

IDESG-KANTARA comparison INCOMPLETE DRAFT
Ordered by tentative equivalency conclusion

Comparison of Certification Requirements: SUMMARY OF INCOMPLETE WORK IN PROCESS														
	Draft	5/30/2016												
	IDESG Reference (From IDEF v.1 Baseline requirements)	IDESG Reference (From IDEF v.1 Baseline requirements)	IDESG Text	(Column P repeated)	Kantara Reference Number	Kantara Title	AL 1	AL 2	AL 3	AL 4	Kantara Text	Kantara Text	Kantara Text	NE=Not Equivalent, NCR=no comparable requirement, or N/A) - Does TFP
1	INTEROP-8.	ACCOUNTABILITY	Entities MUST be accountable for conformance to the IDESG Baseline	F	CO_NUI#050	Record of User Acceptance		✓	✓	✓	Obtain a record (hard-copy or electronic) of the Subscriber's and			F
2	INTEROP-8.	ACCOUNTABILITY	Entities MUST be accountable for conformance to the IDESG Baseline	F	CO_ISM#080	Internal Service Audit			✓	✓	Be audited at least once every 12 months for effective provision of the			F
3	INTEROP-8.	ACCOUNTABILITY	Entities MUST be accountable for conformance to the IDESG Baseline	F	CO_ISM#100	Audit Records		✓	✓	✓	Retain records of all audits, both internal and independent, for a			F
4	INTEROP-8.	ACCOUNTABILITY	Entities MUST be accountable for conformance to the IDESG Baseline	F	CM_SER#010	Security event logs			✓	✓	Ensure that such audit records include:	a) the identity of the point of registration (irrespective of whether		F
5	INTEROP-8.	ACCOUNTABILITY	Entities MUST be accountable for conformance to the IDESG Baseline	F	CM_SER#010	Security event logs			✓	✓	Ensure that such audit records include:	b) generation of the Subject's keys or evidence that the Subject was in		F
6	INTEROP-8.	ACCOUNTABILITY	Entities MUST be accountable for conformance to the IDESG Baseline	F	CM_SER#010	Security event logs			✓	✓	Ensure that such audit records include:	c) generation of the Subject's certificate;		F
7	INTEROP-8.	ACCOUNTABILITY	Entities MUST be accountable for conformance to the IDESG Baseline	F	CM_SER#010	Security event logs			✓	✓	Ensure that such audit records include:	d) dissemination of the Subject's certificate;		F
8	INTEROP-8.	ACCOUNTABILITY	Entities MUST be accountable for conformance to the IDESG Baseline	F	CM_SER#010	Security event logs			✓	✓	Ensure that such audit records include:	e) any revocation or suspension associated with the Subject's		F
9	INTEROP-8.	ACCOUNTABILITY	Entities MUST be accountable for conformance to the IDESG Baseline	F	ID_VRC#025	Provide Subject identity records		✓	✓	✓	If required, provide to qualifying parties records of identity proofing			F
10	INTEROP-8.	ACCOUNTABILITY	Entities MUST be accountable for conformance to the IDESG Baseline	F	ID_VRC#030	Record Retention		✓	✓	✓	Either retain, securely, the record of the verification/revocation process			F
1	PRIVACY-7.	USER DATA CONTROL	Entities MUST provide appropriate mechanisms to enable USERS to	F	CO_NUI#070	Change of Subscriber Information		✓	✓	✓	Require and provide the mechanisms for Subscribers and			F
2	PRIVACY-7.	USER DATA CONTROL	Entities MUST provide appropriate mechanisms to enable USERS to	F	CM_IDP#010	Revision to Subscriber information		✓	✓	✓	Provide a means for Subjects to securely amend their stored			F
1	SECURE-1.	SECURITY PRACTICES	Entities MUST apply appropriate and industrv-accepted information	F	CO_ISM#010	Documented policies and procedures		✓	✓	✓	Have documented all security-relevant administrative management			F
2	SECURE-1.	SECURITY PRACTICES	Entities MUST apply appropriate and industrv-accepted information	F	CO_ISM#120	Best Practice Security Management				✓	Have in place a certified Information Security Management System			F
3	SECURE-1.	SECURITY PRACTICES	Entities MUST apply appropriate and industrv-accepted information	F	CO_OPN#010	Technical security		✓	✓	✓	Demonstrate that the technical controls employed will provide the			F
1	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	CO_SCO#010	Secure remote communications		✓	✓	✓	If the specific service components are located remotely from and	a) implementing mutually-authenticated protected sessions: or		F
