KIAF-1	Applies to:				THESE CRITERIA SHOULD NOT BE APPLIED WITHOUT A THOROUGH UNDERSTANDING OF KANTARA DOCUMENT 'Kantara IAF-1405 Service Assessment Criteria - Overview'				AAL		CRITERION APPLICABILITY (SoCA)
§	CSP	RP	FA	US Fed Agcy	63B tag	index		KI_criterion (text in red is new this version)	2	3	
4					n/a						
4	✓				63B#0010			The CSP SHALL authenticate a Claimant at at least the ~~same~~ requested AAL.	✓	✓	In scope - Applicable
4	✓				63B#0020			The CSP SHALL ensure that, for a given Subject and authenticator, the result of a successful authentication results in a consistent identifier.	✓	✓	In scope - Applicable
4					n/a						
4					n/a						
					n/a						
4					n/a						
4				✓	63B#0030			Agencies SHALL require a minimum of AAL2 when self-asserted PII or other personal information is made available to the Subject online.	✓	✓	In scope - Applicable
4,1											
4.2 (AAL2)											
4.2(AAL2	✓				63B#0040			The CSP SHALL use secure authentication protocol(s) to prove that the Claimant has both possession and control over two distinct authentication factors.	✓	✓	In scope - Applicable

4.2.1(AA	✓				63B#0050			*The CSP SHALL perform authentication using EITHER a multi-factor authenticator OR a combination of two single-factor authenticators.*	✓		In scope - Applicable
4.2.1(AA	✓				63B#0060			*When a multi-factor authenticator is used,the CSP SHALL employ any one of the following:*	✓		**In scope - Not applicable ID.me does not support multi-factor authenticators**
4.2.1 (AAL2)	✓				63B#0060	a)		*Multi-Factor OTP Device;*	✓		In scope - Applicable
4.2.1 (AAL2)	✓				63B#0060	b)		*Multi-Factor Cryptographic Software;*	✓		In scope - Applicable
4.2.1 (AAL2)	✓				63B#0060	c)		*Multi-Factor Cryptographic Device.*	✓		In scope - Applicable
4.2.1(AA	✓				63B#0070			*When a combination of two single-factor authenticators is used, the CSP SHALL employ a Memorized Secret authenticator plus one of the following possession-based authenticators:*	✓		In scope - Applicable
4.2.1(AA	✓				63B#0070	a)		*Look-Up Secret;*	✓		**In scope - Not applicable ID.me does not use look-up secrets**
4.2.1(AA	✓				63B#0070	b)		*Out-of-Band Device;*	✓		In scope - Applicable
4.2.1(AA	✓				63B#0070	c)		*Single-Factor OTP Device;*	✓		In scope - Applicable
4.2.1(AA	✓				63B#0070	d)		*Single-Factor Cryptographic Software;*	✓		In scope - Applicable
4.2.1(AA	✓				63B#0070	e)		*Single-Factor Cryptographic Device.*	✓		In scope - Applicable
4.2.2(AA	✓				63B#0080			*The CSP SHALL ensure that all cryptographic authenticators employ cryptographic techniques approved by a Federal or industry body.*	✓		In scope - Applicable
4.2.2(AAL2)				✓	63B#0090			*Federal agencies SHALL only procure authenticators which have been validated as meeting FIPS 140 Level 1 or higher.*	✓		**Not in scope**

4.2.2(AAL2)					*n/a*						
4.2.2(AA	✓				*63B#0100*			*The CSP SHALL ensure that at least one authenticator used is replay resistant.*	✓	✓	In scope - Applicable
4.2.2(AAL2)					*n/a*						
4.2.2(AA	✓				*63B#0110*			*The CSP SHALL use only mutually-authenticated protected channels when communicating with Claimants*	✓	✓	In scope - Applicable
4.2.2(AAL2)				✓	*63B#0120*			*Federal agencies SHALL only operate verifiers which have been validated as meeting FIPS 140 Level 1 or higher.*	✓		In scope - Applicable
4.2.2(AA	✓				*63B#0130*			*The CSP SHALL NOT consider the unlocking of a device used in the authentication process to be an authentication factor.*	✓	✓	In scope - Applicable
4.2.2(AAL2)					*n/a*						

4.2.2(AA	✓				*63B#0140*			*If a biometric factor is used in an authentication the CSP SHALL ensure that all criteria 63B#1470 to 63B#1550 are fulfilled.*	✓		**In scope - Not applicable** This happens on the user's device and is beyond the scope of ID.me's ability to manage and control. ID.me's service embodies no biometric functionality and no biometric data is handled by the service.
4.2.2(AAL2)					*n/a*						
4.2.3(AAL2)					*n/a*			*Addressed by 63B#0150*			
4.2.3(AAL2)					*n/a*						
4.2.3(AAL2)					*n/a*						
4.2.3(AA	✓	✓			*63B#0150*			*The RP SHALL terminate a session and the life of the current session secret whenever they are unable to receive affirmative re-authentication of the Subject, either:*	✓		**Not in scope The IDIG does not manage its RPs' sessions**
4.2.3(AA	✓	✓			*63B#0150*	*a)*		*a) prior to a period of session inactivity reaching 30 minutes; OR*	✓		**Not in scope The IDIG does not manage its RPs' sessions**
4.2.3(AA	✓	✓			*63B#0150*	*b)*		*b) prior to an extended usage session reaching 12 hours since the last successful re-authentication, regardless of user activity.*	✓		**Not in scope The IDIG does not manage its RPs' sessions**

4.2.3(AAL2)					n/a			*Addressed by 63B#0150*			
4.2.4(AA	✓				*63B#0160*			*The CSP SHALL employ appropriately-tailored moderate baseline security controls, as defined in SP 800-53 or equivalent Federal or industry standards.*	✓		In scope - Applicable
4.2.4(AA	✓				*63B#0170*			*When fulfilling criterion 63A#0210 the CSP SHALL ensure that minimum assurance-related control needs for moderate-impact systems or equivalent are satisfied.*	✓		In scope - Applicable
4.2.5(AA	✓				*63B#0180*			*The CSP SHALL document, periodically review and comply with, a data retention schedule, accounting for:*	✓	✓	In scope - Applicable
4.2.5(AA	✓				*63B#0180*	*a)*		*results of a privacy and security risk assessment;*	✓	✓	In scope - Applicable
4.2.5(AA	✓				*63B#0180*	*b)*		*applicable laws, regulations, policies, and specific record retention schedules;*	✓	✓	In scope - Applicable
4.2.5(AA	✓				*63B#0180*	*c)*		*its own records retention policy.*	✓	✓	In scope - Applicable
4.2.5(AAL2)					*n/a*			See 63B#0180			
4.2.5(AA	✓				*63B#0190*			*The CSP SHALL publish to Subjects its data retention schedule, to the extent appropriate to the context.*	✓	✓	In scope - Applicable
4.3 (AAL3)	✓				*63B#0200*			***The CSP SHALL ensure that at least one authenticator used is hardware-based.***		✓	***Not in scope This AAL not supported***
4.3 (AAL3)	✓				*63B#0210*			***The CSP SHALL ensure that at least one authenticator used is verifier-impersonation resistant.***		✓	***Not in scope This AAL not supported***

4.3 (AAL3)					n/a			Addressed by 63B#0040			
4.3 (AAL3)	✓				*63B#0220*			***The CSP SHALL ensure that all authenticators employ hardware cryptographic techniques approved by a Federal or industry body.***		✓	***Not in scope This AAL not supported***
4.3.1 (AAL3)	✓				*63B#0230*			***The CSP SHALL perform authentication using EITHER***		✓	***Not in scope This AAL not supported***
4.3.1 (AAL3)	✓				*63B#0230*	*a)*		*a Multi-Factor Cryptographic Device*		✓	***Not in scope This AAL not supported***
4.3.1 (AAL3)	✓				*63B#0230*	*b)*		***OR one of the following combinations of authenticators***		✓	***Not in scope This AAL not supported***
4.3.1 (AAL3)	✓				*63B#0230*	*b)*	*i)*	*Single-Factor Cryptographic Device and a Memorized Secret;*		✓	***Not in scope This AAL not supported***
4.3.1 (AAL3)	✓				*63B#0230*	*b)*	*ii)*	***Single-Factor Cryptographic Device and a Multi-Factor OTP device (software or hardware);***		✓	***Not in scope This AAL not supported***
4.3.1 (AAL3)	✓				*63B#0230*	*b)*	*iii)*	***Multi-Factor OTP Device (hardware only) and a Single-Factor Cryptographic Software;***		✓	***Not in scope This AAL not supported***
4.3.1 (AAL3)	✓				*63B#0230*	*b)*	*iv)*	***Single-Factor OTP Device (hardware only) and a Multi-Factor Cryptographic Software Authenticator;***		✓	***Not in scope This AAL not supported***
4.3.1 (AAL3)	✓				*63B#0230*	*b)*	*v)*	***Single-Factor OTP Device (hardware only) and a Single-Factor Cryptographic Software Authenticator, and a Memorized Secret.***		✓	***Not in scope This AAL not supported***

