity proofing event, confirmed the claimed identity by collecting two or more forms of SUPERIOR or STRONG evidence AND the CSP validates the evidence directly with the issuing source; OR**		✓	**Not in scope** **This IAL not supported**
4.5.2 (IAL3)	✓					63A#0350	c)		**Two pieces of STRONG evidence plus one piece of FAIR evidence.**		✓	**Not in scope** **This IAL not supported**
4.5.2 (IAL3)	✓					63A#0355			**Refer to Worksheet 63A_TS-1**		✓	**Not in scope** **This IAL not supported**

4.5.3 (IAL3)	✓				63A#0360			The CSP SHALL, at a minimum, validate identity evidence at the same strength as that at which the evidence was collected. (see 63A#0200 & #0210)			✓	Not in scope This IAL not supported
4.5.3 (IAL3)	✓				63A#0365			Refer to Worksheet 63A_TS-2			✓	Not in scope This IAL not supported
4.5.4 (IAL3)					n/a							
4.5.4 (IAL3)	✓				63A#0370			The CSP SHALL verify the Applicant's binding to the identity evidence by a process which demonstrates a strength of SUPERIOR. [Inc. ref to TS-3]			✓	Not in scope This IAL not supported
4.5.4 (IAL3)	✓				n/a			Superseded by 63A#0240				
4.5.5 (IAL3)	✓				63A#0380			The CSP SHALL perform all identity proofing using either Supervised (In-person) or Supervised (Remote)			✓	Not in scope This IAL not supported
4.5.6 (IAL3)	✓				63A#0390			The CSP SHALL confirm the Applicant's address of record using either:			✓	Not in scope This IAL not supported
4.5.6 (IAL3)	✓				63A#0390	a)		only information taken from any piece of valid identity evidence; or			✓	Not in scope This IAL not supported
4.5.6 (IAL3)	✓				63A#0390	b)		for information values which might reasonably be amended from time-to-time, information substituted by the Applicant which SHALL be validated with the issuing source of the information.			✓	Not in scope This IAL not supported
4.5.6 (IAL3)					n/a			Superseded by 63A#0280				
4.5.6 (IAL3)	✓				63A#0400			The CSP SHALL send a notification of proofing outcome to the confirmed address of record.			✓	Not in scope This IAL not supported
4.5.6 (IAL3)	✓				63A#0410			Superseded by 63A#0290				Not in scope This IAL not supported
4.5.7 (IAL3)	✓				63A#0420			The CSP SHALL collect and record a biometric sample at the time of proofing.			✓	Not in scope This IAL not supported
4.5.8 (IAL3)	✓				63A#0430			The CSP SHALL employ appropriately-tailored security controls, to include control enhancements, from the high baseline of security controls defined in SP 800-53 or equivalent federal (e.g., FEDRAMP) or industry standards. (see 63A#0310)			✓	Not in scope This IAL not supported
4.5.8 (IAL3)	✓				63A#0440			When fulfilling criterion 63A#0430 the CSP SHALL ensure that the minimum assurance-related controls for high-impact systems or equivalent are satisfied.			✓	Not in scope This IAL not supported
4.6	✓				63A#0450			The CSP SHALL only issue enrollment codes that are, minimally, a random six character alphanumeric sequence or other value of equivalent entropy, represented either as:	✓	✓		In scope - Applicable
4.6	✓				63A#0450	a)		a human-readable text string; OR	✓	✓		In scope - Applicable
4.6	✓				63A#0450	b)		A machine-readable optical label.	✓	✓		In scope - Applicable
5.2.1					n/a			Refer to Worksheet 63A_TS-1	✓	✓		
5.2.2					n/a			Refer to Worksheet 63A_TS-2	✓	✓		
5.3.1					n/a			Refer to Worksheet 63A_TS-3	✓	✓		
5.3.1	✓				63A#0460			If the CSP uses KBV to verify identities it SHALL observe the practices required by 63A#0470 and 63A#0480.	✓			In scope - Not applicable No KBV is deployed for -63 rev3 processes
5.3.2	✓				63A#0470			If the CSP uses KBV to verify identities it SHALL allow the Applicant the choice to opt-out of the KBV process and SHALL employ other means of equivalent rigour to achieve verification (in accordance with TS-3).	✓			In scope - Not applicable See 63A#0460
5.3.2	✓				63A#0480			The CSP SHALL verify an Applicant's identity against only a single piece of validated evidence, in accordance with the following restrictions:	✓			In scope - Not applicable See 63A#0460
5.3.2	✓				63A#0480	a)		information used to formulate KBQ/KBA SHALL be expected to be known only to the Applicant and the authoritative source;	✓			In scope - Not applicable See 63A#0460