2	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	CO_SCO#010	Secure remote communications		✓	✓	✓	If the specific service components are located remotely from and	b) time-stamped or sequenced messages signed by their source and		F
3	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	CM_CTR#020	Protocol threat risk assessment and controls				✓	Account for at least the following protocol threats in its risk	a) password guessing, showing that there is sufficient entropy;		F
4	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	CM_CTR#020	Protocol threat risk assessment and controls			✓	✓	Account for at least the following protocol threats in its risk	b) message replay, showing that it is impractical;		F
5	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	CM_CTR#020	Protocol threat risk assessment and controls			✓	✓	Account for at least the following protocol threats in its risk	c) eavesdropping, showing that it is impractical;		F
6	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	CM_CTR#020	Protocol threat risk assessment and controls			✓	✓	Account for at least the following protocol threats in its risk	d) relying party (verifier) impersonation, showing that it is		F
7	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	CM_CTR#020	Protocol threat risk assessment and controls			✓	✓	Account for at least the following protocol threats in its risk	e) man-in-the-middle attack;		F
8	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	CM_CTR#020	Protocol threat risk assessment and controls			✓	✓	Account for at least the following protocol threats in its risk	f) session hijacking, showing that it is impractical.		F
9	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	CM_CTR#030	System Threat Risk Assessment & Controls	✓	✓	✓	✓	Account for the following system threats and apply appropriate	a) the introduction of malicious code;		F
10	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	CM_CTR#030	System Threat Risk Assessment & Controls	✓	✓	✓	✓	Account for the following system threats and apply appropriate	b) compromised authentication arising from insider action;		F
11	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	CM_CTR#030	System Threat Risk Assessment & Controls	✓	✓	✓	✓	Account for the following system threats and apply appropriate	c) out-of-band attacks by both users and svstem operators (e.g., the		F
12	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	CM_CTR#030	System Threat Risk Assessment & Controls	✓	✓	✓	✓	Account for the following system threats and apply appropriate	d) spoofing of system elements/applications;		F
13	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	CM_CTR#030	System Threat Risk Assessment & Controls	✓	✓	✓	✓	Account for the following system threats and apply appropriate	e) malfeasance on the part of subscribers and subjects;		F
14	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	CM_CTR#030	System Threat Risk Assessment & Controls	✓	✓	✓	✓	Account for the following system threats in its risk assessment and	f) intrusions leading to information theft.		F
15	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	ID_IPV#010	Required evidence				✓	Ensure that the applicant is in possession of:	a) a primary Government Picture ID document that bears a photoarabic	unt num utilit y	F
16	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	ID_IPV#010	Required evidence				✓	Ensure that the applicant is in possession of:	a) a primary Government Picture ID document that bears a photoarabic		F
17	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	ID_IPV#030	Evidence checks – primary ID				✓	Ensure that the presented document:	a) appears to be a genuine document properly issued by the claimed		F

18	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	ID_IPV#030	Evidence checks – primary ID	✓	Ensure that the presented document:	b) bears a photographic image of the holder which matches that of the			F
19	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	ID_IPV#030	Evidence checks – primary ID	✓	Ensure that the presented document:	c) is electronically verified by a record check with the specified	records and other		F