4.3.2 (AAL3)					n/a			*Addressed by 63B#0110*				
4.3.2 (AAL3)	✓				*63B#0240*			***The CSP SHALL ensure that all authenticators used are verifier impersonation resistant.***		✓	***Not in scope This AAL not supported***
4.3.2 (AAL3)					n/a			*Addressed by 63B#0110*				
4.3.2 (AAL3)	✓				*63B#0250*			***The CSP SHALL ensure that each authentication and re-authentication instance demonstrates authentication intent from at least one authenticator.***		✓	***Not in scope This AAL not supported***
4.3.2 (AAL3)	✓				*63B#0260*			***The CSP SHALL require multi-factor hardware cryptographic module authenticator which are validated at FIPS 140 Level 2 or higher overall with at least FIPS 140 Level 3 physical security.***		✓	***Not in scope This AAL not supported***
4.3.2 (AAL3)	✓				*63B#0270*			***The CSP SHALL require single-factor hardware cryptographic module authenticator which are validated at FIPS 140 Level 1 or higher with at least FIPS 140 Level 3 physical security.***		✓	***Not in scope This AAL not supported***
4.3.2 (AAL3)	✓				*63B#0280*			***The CSP SHALL only use verifiers which have been validated at FIPS 140 Level 1 or higher***		✓	***Not in scope This AAL not supported***
4.3.2 (AAL3)	✓				*63B#0290*			***The CSP SHALL ensure that verifiers are verifier compromise resistant with respect to at least one authentication factor in accordance with 63B#1630 & '1640.***		✓	***Not in scope This AAL not supported***
4.3.2 (AAL3)	✓				*63B#0300*			***The CSP SHALL include in its risk assessment an evaluation as to which side-channel attacks are relevant.***		✓	***Not in scope This AAL not supported***

4.3.2 (AAL3)	✓				*63B#0305*			***The CSP SHALL NOT consider the unlocking of a smartphone to be an authentication factor.***		✓	***Not in scope This AAL not supported***
4.3.2 (AAL3)					n/a						
4.3.2 (AAL3)	✓				*63B#0310*			*If a biometric factor is used in an authentication the CSP SHALL ensure that the biometric sensor **and subsequent processing** meet the performance requirements stated in 63B#1470 - '#1550 inc.*		✓	***Not in scope This AAL not supported***
4.3.3 (AAL3)	✓	✓			*63B#0320*			*The RP SHALL terminate a session and the life of the current session secret whenever they are unable to receive affirmative re-authentication of the Subject, either:*		✓	***Not in scope This AAL not supported***
4.3.3 (AAL3)	✓	✓			*63B#0320*	*a)*		*prior to a period of session inactivity reaching **15** minutes; OR*		✓	***Not in scope This AAL not supported***
4.3.3 (AAL3)	✓	✓			*63B#0320*	*b)*		*b) prior to a session reaching **12** hours since the last successful re-authentication, regardless of user activity.*		✓	***Not in scope This AAL not supported***
4.3.3 (AAL3)	✓	✓			n/a			*Addressed by 63B#4343*			
4.3.3 (AAL3)	✓				*63B#0320*			***When re-authenticating, the CSP SHALL require the user to prove possession of both authentication factors***		✓	***Not in scope This AAL not supported***

4.3.4 (AAL3)	✓				*63B#0330*			*The CSP SHALL employ appropriately-tailored **high** baseline security controls defined in SP 800-53 or equivalent Federal or industry standards.*		✓	***Not in scope*** ***This AAL not supported***
4.3.4 (AAL3)	✓				*63B#0340*			*When fulfilling criterion 63A#3200 the CSP SHALL ensure that its system satisfies the minimum assurance-related control requirements for **high**-impact systems or equivalent.*		✓	***Not in scope*** ***This AAL not supported***
4.3.5 (AAL3)					n/a			*Addressed by 63B#0220*			
4.3.5 (AAL3)					n/a			Covered by 63B#0220 a)			
4.3.5 (AAL3)					n/a			Covered by 63B#0230			
4,4	✓				*63B#0350*			*The CSP SHALL employ appropriately-tailored privacy controls, to include control enhancements (appropriate for the AAL being souight - refer to 63B#0210 and '#3200) as defined in SP 800-53 or equivalent Federal or industry standards.*	✓	✓	In scope - Applicable
4,4	✓				*63B#0360*			*Unless the Subject has agreed to additional use of their PII, the CSP SHALL NOT use or disclose Subjects' PII for any purpose other than conducting authentication, related fraud mitigation, or to comply with law or legal process.*	✓	✓	In scope - Applicable
4,4	✓				*63B#0370*			*The CSP SHALL provide clear notice and obtain the Subject's consent for any additional uses of their PII, prior to making any such use.*	✓	✓	In scope - Applicable

4,4	✓				*63B#0380*			*The CSP SHALL NOT make consent a condition of the service.*	✓	✓	In scope - Applicable
4,4	✓				*63B#0390*			*The CSP SHALL ensure that use of PII is limited to the purposes for which it was collected, as stated in the Terms of Service / Privacy Policy (see 63A#0030) / CrP (see 63A#0100).*	✓	✓	In scope - Applicable
4,4					*n/a*						
4,4					*n/a*						
4,4				✓	*63B#0400*			Federal Agencies SHALL:	✓	✓	**Not in scope** **Strictly a reqt on Fed agencies**
4,4				✓	*63B#0400*	*a)*		*in consultation with the Agency's Senior Agency Official for Privacy, conduct an analysis determining whether the requirements of the Privacy Act are triggered, according to the agency's CSP and/or RP role(s).*	✓	✓	**Not in scope** **Strictly a reqt on Fed agencies**

4,4				✓	*63B#0400*	*b)*		*according to the outcome of the analysis in a) above, publish or identify coverage by a System of Records Notice, as applicable;*	✓	✓	**Not in scope Strictly a reqt on Fed agencies**
4,4				✓	*63B#0400*	*c)*		*in consultation with the Agency's Senior Agency Official for Privacy, conduct an analysis determining whether the requirements of the E-Government Act are triggered, according to the agency's CSP and/or RP role(s);*	✓	✓	**Not in scope Strictly a reqt on Fed agencies**
4,4				✓	*63B#0400*	*d)*		*according to the outcome of the analysis in c) above, publish or identify coverage by a Privacy Impact Assessment, as applicable.*	✓	✓	**Not in scope Strictly a reqt on Fed agencies**
5					*n/a*						
5,1					*n/a*						
5.1.1.1	✓				*63B#0410*			*The CSP SHALL require memorized secrets chosen by the Subject to be at least 8 characters in length.*	✓	✓	In scope - Applicable
5.1.1.1	✓				*63B#0420*			*The CSP SHALL require memorized secrets generated by itself or a Verifier to be at least 6 characters in length and randomly-generated.*	✓	✓	In scope - Applicable
5.1.1.1	✓				*63B#0430*			*If the CSP [or Verifier] determines that a chosen memorized secret appears on a list of compromised values it SHALL require the Subject to choose a different memorized secret.*	✓	✓	In scope - Applicable
5.1.1.1					*n/a*						
5.1.1.2	✓				*63B#0440*			*The CSP SHALL require memorized secrets chosen by the Subject to be at least 8 characters in length.*	✓	✓	In scope - Applicable
5.1.1.2					*n/a*						

5.1.1.2					*n/a*						
5.1.1.2	✓				*63B#0450*			*The CSP SHALL NOT truncate Subject-chosen memorized secrets*	✓	✓	In scope - Applicable
5.1.1.2	✓				*63B#0460*			*If Unicode is accepted then the CSP SHALL count each Unicode code point as a single character.*	✓	✓	In scope - Applicable
5.1.1.2					*n/a*						
5.1.1.2					*n/a*						
5.1.1.2					*n/a*						