5.3.2	✓				63A#0480	b)		KBQ/KBA SHALL be composed so as to ensure that the information transacted has at least 20 bits of entropy;	✓			In scope - Not applicable See 63A#0460
5.3.2	✓				63A#0480	c)		a minimum of four KBQ SHALL be presented and each question SHALL	✓			In scope - Not applicable See 63A#0460
5.3.2	✓				63A#0480	c)	i)	have a minimum of four possible answers of which only one SHALL be correct; OR	✓			In scope - Not applicable See 63A#0460
5.3.2	✓				63A#0480	c)	ii)	require responses which are not based on a selection from a pre-determined list.	✓			In scope - Not applicable See 63A#0460
5.3.2	✓				63A#0480	d)		a maximum of three attempts to answer each question SHALL be permitted;	✓			In scope - Not applicable See 63A#0460
5.3.2	✓				63A#0480	e)		the KBV session SHALL terminate if no attempt has been made to submit a response to a question within 2 minutes;	✓			In scope - Not applicable See 63A#0460
5.3.2	✓				63A#0480	f)		termination of a session SHALL require a complete re-start of the KBV process;	✓			In scope - Not applicable See 63A#0460
5.3.2	✓				63A#0480	g)		the presence of 'diversionary' questions in the set of possible responses SHALL be minimised;	✓			In scope - Not applicable See 63A#0460
5.3.2	✓				63A#0480	h)		no question SHALL provide the Applicant the opportunity to infer answers to any other KBQs in any subsequent session;	✓			In scope - Not applicable See 63A#0460
5.3.2	✓				63A#0480	i)		no question SHALL offer the Applicant the opportunity to infer answers to any other KBQs;	✓			In scope - Not applicable See 63A#0460
5.3.2	✓				63A#0480	j)		KBQ/KBA SHALL be composed) dynamically and NOT use KBQ for which the answer is in any way static.	✓			In scope - Not applicable See 63A#0460
5.3.3												

5.3.3.1	✓				63A#0490			If the CSP provides Supervised (In-person) proofing it SHALL document and apply technologies and procedures which ensure that the Proofing Supervisor reviews the biometric source (e.g., fingers, face) for presence of non-natural materials and perform such inspections as part of the proofing process.	✓	✓	In scope - Applicable
5.3.3.1	✓				63A#0500			If the CSP provides Supervised (In-person) proofing it SHALL document and apply technologies and procedures such that the Proofing Supervisor SHALL ensure that biometric samples are taken from the Applicant themselves and not from another person.	✓	✓	In scope - Applicable
5.3.3.1	✓				63A#0510			If the CSP provides Supervised (In-person) proofing it SHALL ensure that the technologies and procedures applied by the Proofing Supervisor fulfill the biometric performance requirements expressed in 63A#0620 to 63A#0680 inclusive.	✓	✓	In scope - Applicable
5.3.3.2	✓				63A#0520			The CSP SHALL supervise the entirety of a Remote proofing session, from which the Applicant SHALL NOT depart.	✓	✓	In scope - Applicable
5.3.3.2	✓				63A#0530			The CSP SHALL ensure that a live operator participates with the Applicant for the entirety of a Remote identity proofing session.	✓	✓	In scope - Applicable
5.3.3.2	✓				63A#0540			The CSP SHALL ensure that a live operator clearly witnesses all actions taken by the Applicant, for the entirety of a Remote identity proofing session.	✓	✓	In scope - Applicable
5.3.3.2	✓				63A#0550			The CSP SHALL ensure that all digital verification of evidence is performed by scanners and sensors which are integrated into the CSP-owned/managed Remote proofing terminal.	✓	✓	In scope - Applicable
5.3.3.2	✓				63A#0560			The CSP SHALL train its live operators such that they:	✓	✓	In scope - Applicable
5.3.3.2	✓				63A#0560	a)		are competent to detect potential fraud; and	✓	✓	In scope - Applicable
5.3.3.2	✓				63A#0560	b)		are capable of properly performing a virtual in-process proofing session.	✓	✓	In scope - Applicable
5.3.3.2	✓				63A#0570			The CSP SHALL employ physical tamper detection and resistance features at its Remote proofing terminal appropriate for the environment in which it is located.	✓	✓	In scope - Not applicable. No physical terminal used
5.3.3.2	✓				63A#0580			The CSP SHALL ensure that all communications between the live operator and the remote proofing terminal occur over mutually authenticated protected channels.	✓	✓	In scope - Not applicable. No physical terminal used