20	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	ID_IPV#030	Evidence checks – primary ID	✓	Ensure that the presented document:	c) is electronically verified by a record check with the specified			F
21	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	ID_IPV#030	Evidence checks – primary ID	✓	Ensure that the presented document:	d) provides all reasonable certainty, at AL4, that the identity exists and			F
22	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	ID_IPV#040	Evidence checks – secondary ID	✓	Ensure that the presented document meets the following conditions:	a) If it is secondary Government Picture ID:	the claim holder or within the results and other properly telephoned		F
23	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	ID_IPV#040	Evidence checks – secondary ID	✓	Ensure that the presented document meets the following conditions:	a) If it is secondary Government Picture ID:			F
24	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	ID_IPV#040	Evidence checks – secondary ID	✓	Ensure that the presented document meets the following conditions:	a) If it is secondary Government Picture ID:			F
25	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	ID_IPV#040	Evidence checks – secondary ID	✓	Ensure that the presented document meets the following conditions:	b) If it is a financial institution account number, is verified by a			F
26	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	ID_IPV#040	Evidence checks – secondary ID	✓	Ensure that the presented document meets the following conditions:	b) If it is a financial institution account number, is verified by a			F
27	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	ID_IPV#040	Evidence checks – secondary ID	✓	Ensure that the presented document meets the following conditions:	c) If it is two utility bills or equivalent documents:			F
28	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	ID_IPV#040	Evidence checks – secondary ID	✓	Ensure that the presented document meets the following conditions:	c) If it is two utility bills or equivalent documents:			F
29	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	ID_IPV#050	Applicant knowledge checks	✓	Where the applicant is unable to satisfy any of the above				F
30	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	ID_AFV#010	Required evidence	✓	Ensure that the applicant possesses:	a) identification from the organization with which it is claiming affiliation:			F
31	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	ID_AFV#010	Required evidence	✓	Ensure that the applicant possesses:	b) agreement from the organization that the applicant may be issued a			F
32	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	ID_AFV#020	Evidence checks	✓	Have in place and apply processes which ensure that the presented	a) each appear to be a genuine document properly issued by the			F
33	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	ID_AFV#020	Evidence checks	✓	Have in place and apply processes which ensure that the presented	b) refer to an existing organization with a contact address:			F
34	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	ID_AFV#020	Evidence checks	✓	Have in place and apply processes which ensure that the presented	c) indicate that the applicant has some form of recognizable affiliation			F
35	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	ID_AFV#020	Evidence checks	✓	Have in place and apply processes which ensure that the presented	d) appear to grant the applicant an entitlement to obtain a credential			F
36	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	ID_IDC#010	Authenticate Original Credential	✓	Prior to issuing any derived credential the original credential on	a) authenticated by a source trusted by the CSP as being valid and un-			F
37	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	ID_IDC#010	Authenticate Original Credential	✓	Prior to issuing any derived credential the original credential on	c) issued in the same name as that which the Applicant is claiming:			F
38	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	ID_IDC#010	Authenticate Original Credential	✓	Prior to issuing any derived credential the original credential on	b) issued at Assurance Level 4;			F