5.1.1.2	✓				*63B#0470*			*The CSP SHALL require memorized secrets generated by itself or a Verifier to be at least 6 characters in length and randomly-generated using an approved random-bit generator [SP 800-90Ar1].*	✓	✓	**In scope - Not Applicable ID.me does not generate secrets. Subject selects own password**
5.1.1.2	✓				*63B#0480*			*The CSP SHALL NOT permit Subjects to store password-recollection hints.*	✓	✓	In scope - Applicable
5.1.1.2	✓				*63B#0490*			*The CSP SHALL NOT prompt Subjects in any manner when Subjects are choosing secrets*	✓	✓	In scope - Applicable
5.1.1.2	✓				*63B#0500*			*The CSP SHALL compare Subjects' chosen secrets against a list that contains values known to be commonly-used, expected, or compromised and if found:*	✓	✓	In scope - Applicable
5.1.1.2					n/a						
5.1.1.2					n/a			*Addressed by 63B#0380*			

5.1.1.2	✓				*63B#0500*	*a)*		*provide the reason for rejection;*	✓	✓	In scope - Applicable
5.1.1.2	✓				*63B#0500*	*b)*		*require the Subject to choose another secret.*	✓	✓	In scope - Applicable
5.1.1.2					n/a						
5.1.1.2					n/a						
5.1.1.2	✓				*63B#0510*			*The Verifier SHALL implement a rate-limiting mechanism which:*	✓	✓	In scope - Applicable
5.1.1.2	✓				*63B#0510*	*a)*		*protects against online guessing attacks;*	✓	✓	In scope - Applicable
5.1.1.2	✓				*63B#0510*	*b)*		*limits consecutive failed authentication attempts on a single account to no more than 100.*	✓	✓	In scope - Applicable
5.1.1.2					*n/a*						
5.1.1.2	✓				*63B#0520*			*IF there is evidence of compromise of the Claimant's authenticator the CSP SHALL require the Claimant to select a new memorized secret, consistent with 63B#0440 - '0500.*	✓	✓	In scope - Applicable

5.1.1.2					*n/a*						
5.1.1.2					*n/a*						
5.1.1.2					*n/a*						
5.1.1.2	✓				*63B#0530*			*The CSP SHALL use approved encryption and an authenticated protected channel when requesting memorized secrets.*	✓	✓	In scope - Applicable
5.1.1.2	✓				*63B#0540*			*The CSP SHALL store memorized secrets in a form that is resistant to offline attacks.*	✓	✓	In scope - Applicable
5.1.1.2	✓				*63B#0550*			*The CSP SHALL salt and hash stored memorized secrets using an approved algorithm, ensuring that:*	✓	✓	In scope - Applicable
5.1.1.2	✓				*63B#0550*	*a)*		*a randomly-chosen salt value of at least 32 bits in length is used;*	✓	✓	In scope - Applicable

5.1.1.2	✓				*63B#0550*	*b)*		*both the salt value and the resulting hash are stored for each subscriber using a memorized secret authenticator;*	✓	✓	In scope - Applicable
5.1.1.2	✓				*63B#0560*			*The CSP SHALL generate salt values using an approved random-bit generator [SP 800-90Ar1] which provides at least the minimum security strength specified in the latest revision of SP 800-131A.*	✓	✓	In scope - Applicable
5.1.1.2	✓				*63B#0570*			*The CSP SHALL store secret salt value(s) separately from the hashed memorized secrets.*	✓	✓	In scope - Applicable
5.1.1.2					n/a						
5.1.1.2	✓				*63B#0570*			*The CSP SHALL use only approved one-way key derivation functions.*	✓	✓	In scope - Applicable
5.1.1.2					n/a						

5.1.1.2					n/a						
5.1.1.2					n/a						
5.1.1.2					n/a						
5.1.1.2					n/a						
5.1.1.2					n/a						
5.1.1.2					*n/a*						
5.1.1.2					*n/a*						
5.1.1.2					*n/a*						
5.1.1.2					*n/a*						
5.1.1.2					*n/a*						
5.1.2	✓				*63B#0580*			*The CSP SHALL create lists of look-up secret authenticators using an approved random-bit generator [SP 800-90Ar1] which creates secrets having at least 20 bits of entropy;*	✓	✓	**In scope - Not applicable ID.me does not support look-up secrets**

5.1.2	✓				*63B#0590*			*The CSP SHALL securely deliver the authenticator to the Subject.*	✓	✓	**In scope - Not applicable ID.me does not support look-up secrets**
5.1.2					*n/a*			*Addressed within 63B#0580*			
5.1.2.1					*n/a*						
5.1.2.1	✓				*63B#0600*			*IF the CSP distributes lists of look-up secret authenticators it SHALL do so using a secure channel which meets the criteria defined in 63B#1400.*	✓	✓	**In scope - Not applicable ID.me does not support look-up secrets**
5.1.2.1					*n/a*						
5.1.2.2	✓				*63B#0610*			*The CSP SHALL prompt the Claimant for the next secret from their authenticator or for a specific (e.g., numbered) secret.*	✓	✓	**In scope - Not applicable ID.me does not support look-up secrets**
5.1.2.2	✓				*63B#0620*			*The CSP SHALL succesfully use a secret from an authenticator list only once.*	✓	✓	**In scope - Not applicable ID.me does not support look-up secrets**
5.1.2.2	✓				*63B#0630*			*IF a look-up secret is derived from a grid card, the CSP SHALL use each cell of the grid only once.*	✓	✓	**In scope - Not applicable ID.me does not support look-up secrets**
5.1.2.2	✓				*63B#0640*			*The CSP SHALL store look-up secrets in a form that is resistant to offline attacks.*	✓	✓	**In scope - Not applicable ID.me does not support look-up secrets**

5.1.2.2	✓				*63B#0650*			*IF a look-up secret has at least 112 bits of entropy the CSP SHALL hash the secret iaw 63B#0550*	✓	✓	**In scope - Not applicable ID.me does not support look-up secrets**
5.1.2.2	✓				*63B#0660*			*IF a look-up secret has fewer than 112 bits of entropy the CSP SHALL hash the secret iaw 63B#0550*	✓	✓	**In scope - Not applicable ID.me does not support look-up secrets**
5.1.2.2	✓				*63B#0670*			*The CSP SHALL use an arbitrarily-chosen salt value of at least 32 bits length.*	✓	✓	In scope - Applicable
5.1.2.2	✓				*63B#0680*			*The CSP SHALL, for each look-up secret, store the salt value and the resulting hash.*	✓	✓	In scope - Applicable
5.1.2.2	✓				*63B#0690*			*IF a look-up secret has fewer than 64 bits of entropy the CSP SHALL enforce a rate-limiting mechanism iaw 63B#0510*	✓	✓	In scope - Applicable
5.1.2.2	✓				*63B#0700*			*The CSP SHALL use approved encryption and an authenticated protected channel when requesting look-up secrets.*	✓	✓	In scope - Applicable
5.1.3					*n/a*						
5.1.3.1	✓				*63B#0710*			*The CSP SHALL establish a separate channel with the Claimant's OOB authenticator in order to retrieve out-of-band secrets or authentication requests.*	✓	✓	In scope - Applicable

5.1.3.1					*n/a*						
5.1.3.1					*n/a*						
5.1.3.1	✓				*63B#0720*			*When performing out-of-band authentication the CSP SHALL use an authentication method which positively establishes the Claimant's possession of a specific device.*	✓	✓	In scope - Applicable
5.1.3.1	✓				*63B#0730*			*The CSP SHALL ensure that the Claimant's authentictor is positively authenticated by one of the following ways:*	✓	✓	In scope - Applicable
5.1.3.1	✓				*63B#0730*	*a)*		*establishing an authenticated protected channel using approved cryptography whilst ensuring that the key used is stored in suitably secure storage available to the authenticator application;*	✓	✓	**In scope - Not Applicable ID.me does not leverage key-based out-of-band secrets. ID.me sends a 6-digit code to the Claimant iaw 63B#0510**
5.1.3.1	✓				*63B#0730*	*b)*		*Authenticating via a public mobile telephone network using a SIM card or equivalent that uniquely identifies the device, whilst ensuring that the secret is sent to the out-of-band device via the PSTN.*	✓	✓	In scope - Applicable
5.1.3.1					*n/a*						

5.1.3.1					*n/a*						
5.1.3.1	✓				*63B#0740*			*The CSP SHALL ensure that if the out-of-band authenticator sends an approval message over the secondary communication channel one of the following is done:*	✓	✓	**In scope - Not applicable the ID.me web app requires that the claimant transfers a secret send via SMS as an OOB/secondary channel to the primary communication channel**
5.1.3.1	✓				*63B#0740*	*a)*		*the OOB Authenticator accepts transfer of the secret from the primary channel which it sends to the CSP over the secondary channel to associate the approval with the authentication transactio; OR*	✓	✓	**In scope - Not applicable the ID.me web app requires that the claimant transfers a secret send via SMS as an OOB/secondary channel to the primary communication channel**
5.1.3.1	✓				*63B#0740*	*b)*		*the OOB Authenticator accepts transfer of the secret from the primary channel which it sends to the CSP over the secondary channel to associate the approval with the authentication transaction and then:*	✓	✓	**In scope - Not applicable the ID.me web app requires that the claimant transfers a secret send via SMS as an OOB/secondary channel to the primary communication channel**
5.1.3.1	✓				*63B#0740*	*b)*	*i)*	*the OOB Authenticator accepts a 'yes/no' response from the Claimant;*	✓	✓	**In scope - Not applicable the ID.me web app requires that the claimant transfers a secret send via SMS as an OOB/secondary channel to the primary communication channel**