5.3.4	✓				63A#0590			The CSP SHALL include in its CP the following:	✓	✓	In scope - Applicable
5.3.4	✓				63A#0590	a)		how a Trusted Referee is determined;	✓	✓	In scope - Applicable
5.3.4	✓				63A#0590	b)		the lifecycle by which the Trusted Referee retains their status as a valid referee;	✓	✓	In scope - Applicable
5.3.4	✓				63A#0590	c)		any restrictions, as well as any revocation and suspension requirements, which are applicable to Trusted Referees;	✓	✓	In scope - Applicable
5.3.4					n/a			See 63A#0330			
5.3.4	✓				63A#0600	d)		the minimum evidence required to bind the relationship between the Trusted Referee and the Applicant.	✓	✓	In scope - Applicable
5.3.4.1					n/a			See 63A#0610			
5.3.4.1	✓				63A#0610			The CSP SHALL document and apply policies and practices which show that it identifies and complies with all applicable laws and regulations, concerning interacting with minors unable to meet the evidence requirements of identity proofing .	✓	✓	In scope - Applicable
5.3.4.1	✓							See 63A#0610			
End of 63A criteria					**End of 63A criteria**						
					Referenced 63B_SAC criteria - NOTE - the following criteria are required to be met in the context of 63A#0510 and evidence for						
5.2.3	✓				63A#0620			The CSP shall implement biometric systems which have at least the following characteristics:	✓	✓	In scope - Applicable
5.2.3	✓				63A#0620	a)		operate with an FMR [ISO/IEC 2382-37] of 1 in 1000 or better;	✓	✓	In scope - Applicable
5.2.3	✓				63A#0620	b)		achieved that FMR operation under conditions of a conformant attack (i.e., zero-effort impostor attempt) in accordance with ISO/IEC 30107-1.	✓	✓	In scope - Applicable
5.2.3	✓				63A#0630			If Presentation Attack Detection is implemented the CSP SHALL perform testing of presentation attack resistance in accordance with §12 of ISO/IEC 30107-3.	✓	✓	In scope - Applicable
5.2.3	✓				63A#0640				✓	✓	In scope - Applicable
5.2.3	✓				63A#0640	a)		where analysis has shown at least 90% resistance to presentation attacks for each relevant attack type (i.e., species), where resistance is defined as the number of thwarted presentation attacks divided by the number of trial presentation attacks, THEN up to 10 consecutive failed authentication attempts can occur; OTHERWISE	✓	✓	In scope - Not Applicable ID.me does not use biometrics as an authenticator
5.2.3	✓				63A#0640	b)		no more than 5 consecutive failed authentication attempts can occur.	✓	✓	In scope - Applicable
5.2.3	✓				63A#0650			If either limit set in 63A#0640 is reached the CSP SHALL:	✓	✓	In scope - Applicable
5.2.3	✓				63A#0650	a)		disable the biometric user authentication, and if an alternative authentication factor is already available use that other factor; OR OTHERWISE	✓	✓	In scope - Applicable
5.2.3	✓				63A#0650	b)		impose a delay of at least 30 seconds before the next attempt, increasing exponentially with each successive attempt.	✓	✓	In scope - Applicable
5.2.3	✓				63A#0660			No stipulation - not applicable to identity proofing.	✓	✓	In scope - Applicable
5.2.3	✓				63A#0670			If biometric comparisom is performed centrally rather than locally the CSP SHALL:	✓	✓	In scope - Applicable
5.2.3	✓				63A#0670	a)		limit use of the biometric as an authentication factor to one or more specific devices that are authenticated using approved cryptography;	✓	✓	In scope - Applicable
5.2.3	✓				63A#0670	b)		use a separate key to identify the device;	✓	✓	In scope - Applicable
5.2.3	✓				63A#0670	c)		Implement biometric revocation (a.k.a. biometric template protection); Note - this is for both revocation of the credential as much as for privacy protection	✓	✓	In scope - Applicable
5.2.3	✓				63A#0670	d)		transmit all biometric data over an authenticated protected channel.	✓	✓	In scope - Applicable
5.2.3	✓				63A#0680			The CSP SHALL zeroize the biometric sample (including any associated biometric data) immediately after any training or research data has been derived.	✓	✓	In scope - Not applicable ID.me does not store the biometric template
					End of 'referenced' 63B criteria						