39	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	ID_IDC#010	Authenticate Original Credential	✓	Prior to issuing any derived credential the original credential on	d) proven to be in the possession and under the control of the			F
40	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	ID_IDC#020	Record Original Credential	✓	Record the details of the original credential, the biometric sample				F
41	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	ID_IDC#030	Issue Derived Credential	✓	Only issue the derived credential in-person after performing biometric				F
42	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	ID_SCV#010	Secondary checks	✓	Have in place additional measures (e.g., require additional				F
43	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	CM_CRN#010	Authenticated Request	✓	Only accept a request to generate a credential and bind it to an identity if				F
44	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	CM_CRN#020	Unique identity	✓	Ensure that the identity which relates to a specific applicant is				F
45	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	CM_CRN#030	Credential uniqueness	✓	Allow the Subject to select a credential (e.g., UserID) that is				F
46	SECURE-5.	CREDENTIAL ISSUANCE	Entities that issue or manage credentials and tokens MUST do so	F	CM_CRD#015	Confirm Applicant's identity (in person)	✓	Prior to delivering the credential, require the Applicant to identify				F
1	SECURE-12.	RECOVERY AND REISSUANCE	Entities that issue credentials and tokens MUST implement methods	F	ID_IDC#010	Authenticate Original Credential	✓	Prior to issuing any derived credential the original credential on	a) authenticated by a source trusted by the CSP as being valid and un-			F
2	SECURE-12.	RECOVERY AND REISSUANCE	Entities that issue credentials and tokens MUST implement methods	F	ID_IDC#010	Authenticate Original Credential	✓	Prior to issuing any derived credential the original credential on	c) issued in the same name as that which the Applicant is claiming:			F
3	SECURE-12.	RECOVERY AND REISSUANCE	Entities that issue credentials and tokens MUST implement methods	F	ID_IDC#010	Authenticate Original Credential	✓	Prior to issuing any derived credential the original credential on	b) issued at Assurance Level 4;			F
4	SECURE-12.	RECOVERY AND REISSUANCE	Entities that issue credentials and tokens MUST implement methods	F	ID_IDC#010	Authenticate Original Credential	✓	Prior to issuing any derived credential the original credential on	d) proven to be in the possession and under the control of the			F
5	SECURE-12.	RECOVERY AND REISSUANCE	Entities that issue credentials and tokens MUST implement methods	F	CM_RNR#010	Changeable PIN/Password	✓	Permit Subjects to change the passwords used to activate their				F
6	SECURE-12.	RECOVERY AND REISSUANCE	Entities that issue credentials and tokens MUST implement methods	F	CM_RNR#020	Proof-of-possession on Renewal/Re-issuance	✓	Subjects wishing to change their passwords must demonstrate that				F
7	SECURE-12.	RECOVERY AND REISSUANCE	Entities that issue credentials and tokens MUST implement methods	F	CM_RNR#030	Renewal/Re-issuance limitations	✓	d) cryptographically authenticate all sensitive renewal / re-issuance				F
8	SECURE-12.	RECOVERY AND REISSUANCE	Entities that issue credentials and tokens MUST implement methods	F	CM_RNR#040	Authentication key life	✓	Expire after 24 hours all temporary or short-term keys derived during				F
9	SECURE-12.	RECOVERY AND REISSUANCE	Entities that issue credentials and tokens MUST implement methods	F	CM_RNR#050	Record Retention	✓	Retain, securely, the record of any renewal/re-issuance process for the				F

10	SECURE-12.	RECOVERY AND REISSUANCE	Entities that issue credentials and tokens MUST implement methods	F	CM_RKY#010	Verify Requestor as Subscriber	✓	Where the Subject seeks a re-key for a) if in-person, require presentation of the Subject's own credential;	F
11	SECURE-12.	RECOVERY AND REISSUANCE	Entities that issue credentials and tokens MUST implement methods	F	CM_RKY#010	Verify Requestor as Subscriber	✓	Where the Subject seeks a re-key for b) if remote: the Subject's own credential;	F