5.1.3.1	✓				*63B#0740*	*b)*	*ii)*	*the OOB Authenticator sends that response to the CSP*	✓	✓	**In scope - Not applicable the ID.me web app requires that the claimant transfers a secret send via SMS as an OOB/secondary channel to the primary communication channel**
5.1.3.2					*n/a*						
5.1.3.2					*n/a*						
5.1.3.2	✓				*63B#0750*			*The CSP SHALL use a verification method to securely and uniquely identify the Claimant's authenticator without storing the actual identifying key.*	✓	✓	In scope - Applicable
5.1.3.2	✓				*63B#0760*			*The CSP SHALL, according to the type of OOB authenticator used, effect one of the following three options:.*	✓	✓	**In scope - Not applicable** the ID.me web app requires that the claimant transfers a secret sent via SMS as an OOB/secondary channel to the primary communication channel

5.1.3.2	✓				*63B#0760*	*a)*		*Transferring the secret to the primary channel; OR*			**In scope - Not applicable** the ID.me web app requires that the claimant transfers a secret sent via SMS as an OOB/secondary channel to the primary communication channel
5.1.3.2	✓				*63B#0760*	*b)*		*transferring the secret via the secondary channel by transmitting a random authentication secret to the Claimant via the primary channel and then waiting for the secret to be returned from the Claimant's OOB authenticator via the secondary channel; OR*	✓	✓	**In scope - Not applicable** the ID.me web app requires that the claimant transfers a secret sent via SMS as an OOB/secondary channel to the primary communication channel
5.1.3.2	✓				*63B#0760*	*c)*		*requiring the Claimant to verify the secret by sending a random authentication secret to the claimant via the primary channel, and also to their OOB authenticator via the secondary channel and then waiting for an approval (or disapproval) message via the secondary channel*	✓	✓	**In scope - Not applicable** the ID.me web app requires that the claimant transfers a secret sent via SMS as an OOB/secondary channel to the primary communication channel
5.1.3.2	✓				*63B#0770*			*The CSP SHALL time-out and fail the authentication process if no response is received within 10 minutes of its initiation*	✓	✓	In scope - Applicable
5.1.3.2	✓				*63B#0780*			*The CSP SHALL accept a given authentication secret only once during its validity period.*	✓	✓	In scope - Applicable
5.1.3.2	✓				*63B#0790*			*The CSP SHALL create lists of look-up secret authenticators using an approved random bit generator [SP 800-90Ar1] which creates secrets having at least 20 bits of entropy;*	✓	✓	**In scope - Not applicable** ID.me does not support look-up secrets

5.1.3.2	✓				*63B#0800*			*IF an authentication secret has fewer than 64 bits of entropy the CSP SHALL enforce a rate-limiting mechanism iaw 63B#0510*	✓	✓	In scope - Applicable
5.1.3.3					*n/a*						
5.1.3.3	✓				*63B#0810*			*The CSP shall determine that a pre-registered 'phone number is registered to a specific physical device before using that device in OOB verification attempts.*	✓	✓	In scope - Applicable
5.1.3.3	✓				*63B#0820*			*IF the CSP allows the Subject to register a new 'phone number as an authenticator it shall do so in a manner which fulfills the criteria in 63B#1800 &'1810.*	✓	✓	In scope - Applicable
5.1.3.3					*n/a*						
	✓				*63B#0830*			*The CSP SHALL use SF-OTP Devices whose secret key and associated algorithm provide at least the minimum security strength specified in the latest revision of SP 800-131A.*	✓	✓	In scope - Applicable
5.1.4.1	✓				*63B#0840*			*The CSP SHALL ensure that the nonce used to generate a OTP is of sufficient length to ensure that it is unique for each operation of the device over its lifetime.*	✓	✓	In scope - Applicable

5.1.4.1	✓				*63B#0850*			*Thd CSP SHALL ensure that it uses SF-OTP Devices which do not facilitate the cloning of the secret key onto multiple devices.*	✓	✓	**In scope - Not applicable There is reasonable cause for Google Authenticator to not allow key cloning.**
5.1.4.1					*n/a*						
5.1.4.1	✓				*63B#0860*			*The CSP SHALL ensure that, if the nonce used to generate the authenticator output is based on a real-time clock, the nonce is changed at least once every 2 minutes.*	✓	✓	In scope - Applicable
5.1.4.1	✓				*63B#0870*			*The CSP SHALL ensure that,the OTP value associated with a given nonce is accepted only once.*	✓	✓	In scope - Applicable
5.1.4.2	✓				*63B#0880*			*The CSP SHALL employ techniques which strongly protect against compromise of symmetric keys used by authenticators.*	✓	✓	**In scope - Not applicable ID.me does not use PKI**
5.1.4.2	✓				*63B#0890*			*The CSP SHALL use approved cryptography to ensure that a Subject's SF-OTP authenticator to either:*	✓	✓	**In scope - Not applicable ID.me receives the OTP over an authenticated protected channel from the subject**
5.1.4.2	✓				*63B#0890*	*a)*		*generate and exchange the secrets required to duplicate the authenticator output.*	✓	✓	**In scope - Not applicable ID.me receives the OTP over an authenticated protected channel from the subject**

	✓				*63B#0890*	*b*		*obtain the secrets required to duplicate the authenticator output; OR*	✓	✓	**In scope - Not applicable ID.me receives the OTP over an authenticated protected channel from the subject**
5.1.4.2	✓				*63B#0900*			*The CSP SHALL use approved encryption and an authenticated protected channel when retrieving the OTP.*	✓	✓	In scope - Applicable
5.1.4.2	✓				*63B#0910*			*The CSP SHALL ensure that, when using time-based OTPs [RFC238], their lifetime is determined taking into account:*	✓	✓	In scope - Applicable
5.1.4.2	✓				*63B#0910*	*a)*		*the expected clock drift (in either direction) of the authenticator over its lifetime;*	✓	✓	In scope - Applicable
5.1.4.2	✓				*63B#0910*	*b)*		*allowance for network delay;*	✓	✓	In scope - Applicable
5.1.4.2	✓				*63B#0910*	*c)*		*an allowance for user entry of the OTP.*	✓	✓	In scope - Applicable
5.1.4.2	✓				*63B#0920*			*The CSP SHALL accept a given time-based OTP only once during its validity period.*	✓	✓	In scope - Applicable
5.1.4.2	✓				*63B#0930*			*IF an authentication secret has fewer than 64 bits of entropy the CSP SHALL enforce a rate-limiting mechanism iaw 63B#0510*	✓	✓	In scope - Applicable

5	✓				*63B#0940*			*The CSP shall ensure that each use of a MF-OTP authenticator equires both factors to be input*	✓	✓	**In scope - Not applicable ID.me does not differeniate between SF-OTP and MF-OTP**
5.1.5.1					*n/a*						
5.1.5.1	✓				*63B#0950*			*The CSP SHALL use MF-OTP Devices whose secret key and associated algorithm provide at least the minimum security strength specified in the latest revision of SP 800-131A.*	✓	✓	**In scope - Not applicable See 63B#0940**
5.1.5.1	✓				*63B#0960*			*The CSP SHALL ensure that the nonce used to generate a OTP is of sufficient length to ensure that it is unique for each operation of the device over its lifetime.*	✓	✓	**In scope - Not applicable See 63B#0940**
5.1.5.1	✓				*63B#0970*			*Thd CSP SHALL ensure that it uses MF-OTP Devices which do not facilitate the cloning of the secret key onto multiple devices.*	✓	✓	**In scope - Not applicable See 63B#0940**
5.1.5.1					*n/a*						