12	SECURE-12.	RECOVERY AND REISSUANCE	Entities that issue credentials and tokens MUST implement methods	F	CM_RKY#010	Verify Requestor as Subscriber	✓	Where the Subject seeks a re-key for b) if remote: the Subject's own credential;	F
13	SECURE-12.	RECOVERY AND REISSUANCE	Entities that issue credentials and tokens MUST implement methods	F	CM_RKY#020	Re-key requests other than Subject Submit Request	✓	Re-key requests from any parties other than the Subject must not be	F
14	SECURE-12.	RECOVERY AND REISSUANCE	Entities that issue credentials and tokens MUST implement methods	F	CM_SRR#010	Submit Request	✓	Submit a request for the revocation to the Credential Issuer service	F
1	SECURE-13.	REVOCATION	Entities that issue credentials or tokens MUST have processes and	F	CM_RVP#010	Revocation procedures	✓	a) State the conditions under which revocation of an issued	F
2	SECURE-13.	REVOCATION	Entities that issue credentials or tokens MUST have processes and	F	CM_RVP#010	Revocation procedures	✓	b) State the processes by which a revocation request may be	F
3	SECURE-13.	REVOCATION	Entities that issue credentials or tokens MUST have processes and	F	CM_RVP#010	Revocation procedures	✓	c) State the persons and organizations from which a	F
4	SECURE-13.	REVOCATION	Entities that issue credentials or tokens MUST have processes and	F	CM_RVP#010	Revocation procedures	✓	d) State the validation steps that will be applied to ensure the validity	F
5	SECURE-13.	REVOCATION	Entities that issue credentials or tokens MUST have processes and	F	CM_RVP#010	Revocation procedures	✓	e) State the response time between a revocation request being	F
6	SECURE-13.	REVOCATION	Entities that issue credentials or tokens MUST have processes and	F	CM_RVP#020	Secure status notification	✓	Ensure that published credential status notification information can	F
7	SECURE-13.	REVOCATION	Entities that issue credentials or tokens MUST have processes and	F	CM_RVP#030	Revocation publication	✓	Ensure that published credential status notification is revised within	F
8	SECURE-13.	REVOCATION	Entities that issue credentials or tokens MUST have processes and	F	CM_RVP#040	Verify Revocation Identity	✓	Establish that the identity for which a revocation request is received is	F
9	SECURE-13.	REVOCATION	Entities that issue credentials or tokens MUST have processes and	F	CM_RVP#050	Revocation Records	✓	Retain a record of any revocation of a credential that is related to a	F
10	SECURE-13.	REVOCATION	Entities that issue credentials or tokens MUST have processes and	F	CM_RVP#050	Revocation Records	✓	Retain a record of any revocation of a credential that is related to a	F
11	SECURE-13.	REVOCATION	Entities that issue credentials or tokens MUST have processes and	F	CM_RVP#050	Revocation Records	✓	Retain a record of any revocation of a credential that is related to a	F
12	SECURE-13.	REVOCATION	Entities that issue credentials or tokens MUST have processes and	F	CM_RVP#050	Revocation Records	✓	Retain a record of any revocation of a credential that is related to a	F
13	SECURE-13.	REVOCATION	Entities that issue credentials or tokens MUST have processes and	F	CM_RVP#060	Record Retention	✓	Retain, securely, the record of the revocation process for a period	F
14	SECURE-13.	REVOCATION	Entities that issue credentials or tokens MUST have processes and	F	CM_RVP#060	Record Retention	✓	Retain, securely, the record of the revocation process for a period	F
15	SECURE-13.	REVOCATION	Entities that issue credentials or tokens MUST have processes and	F	CM_RVR#010	Verify revocation identity	✓	Establish that the credential for which a revocation request is	F
16	SECURE-13.	REVOCATION	Entities that issue credentials or tokens MUST have processes and	F	CM_RVR#020	Revocation reason	✓	Establish the reason for the revocation request as being sound	F
17	SECURE-13.	REVOCATION	Entities that issue credentials or tokens MUST have processes and	F	CM_RVR#030	Verify Subscriber as Revocant	✓	When the Subscriber or Subject seeks revocation of the Subject's	F
18	SECURE-13.	REVOCATION	Entities that issue credentials or tokens MUST have processes and	F	CM_RVR#030	Verify Subscriber as Revocant	✓	When the Subscriber or Subject seeks revocation of the Subject's	F
19	SECURE-13.	REVOCATION	Entities that issue credentials or tokens MUST have processes and	F	CM_RVR#030	Verify Subscriber as Revocant	✓	When the Subscriber or Subject seeks revocation of the Subject's	F
20	SECURE-13.	REVOCATION	Entities that issue credentials or tokens MUST have processes and	F	CM_RVR#040	Verify CSP as Revocant	✓	Where a CSP seeks revocation of a Subject's credential, establish that	F
21	SECURE-13.	REVOCATION	Entities that issue credentials or tokens MUST have processes and	F	CM_RVR#040	Verify CSP as Revocant	✓	Where a CSP seeks revocation of a Subject's credential, establish that	F
22	SECURE-13.	REVOCATION	Entities that issue credentials or tokens MUST have processes and	F	CM_RVR#050	Verify Legal Representative as	✓	Where the request for revocation is made by a law enforcement officer	F
23	SECURE-13.	REVOCATION	Entities that issue credentials or tokens MUST have processes and	F	CM_RVR#050	Verify Legal Representative as	✓	Where the request for revocation is made by a law enforcement officer	F
24	SECURE-13.	REVOCATION	Entities that issue credentials or tokens MUST have processes and	F	CM_RVR#050	Verify Legal Representative as	✓	Where the request for revocation is made by a law enforcement officer	F
25	SECURE-13.	REVOCATION	Entities that issue credentials or tokens MUST have processes and	F	CM_SRR#010	Submit Request	✓	Submit a request for the revocation to the Credential Issuer service	F
26	SECURE-13.	REVOCATION	Entities that issue credentials or tokens MUST have processes and	F	CM_ASS#020	Post Authentication	✓	Not authenticate credentials that have been revoked unless the time	F
1	SECURE-14.	SECURITY LOGS	Entities conducting digital identity management functions MUST log	F	CO_NUI#050	Record of User Acceptance	✓	Obtain a record (hard-copy or electronic) of the Subscriber's and	F
2	SECURE-14.	SECURITY LOGS	Entities conducting digital identity management functions MUST log	F	CO_SER#010	Security Event Logging	✓	Maintain a log of all relevant security events concerning the operation of	F
3	SECURE-14.	SECURITY LOGS	Entities conducting digital identity management functions MUST log	F	CM_SER#010	Security event logs	✓	Ensure that such audit records include:	F
4	SECURE-14.	SECURITY LOGS	Entities conducting digital identity management functions MUST log	F	CM_SER#010	Security event logs	✓	Ensure that such audit records include:	F
5	SECURE-14.	SECURITY LOGS	Entities conducting digital identity management functions MUST log	F	CM_SER#010	Security event logs	✓	Ensure that such audit records include:	F
6	SECURE-14.	SECURITY LOGS	Entities conducting digital identity management functions MUST log	F	CM_SER#010	Security event logs	✓	Ensure that such audit records include:	F
7	SECURE-14.	SECURITY LOGS	Entities conducting digital identity management functions MUST log	F	CM_SER#010	Security event logs	✓	Ensure that such audit records include:	F

[illegible]

16	SECURE-3.	SECURE-3. CREDENTIAL REPRODUCTION	Entities that issue or manage credentials and tokens MUST	F/P	CM_VAS#060	No assertion manufacture/modificatio	✓	✓	✓	✓	Ensure that it is impractical to manufacture an assertion or	c) Creating an assertion reference which has a minimum of 64 bits of			F/P
17	SECURE-3.	SECURE-3. CREDENTIAL REPRODUCTION	Entities that issue or manage credentials and tokens MUST	F/P	CM_VAS#060	No assertion manufacture/modificatio	✓	✓	✓	✓	Ensure that it is impractical to manufacture an assertion or	d) Sending the assertion over a protected channel during a mutually-			F/P
18	SECURE-3.	SECURE-3. CREDENTIAL REPRODUCTION	Entities that issue or manage credentials and tokens MUST	F/P	CM_VAS#070	Assertion protections		✓	✓	✓	Provide protection of assertion-related data such that:	a) both assertions and assertion references are protected against			F/P
19	SECURE-3.	SECURE-3. CREDENTIAL REPRODUCTION	Entities that issue or manage credentials and tokens MUST	F/P	CM_VAS#070	Assertion protections		✓	✓	✓	Provide protection of assertion-related data such that:	b) assertions are also protected against redirection:			F/P