5.1.5.1	✓				*63B#0980*			*The CSP SHALL ensure that, if the nonce used to generate the authenticator output is based on a real-time clock, the nonce is changed at least once every 2 minutes.*	✓	✓	**In scope - Not applicable See 63B#0940**
5.1.5.1	✓				*63B#0990*			*The CSP SHALL ensure that,the OTP value associated with a given nonce is accepted only once.*	✓	✓	**In scope - Not applicable See 63B#0940**
5.1.5.1	✓				*63B#1000*			*The CSP SHALL ensure that memorized secrets used by the authenticator for activation are a randomly-chosen numeric secret at least 6 decimal digits in length or other memorized secret of equivalent complexity*	✓	✓	**In scope - Not applicable See 63B#0940**
5.1.5.1	✓				*63B#1010*			*The CSP SHALL enforce a rate-limiting mechanism iaw 63B#1450 & '1460 (without qualification regarding the degree of entropy the memorized secret exhibits).*	✓	✓	**In scope - Not applicable See 63B#0940**
5.1.5.1	✓				*63B#1020*			*If a biometric factor is used in an authentication the CSP SHALL ensure that all criteria 63B#1470 - '1550 are fulfilled.*	✓	✓	**In scope - Not applicable ID.me does not support a biometric factor for authentication.**
5.1.5.1	✓				*63B#1030*			*The CSP SHALL zeroize the unencrypted secret key and the activation secret or biometric sample (including any associated biometric data) immediately after an OTP has been generated.*	✓	✓	**In scope - Not applicable ID.me does not support a biometric factor for authentication.**
5.1.5.2	✓				*63B#1040*			*The CSP SHALL ensure that MF-OTP authenticators strongly protected against compromise the associated symmetric keys.*	✓	✓	**In scope - Not applicable See 63B#0940**

5.1.5.2	✓				*63B#1050*			*The CSP SHALL use approved cryptography to ensure that a Subject's MF-OTP authenticator to either:*	✓	✓	**In scope - Not applicable See 63B#0940**
5.1.5.2	✓				*63B#1050*	*a)*		*generate and exchange the secrets required to duplicate the authenticator output; OR*	✓	✓	**In scope - Not applicable See 63B#0940**
5.1.5.2	✓				*63B#1050*	*b)*		*obtain the secrets required to duplicate the authenticator output.*	✓	✓	**In scope - Not applicable See 63B#0940**
5.1.5.2	✓				*63B#1060*			*The CSP SHALL treat all authenticators as being single-factor devices unelss they establish, via the authenticator source, that the authenticator device is multi-factor.*	✓	✓	**In scope - Not applicable ID.me does not differeniate between SF-OTP and MF-OTP**
5.1.5.2	✓				*63B#1070*			*Unless it is able to rely upon a statement via the authenticator source that a device is multi-factor the CSP SHALL treat the authenticator as if it was single-factor.*	✓	✓	In scope - Applicable
5.1.5.2	✓				*63B#1080*			*The CSP SHALL ensure that all communication between the Claimant and Verifier use approved encryption and is via an authenticated protected channel.*	✓	✓	In scope - Applicable
5.1.5.2	✓				*63B#1090*			*The CSP SHALL use verification methods which ensure that, when using time-based OTPs [RFC238], their lifetime is determined taking into account:*	✓	✓	**In scope - Not applicable ID.me does not differeniate between SF-TOTP and MF-TOTP.** **See 63B#0910 for SF-TOTP lifetime controls**
5.1.5.2	✓				*63B#1090*	*a)*		*the expected clock drift (in either direction) of the authenticator over its lifetime;*	✓	✓	
5.1.5.2	✓				*63B#1090*	*b)*		*allowance for network delay;*	✓	✓	
5.1.5.2	✓				*63B#1090*	*c)*		*an allowance for user entry of the OTP.*	✓	✓	
5.1.5.2	✓				*63B#1100*			*The CSP SHALL accept a given time-based OTP only once during its validity period.*	✓	✓	

5.1.5.2					*n/a*						
5.1.5.2	✓				*63B#1110*			*IF an authentication output or activation secret has fewer than 64 bits of entropy the CSP SHALL enforce a rate-limiting mechanism iaw 63B#0510*	✔	✓	In scope - Applicable
5.1.5.2	✓				*63B#1120*			*If a biometric factor is used in an authentication the CSP SHALL ensure that all criteria 63B#1470 - '1550 are fulfilled.*	✔	✓	**In scope - Not applicable ID.me does not support a biometric factor for authentication.**
	✓				*63B#1130*			*The CSP SHALL ensure that SF-CS keys are stored in suitably secure storage available to the authenticator application.*	✔	✓	In scope - Applicable
5.1.6.1	✓				*63B#1140*			*The CSP SHALL ensure that SF-CS keys are strongly protected against unauthorized disclosure by the use of access controls that limit access to the key to only those software components on the device requiring access.*	✔	✓	In scope - Applicable
5.1.6.1	✓				*63B#1150*			*The CSP SHALL ensure that SF-CS key authenticators DO NOT facilitate the cloning of the secret key onto multiple devices.*	✔	✓	In scope - Applicable

5.1.6.2	✓				*63B#1160*			*Criteria 63B#1210 to '1240 SHALL be fulfilled.*	✔	✓	In scope - Applicable
5	✓				*63B#1170*			*The CSP SHALL use SF-CD authenticators that are incapable of exporting their [unique] secret key.*	✔	✓	In scope - Applicable
5.1.7.1					*n/a*						
5.1.7.1	✓				*63B#1180*			*The CSP SHALL use SF-CD authenticators whose secret key and associated algorithm provide at least the minimum security strength specified in the latest revision of SP 800-131A.*	✔	✓	In scope - Applicable
5.1.7.1	✓				*63B#1190*			*The CSP SHALL use SF-CD authenticators which employ a nonce of at least 64 bits length.*	✔	✓	In scope - Applicable
5.1.7.1	✓				*63B#1200*			*The CSP SHALL use SF-CD Devices that use approved cryptography*	✔	✓	In scope - Applicable

5.1.7.1					*n/a*						
5.1.7.2					*n/a*						
5.1.7.2	✓				*63B#1210*			*The CSP SHALL use verification methods which protect any secret keys against modification.*	✓	✓	In scope - Applicable
5.1.7.2	✓				*63B#1220*			*The CSP SHALL use verification methods which protect symmetric secret keys against unauthorized disclosure.*	✓	✓	**In scope - Not applicable ID.me uses asymmetric keys for authentication**
5.1.7.2	✓				*63B#1230*			*The CSP SHALL use verification methods for which the nonce is:*	✓	✓	In scope - Applicable
5.1.7.2	✓				*63B#1230*	*a)*		*at least 64 bits in length; AND*	✓	✓	In scope - Applicable
5.1.7.2	✓				*63B#1230*	*b)*		*either:*	✓	✓	In scope - Applicable
5.1.7.2	✓				*63B#1230*	*b)*	*i)*	*unique over the authenticator's lifetime; OR*	✓	✓	In scope - Not applicable see b) ii)
5.1.7.2	✓				*63B#1230*	*b)*	*ii)*	*generated using an approved random bit generator [SP 800-90Ar1]*	✓	✓	In scope - Applicable
5.1.7.2	✓				*63B#1240*			*The CSP's verification methods SHALL use approved cryptography.*	✓	✓	In scope - Applicable
5.1.8					*n/a*						

5.1.8	✓				*63B#1250*			*The CSP SHALL ensure that MF-CS authenticators are activated by either* something [the Claimant] knows *or* something [the Claimant] is.	✔	✓	**In scope - Not applicable ID.me does not differeniate between SF-CS and MF-CS**
5.1.8.1					*n/a*						
5.1.8.1	✓				*63B#1260*			*The CSP SHALL ensure that MF-CS keys are strongly protected against unauthorized disclosure by the use of access controls that limit access to the key to only those software components on the device requiring access.*	✔	✓	**In scope - Not applicable ID.me does not differeniate between SF-CS and MF-CS**
5.1.8.1	✓				*63B#1270*			*The CSP SHALL ensure that MF-CS key authenticators DO NOT facilitate the cloning of the secret key onto multiple devices.*	✔	✓	**In scope - Not applicable ID.me does not differeniate between SF-CS and MF-CS**
5.1.8.1	✓				*63B#1280*			*The CSP SHALL ensure that MF-CS key authenticators require the input of all factors before performing the authentication operation.*	✔	✓	**In scope - Not applicable ID.me does not differeniate between SF-CS and MF-CS**

5.1.8.1	✓				*63B#1290*			*The CSP SHALL ensure that memorized secrets used by the authenticator for activation are a randomly-chosen numeric value at least 6 decimal digits in length or other memorized secret meeting the requirements of the applicable criteria 63B#0410 - '0450.*	✔	✓	**In scope - Not applicable ID.me does not differeniate between SF-CS and MF-CS**
5.1.8.1	✓				*63B#1300*			*The CSP SHALL enforce a rate-limiting mechanism iaw 63B#1450 & '1460 (without qualification regarding the degree of entropy which the memorized secret exhibits).*	✔	✓	**In scope - Not applicable ID.me does not differeniate between SF-CS and MF-CS**
5.1.8.1	✓				*63B#1310*			*If a biometric factor is used in an authentication the CSP SHALL ensure that all criteria 63B#1470 - '1550 are fulfilled.*	✔	✓	**In scope - Not applicable ID.me does not support a biometric factor for authentication.**
5.1.8.1	✓				*63B#1320*			*The CSP SHALL zeroize the unencrypted secret key and the activation secret or biometric sample (including any associated biometric data) immediately after an authentication transaction has taken place.*	✔	✓	**In scope - Not applicable ID.me does not support a biometric factor for authentication.**
5.1.8.2	✓				*63B#1330*			*Criteria 63B#1040 to '1070 SHALL be fulfilled.*	✔	✓	**In scope - Not applicable ID.me does not support a biometric factor for authentication.**

5.1.9	✓				*63B#1340*			*The CSP SHALL ensure that MF-CS authenticators are activated by either* something [the Claimant] knows *or* something [the Claimant] is.	✔	✓	**In scope - Not applicable ID.me does not differeniate between SF-CS and MF-CS**
5.1.9.1					*n/a*						
5.1.9.1	✓				*63B#1350*			*The CSP SHALL use MF-CD authenticators whose secret key and associated algorithm provide at least the minimum security strength specified in the latest revision of SP 800-131A.*	✔	✓	**In scope - Not applicable ID.me does not differeniate between SF-CS and MF-CS**
5.1.9.1	✓				*63B#1360*			*The CSP SHALL use MF-CD authenticators which employ a nonce of at least 64 bits length.*	✔	✓	**In scope - Not applicable ID.me does not differeniate between SF-CS and MF-CS**
5.1.9.1	✓				*63B#1370*			*The CSP SHALL use MF-CD Devices that use approved cryptography*	✔	✓	**In scope - Not applicable ID.me does not differeniate between SF-CS and MF-CS**
5.1.9.1					*n/a*						

5.1.9.1	✓				*63B#1380*			*The CSP SHALL ensure that memorized secrets used by the authenticator for activation are a randomly-chosen numeric value at least 6 decimal digits in length or other memorized secret meeting the requirements of the applicable criteria 63B#0410 - '0450.*	✔	✓	In scope - Applicable
5.1.9.1	✓				*63B#1390*			*The CSP SHALL enforce a rate-limiting mechanism iaw 63B#0510 (without qualification regarding the degree of entropy the memorized secret exhibits).*	✔	✓	In scope - Applicable
5.1.9.1	✓				*63B#1400*			*If a biometric factor is used in an authentication the CSP SHALL ensure that all criteria 63B#1470 - '1550 are fulfilled.*	✔	✓	**In scope - Not applicable ID.me does not support a biometric factor for authentication.**
5.1.9.1	✓				*63B#1410*			*The CSP SHALL zeroize the unencrypted secret key and the activation secret or biometric sample (including any associated biometric data) immediately after an authentication transaction has taken place.*	✔	✓	**In scope - Not applicable ID.me does not support a biometric factor for authentication.**
5.1.9.2	✓				*63B#1420*			*Criteria 63B#1040 to '1070 SHALL be fulfilled.*	✔	✓	**In scope - Not applicable ID.me does not support a biometric factor for authentication.**
5,2					*n/a*						
5.2.1	✓				*63B#1430*			*The CSP SHALL provide Subjects instructions on how to appropriately protect the authenticator against theft or loss.*	✔	✓	In scope - Applicable

5.2.1	✓				*63B#1440*			*The CSP SHALL provide a documented mechanism to revoke or suspend the authenticator immediately upon notification from the Subject that loss or theft of the authenticator is suspected.*	✔	✓	In scope - Applicable
5.2.2	✓				*63B#1450*			*The CSP SHALL implement controls to protect against online guessing attacks.*	✔	✓	In scope - Applicable
5.2.2	✓				*63B#1460*			*The CSP SHALL limit consecutive failed authentication attempts on a single account to no more than 100.*	✔	✓	In scope - Applicable
5.2.2					*n/a*						
5.2.2					*n/a*						
5.2.2					*n/a*						
5.2.2					*n/a*						
5.2.2					*n/a*						

5.2.2					*n/a*						
5.2.3					*n/a*						
5.2.3	✓				*63B#1470*			*The CSP SHALL only use biometric techniques as part of a multi-factor authentication which requires the Claimant to utilise a physical authenticator.*	✔	✓	**In scope - Not applicable** This happens on the user's device and is beyond the scope of ID.me's ability to manage and control. ID.me's service embodies no biometric functionality and no biometric data is handled by the service.
5.2.3	✓				*63B#1480*			*When using biometrics for authentication, the CSP SHALL establish an authenticated protected channel between the sensor (or an endpoint containing a sensor that resists sensor replacement) and the verifier.*	✔	✓	In scope - Applicable
5.2.3	✓				*63B#1490*			*When using biometrics for authentication, the CSP SHALL ensure that the sensor or endpoint is authenticated prior to capturing the biometric sample from the Claimant.*	✔	✓	In scope - Applicable
5.2.3	✓				*63B#1500*			*The CSP shall implement biometric systems which have at least the following characteristics:*	✔	✓	In scope - Applicable
5.2.3	✓				*63B#1500*	*a)*		*operate with an FMR [ISO/IEC 2382-37] of 1 in 1000 or better;*	✔	✓	In scope - Applicable
5.2.3	✓				*63B#1500*	*b)*		*achieved that FMR operation under conditions of a conformant attack (i.e., zero-effort impostor attempt) in accordance with ISO/IEC 30107-1;*	✔	✓	In scope - Applicable

5.2.3					*n/a*						
5.2.3	✓				*63B#1500*	*c)*		*perform testing of presentation attack resistance in accordance with §12 of ISO/IEC 30107-3.*	✔	✓	In scope - Applicable
5.2.3					*n/a*						
5.2.3	✓				*63B#1510*			*The CSP SHALL implement rate-limiting measures on failed authentication attempts as follows:*	✔	✓	In scope - Applicable
5.2.3	✓				*63B#1510*	*a)*		*where analysis has shown at least 90% resistance to presentation attacks for each relevant attack type (i.e., species), where resistance is defined as the number of thwarted presentation attacks divided by the number of trial presentation attacks, THEN up to 10 consecutive failed authentication attempts can occur; OTHERWISE*	✔	✓	**In scope - Not Applicable ID.me does not use biometrics as an authenticator**
5.2.3	✓				*63B#1510*	*b)*		*no more than 5 consecutive failed authentication attempts can occur.*	✔	✓	In scope - Applicable
5.2.3	✓				*63B#1520*			*If either limit set in 63B#1510 is reached the CSP SHALL:*	✔	✓	In scope - Applicable
5.2.3	✓				*63B#1520*	*a)*		*disable the biometric user authentication, and if an alternative authentication factor is already available use that other factor; OR OTHERWISE*	✔	✓	In scope - Not applicable b) is selected

5.2.3	✓				*63B#1520*	*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	✓				*63B#1530*			*When using biometric data in an authentication the CSP SHALL ensure that the sensor and endpoint performance, integrity, and authenticity are such as to not present unacceptable risk during the operation of the authentication protocol.*	✓	✓	**In scope - Not Applicable ID.me does not use biometrics as an authenticator**
5.2.3					*n/a*						
5.2.3					*n/a*						
5.2.3					*n/a*						
5.2.3					*n/a*						
5.2.3					*n/a*						
5.2.3	✓				*63B#1540*			*If biometric comparisom is performed centrally rather than locally the CSP SHALL:*	✓	✓	In scope - Applicable
5.2.3	✓				*63B#1540*	*a)*		*limit use of the biometric as an authentication factor to one or more specific devices that are authenticated using approved cryptography;*	✓	✓	**In scope - Not Applicable ID.me does not use biometrics as an authenticator**
5.2.3	✓				*63B#1540*	*b)*		*use a separate key to identify the device;*	✓	✓	**In scope - Not Applicable ID.me does not use biometrics as an authenticator**

5.2.3	✓				*63B#1540*	*c)*		*implement biometric revocation (a.k.a. biometric template protection);* Note - this is for both revocation of the credential as much as for privacy protection	✔	✓	**In scope - Not Applicable ID.me does not use biometrics as an authenticator**
5.2.3	✓				*63B#1540*	*d)*		*transmit all biometric data over an authenticated protected channel.*	✔	✓	In scope - Applicable
5.2.3					*n/a*						
5.2.3	✓				*63B#1550*			*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**
5.2.3					*n/a*						
5.2.4					*n/a*						
5.2.4					*n/a*						
5.2.4					*n/a*						
5.2.4					*n/a*						
5.2.4					*n/a*						

5.2.4	✓				*63B#1560*			*If it signs authentication attestations the CSP SHALL use a digital signature that provides at least the minimum security strength specified in the latest revision of SP 800-131A.*	✔	✓	**In scope - Not applicable U2F does not presently support signing the attestation.**
5.2.4					*n/a*						
5.2.5					*n/a*						
5.2.5	✓				*63B#1570*			***The CSP SHALL establish an authenticated protected channel between itself and the verifier by use of a verifier impersonation-resistant authentication protocol***		✔	***Not in scope This AAL not supported***
5.2.5	✓				*63B#1580*			***The CSP SHALL strongly and irreversibly bind to the authenticator output a channel identifier which was negotiated during the establishment of the authenticated protected channel***		✔	***Not in scope This AAL not supported***
5.2.5	✓				*63B#1590*			***At the time of binding the channel identifier the CSP SHALL validate the information used to prove verifier impersonation-resistance.***		✔	***Not in scope This AAL not supported***

5.2.5	✓				*63B#1600*			***The CSP SHALL establish the verifier impersonation resistant channel using approved cryptographic algorithms the keys for which meet at least the minimum security strength specified in the latest revision of SP 800-131A.***		✓	***Not in scope This AAL not supported***
5.2.5					*n/a*						
5.2.5	✓				*63B#1610*			***The CSP SHALL NOT accept as verifier impersonation-resistant authenticators those that involve the manual entry of an authenticator output.***		✓	***Not in scope This AAL not supported***
5.2.6	✓				*63B#1620*			*If the CSP uses the services of a remote/independent Verifier, all communications with that entity SHALL occur through a mutually-authenticated secure channel using approved cryptography.*	✓	✓	In scope - Applicable
					n/a						

5.2.7	✓				*63B#1630*			*For verifier's public keys to be considered verifier compromise resistant, the CSP SHALL only store such keys when they:*		✓	***Not in scope*** ***This AAL not supported***
5.2.7	✓				*63B#1630*	*a)*		*use approved cryptographic algorithms;*		✓	***Not in scope*** ***This AAL not supported***
5.2.7	✓				*63B#1630*	*b)*		*provide at least the minimum security strength specified in the latest revision of SP 800-131A.*		✓	***Not in scope*** ***This AAL not supported***
5.2.7	✓				*63B#1640*			*For verifier's secrets other than public key to be considered verifier compromise resistant, the CSP SHALL only only store such secrets when they:*		✓	***Not in scope*** ***This AAL not supported***
5.2.7	✓				*63B#1640*	*a)*		*use approved hashing algorithms;*		✓	***Not in scope*** ***This AAL not supported***
5.2.7	✓				*63B#1640*	b)		*provide at least the minimum security strength specified in the latest revision of SP 800-131A.*		✓	***Not in scope*** ***This AAL not supported***
5.2.7					*n/a*			*Superseded by the two criteria above*			
5.2.8					*n/a*						
5.2.9					*n/a*						
5.2.9	✓				*63B#1650*			*The CSP SHALL use only those authenticators which demonstrate authentication intent.*	✓	✓	In scope - Applicable
5.2.9					*n/a*						
5.2.9					*n/a*						
5.2.10					*n/a*						
5.2.10	✓				*63B#1660*			*If the CSP employs RESTRICTED authenticators then the associated risks shall be considered in its risk assessments.*	✓	✓	In scope - Not applicable ID.me does not use restricted authenticators

5.2.10					*n/a*						
5.2.10	✓				*63B#1670*			*If the CSP employs RESTRICTED authenticators then it SHALL:*	✔	✓	In scope - Applicable
5.2.10	✓				*63B#1670*	*a)*		*require at least one alternate authenticator that is not RESTRICTED;*	✔	✓	In scope - Applicable
5.2.10	✓				*63B#1670*	*b)*		*provide meaningful notice to subscribers regarding the security risks of the RESTRICTED authenticator and availability of alternative(s) that are not RESTRICTED;*	✔	✓	In scope - Applicable
5.2.10					*n/a*			*See 63B#1660*			
5.2.10				✓	*63B#1680*			*The CSP SHALL, in a digital identity acceptance statement (DIAS), develop a migration plan to account for the possibility that the RESTRICTED authenticator is no longer acceptable at some point in the future.*	✔	✓	**In scope - Not applicable Only the applicable Fed Agency can complete its DIAS**
6					*n/a*						
6,1					*n/a*						
6,1	✓				*63B#1690*			*The CSP SHALL bind authenticators to Subject accounts by either:*	✔	✓	In scope - Applicable
6,1	✓				*63B#1690*	*a)*		*issuing them at the time of enrollment; OR*	✔	✓	**In scope - Not applicable We do not issue authenticators**

6,1	✓				*63B#1690*	*b)*		*associating a subscriber-provided authenticator that is acceptable to the CSP.*	✔	✓	In scope - Applicable
6,1					*n/a*						
6,1	✓				*63B#1700*			*The CSP SHALL maintain, for the duration of the digital identity lifecycle accounting for the provisions of its data retention schedule, a record of all authenticators that are or have been associated with each identity and of all significant actions taken with regard to the maintenance of each authenticator.*	✔	✓	In scope - Applicable
6,1	✓				*63B#1710*			*The CSP SHALL maintain information required for throttling authentication attempts when required (see 63B#1450 & '#1460).*	✔	✓	In scope - Applicable
6,1	✓				*63B#1720*			*The CSP SHALL determine the type of user-provided authenticator and make that determination available to Verifiers to fulfill AAL2 requirements.*	✔	✓	In scope - Applicable
6,1	✓				*63B#1730*			*The CSP SHALL maintain, for the duration of the digital identity lifecycle accounting for the provisions of its data retention schedule, a record of all authenticators that are or have been associated with each identity:*	✔	✓	In scope - Applicable
6,1					*n/a*						
6,1					*n/a*						
6,1					*n/a*						

6,1	✓				*63B#1740*			*The CSP SHALL ensure that, when any new authenticator is bound to a subscriber account, the binding protocol and the protocol for provisioning the associated key(s) are done at a level of security commensurate with use of the authenticator at AAL2.*	✔	✓	In scope - Applicable
6,1					*n/a*						
6,1	✓				*63B#1750*			*The CSP SHALL NOT bind multifactor authenticators unless at the end of a session in which identity proofing has been completed or after multifactor authentication has already been accomplished.*	✔	✓	In scope - Applicable
6,1					*n/a*			Included within 63B#1750			
6.1.1					*n/a*			Though not normatively-stated, accommodated within the following criterion.			
6.1.1	✓				*63B#1760*			*When the CSP binds an authenticator to an identity as a result of the CSP having performed a successful identity proofing of the Subject, the CSP SHALL bind to the Subject's online identity:*	✔	✓	In scope - Applicable

6.1.1	✓				*63B#1760*	*a)*		*at least one physical (*something [the Subject] has*) authenticator; AND*	✔	✓	In scope - Applicable
6.1.1	✓				*63B#1760*	*b)*		*a memorized secret or at least one biometric.*	✔	✓	In scope - Applicable
6.1.1					*n/a*						
6.1.1					*n/a*						
6.1.1	✓				*63B#1770*			*The CSP SHALL ensure that authenticators bound to the Subject's online identity are AAL2 or higher.*	✔	✓	In scope - Applicable
6.1.1					*n/a*						
6.1.1					*n/a*						

6.1.1	✓				*63B#1780*			*The CSP SHALL NOT expose personal information to the subscriber, even if self-asserted, unless AAL2 authentication has been accomplished.*	✓	✓	In scope - Applicable
6.1.1					*n/a*						
6.1.1	✓				*63B#1790*			*If enrollment and binding cannot be completed in a single physical encounter or within a single protected electronic transactional session, the CSP SHALL employ the following methods to ensure that the same party acts as the Applicant throughout the processes:*	✓	✓	In scope - Applicable
6.1.1	✓				*63B#1790*	*a)*		*For remote transactions the CSP SHALL:*	✓	✓	In scope - Applicable
6.1.1	✓				*63B#1790*	*a)*	*i)*	*require the Applicant to identify themselves in each new binding transaction by presenting a temporary secret which was either:*	✓	✓	In scope - Applicable
6.1.1	✓				*63B#1790*	*a)*	*i)*	*established during a prior transaction; or*	✓	✓	In scope - Applicable
6.1.1	✓				*63B#1790*	*a)*	*i)*	*sent to the Applicant's phone number, email address, or postal address of record.*	✓	✓	In scope - Applicable
6.1.1	✓				*63B#1790*	*a)*	*ii)*	*Only issue long-term authenticator secrets to the Applicant within a protected session.*	✓	✓	In scope - Applicable
6.1.1	✓				*63B#1790*	*b)*		*For in-person transactions the CSP SHALL:*	✓	✓	In scope - Applicable
6.1.1	✓				*63B#1790*	*b)*	*i)*	*require the Applicant to identify themselves in person by either:*	✓	✓	In scope - Applicable
6.1.1	✓				*63B#1790*	*b)*	*i)*	*using a secret as described in remote transaction a) i) above; OR*	✓	✓	In scope - Applicable
6.1.1	✓				*63B#1790*	*b)*	*i)*	*through use of a biometric that was recorded during a prior encounter.*	✓	✓	In scope - Applicable

6.1.1	✓				*63B#1790*	*b)*	*ii)*	*only accepting a temporary secret once;*	✓	✓	**In scope - Not applicable ID.me does not support a temporary secret during in-person transactions**
6.1.1	✓				*63B#1790*	*b)*	*iii)*	*only relying upon long-term authenticator secrets during a physical transaction, if they have been loaded locally onto a physical device that is issued in person to the Applicant or delivered in a manner that confirms the Applicant's address of record.*	✓	✓	In scope - Applicable
6.1.2					*n/a*						
6.1.2.1					*n/a*						
6.1.2.1					*n/a*						
6.1.2.1	✓				*63B#1800*			*Prior to issuing the Subject with new/additional AAL2 authenticators the CSP SHALL first authenticate the Subject at AAL2.*	✓	✓	In scope - Applicable

6.1.2.1					*n/a*						
6.1.2.2					*n/a*						
6.1.2.2					*n/a*						
6.1.2.2					*n/a*						
6.1.2.3	✓				*63B#1810*			*If a Claimant loses all authenticators of a factor necessary to complete multi-factor authentication the CSP SHALL enable replacement of lost authentication factors by one of the following methods:*	✔	✓	In scope - Applicable
6.1.2.3	✓				*63B#1810*	*a)*		*require the Claimant to present themselves for full identity proofing as per the CSP's policies and processes as operated in conformity with the applicable 63A_SAC criteria; OR*	✔	✓	In scope - Not applicable b) is selected

6.1.2.3					*n/a*						
6.1.2.3	✓				*63B#1810*	*b)*		*IF the CSP has retained evidence from the original proofing process pursuant to a privacy risk assessment iaw 63A#0180, the CSP SHALL authenticate the Claimant using an authenticator of the remaining factor, if any, to confirm binding to the existing identity.*	✔	✓	In scope - Applicable
6.1.2.3	✓				*63B#1820*			*The CSP SHALL re-establish authentication factors by:*		✓	***Not in scope*** ***This AAL not supported***
6.1.2.3	✓				*63B#1820*	a)		*using a Supervised (In-Person or Remote) process; AND*		✓	***Not in scope*** ***This AAL not supported***
6.1.2.3	✓				*63B#1820*	b)		*verifying the biometric collected during the original proofing process.*		✓	***Not in scope*** ***This AAL not supported***
6.1.2.3					*n/a*						
6.1.2.3					*n/a*						

6.1.2.3					*n/a*						
6.1.2.3					*n/a*						
6.1.2.3	✓				*63B#1830*			*The CSP SHALL, if it supports re-proofing through binding memorized secrets using two physical authenticators, use confirmation codes that consist of at least 6 random alphanumeric characters generated by an approved random-bit generator [SP 800-90Ar1].*	✔	✓	In scope - Not applicable ID.me does not support re-proofing using two physical authenticators
6.1.2.3	✓				*63B#1840*			*The CSP SHALL only issue confirmation codes that have the following [maximum] validities:*	✔	✓	In scope - Not applicable As #1830
6.1.3					*n/a*						
6.1.3					*n/a*						
6.1.3	✓				*63B#1850*			*See 63B#1800*	✔	✓	In scope - Applicable

6.1.3					*n/a*						
6.1.4					*n/a*						
6,2					*n/a*						
6,2					*n/a*						
6,2					*n/a*						
6,2	✓				*63B#1860*			*IF the CSP supports a method by which it can authenticate the Subject using a backup or alternate authenticator the CSP SHALL only accept backup authenticators which are either a memorized secret or a physical authenticator.*	✔	✓	**In scope - Not applicable ID.me does not support authenticating subjects with a backup authenticator.**

6,2					*n/a*						
6,2	✓				*63B#1870*			*The CSP SHALL, if it supports suspension of authenticators reported as having been compromised, ensure that such suspension is reversible if the Subject is successfully authenticated by the CSP using an alternative valid (i.e., not suspended) authenticator, at the same or higher assurance level, and the Subject requests reactivation of the suspended authenticator.*	✔	✓	In scope - Applicable
6,2					*n/a*						
6,3					*n/a*						
6,3	✓				*63B#1880*			*If the CSP issues authenticators which expire the CSP SHALL NOT accept authentication claims which attempt to use an expired authenticator.*	✔	✓	**In scope - Not applicable ID.me does not issue short-lived authenticators.**
6,3					*n/a*						
6,3	✓				*63B#1890*			*The CSP SHALL require Subjects to surrender or attest to destruction of any physical authenticator containing attribute certificates signed by the CSP as soon as practical after expiration or receipt of a renewed authenticator, or after receipt of notice of either revocation or termination.*	✔	✓	**In scope - Not applicable ID.me does not issue signed attribute cerificates**

6,4					*n/a*						
6,4	✓				*63B#1900*			*The CSP SHALL revoke promptly the binding of authenticators to the Subject's online identity, and give notice of such to the Subject, when any one of the following occurs:*	✔	✓	In scope - Applicable
6,4	✓				*63B#1900*	*a)*		*the Subject's online identity ceases to exist; OR*	✔	✓	In scope - Applicable
6,4	✓				*63B#1900*	*b)*		*the Subject requests revocation; OR*	✔	✓	In scope - Applicable
6,4	✓				*63B#1900*	*c)*		*the CSP determines that the Subject no longer meets its eligibility requirements; OR*	✔	✓	In scope - Applicable
6,4	✓				*63B#1900*	*d)*		*the CSP is obligated to do so in response to a legal instrument.*	✔	✓	In scope - Applicable
6,4	✓				*63B#1910*			*The CSP SHALL require Subscribers/Subjects to surrender or certify destruction of any physical authenticator containing certified attributes signed by the CSP as soon as practical after revocation or termination takes place.*	✔	✓	In scope - Applicable
6,4					*n/a*						
7					*n/a*						

7.1.1					*n/a*						
7.1.2					*n/a*						
7.1.3					*n/a*						
7,2	✓				*63B#1920*			*The CSP SHALL issue a session secret at the time of initial verification of a User and SHALL maintain that session secret OR a refreshed replacement session secret for the duration of the session.*	✔	✓	In scope - Applicable
7,2					*n/a*						
7,2					*n/a*						
7,2					*n/a*						
7,2	✓				*63B#1930*			*The CSP SHALL NOT allow session secrets (whether ~~one~~ issued initially or ~~one~~ refreshed) to persist beyond the termination of a session.*	✔	✓	In scope - Applicable
7,2					*n/a*			At AAL2, see 63B#0150 At AAL3, see 63B#0320			

7,2					*n/a*			See 63B#0140			
7,2	✓				*63B#1940*			*Prior to terminating a session for reason of inactivity the CSP SHALL prompt the Subject for their memorized secret or biometric attribute to extend the re-authentication time limit.*	✓	✓	In scope - Applicable
7,2	✓				*63B#1950*			*The CSP SHALL require a new session to be started, with re-authentication of the Subject after any session termination (for whatever reason).*	✓	✓	In scope - Applicable
7.2.1					*n/a*						
7.2.1	✓				*63B#1960*			*Unless the CSP is supporting a federation protocol which permits RPs to specify an acceptable authentication age then the CSP SHALL make no assumptions of correlation between its session with the Subscriber and those of any other party.*	✓	✓	In scope - Applicable
7.2.1					*n/a*						

7.2.1					*n/a*						
7.2.1	✓				*63B#1970*			*If the CSP is supporting a federation protocol which permits RPs to specify a maximum acceptable authentication age then the CSP SHALL modify its conformity to [tag above re 12 hrs] so as to:*	✔	✓	In scope - Applicable
7.2.1	✓				*63B#1970*	*a)*		*re-authenticate the Subscriber within the RP-specified time period;*	✔	✓	In scope - Applicable
7.2.1	✓				*63B#1970*	*b)*		*communicate the authentication event time to the RP;*	✔	✓	In scope - Applicable