20	SECURE-3.	SECURE-3. CREDENTIAL REPRODUCTION	Entities that issue or manage credentials and tokens MUST	F/P	CM_VAS#070	Assertion protections		✓	✓	✓	Provide protection of assertion-related data such that:	c) assertions, assertion references and session cookies used for			F/P
1	SECURE-4.	PROTECTION CREDENTIAL	Entities that issue or manage credentials and tokens MUST	F/P	CO_SCO#010	Secure remote communications		✓	✓	✓	If the specific service components are located remotely from and	a) implementing mutually-authenticated protected sessions: or			F/P
2	SECURE-4.	PROTECTION CREDENTIAL	Entities that issue or manage credentials and tokens MUST	F/P	CO_SCO#010	Secure remote communications		✓	✓	✓	If the specific service components are located remotely from and	b) time-stamped or sequenced messages signed by their source and			F/P
3	SECURE-4.	PROTECTION CREDENTIAL	Entities that issue or manage credentials and tokens MUST	F/P	CO_SCO#020	Limited access to shared secrets			✓	✓	Ensure that: These roles should be defined and documented by the CSP	a) access to shared secrets shall be subject to discretionary controls			F/P
4	SECURE-4.	PROTECTION CREDENTIAL	Entities that issue or manage credentials and tokens MUST	F/P	CO_SCO#020	Limited access to shared secrets			✓	✓	Ensure that: These roles should be defined and documented by the CSP	b) stored shared secrets are encrypted such that:	140-2		F/P
5	SECURE-4.	PROTECTION CREDENTIAL	Entities that issue or manage credentials and tokens MUST	F/P	CO_SCO#020	Limited access to shared secrets			✓	✓	Ensure that: These roles should be defined and documented by the CSP	b) stored shared secrets are encrypted such that:	13 or 4		F/P
6	SECURE-4.	PROTECTION CREDENTIAL	Entities that issue or manage credentials and tokens MUST	F/P	CO_SCO#020	Limited access to shared secrets			✓	✓	Ensure that: These roles should be defined and documented by the CSP	b) stored shared secrets are encrypted such that:	100/4		F/P
7	SECURE-4.	PROTECTION CREDENTIAL	Entities that issue or manage credentials and tokens MUST	F/P	CO_SCO#020	Limited access to shared secrets			✓	✓	Ensure that: These roles should be defined and documented by the CSP	c) any long-term (i.e., not session) shared secrets are revealed only to	44-41		F/P
8	SECURE-4.	PROTECTION CREDENTIAL	Entities that issue or manage credentials and tokens MUST	F/P	CM_CTR#020	Protocol threat risk assessment and controls			✓	✓	Account for at least the following protocol threats in its risk	a) password guessing, showing that there is sufficient entropy:			F/P
9	SECURE-4.	PROTECTION CREDENTIAL	Entities that issue or manage credentials and tokens MUST	F/P	CM_CTR#020	Protocol threat risk assessment and controls			✓	✓	Account for at least the following protocol threats in its risk	b) message replay, showing that it is impractical:			F/P
10	SECURE-4.	PROTECTION CREDENTIAL	Entities that issue or manage credentials and tokens MUST	F/P	CM_CTR#020	Protocol threat risk assessment and controls			✓	✓	Account for at least the following protocol threats in its risk	c) eavesdropping, showing that it is impractical:			F/P
11	SECURE-4.	PROTECTION CREDENTIAL	Entities that issue or manage credentials and tokens MUST	F/P	CM_CTR#020	Protocol threat risk assessment and controls			✓	✓	Account for at least the following protocol threats in its risk	d) relying party (verifier) impersonation, showing that it is			F/P
12	SECURE-4.	PROTECTION CREDENTIAL	Entities that issue or manage credentials and tokens MUST	F/P	CM_CTR#020	Protocol threat risk assessment and controls			✓	✓	Account for at least the following protocol threats in its risk	e) man-in-the-middle attack;			F/P
13	SECURE-4.	PROTECTION CREDENTIAL	Entities that issue or manage credentials and tokens MUST	F/P	CM_CTR#020	Protocol threat risk assessment and controls			✓	✓	Account for at least the following protocol threats in its risk	f) session hijacking, showing that it is impractical.			F/P
14	SECURE-4.	PROTECTION CREDENTIAL	Entities that issue or manage credentials and tokens MUST	F/P	CM_CTR#030	System Threat Risk Assessment & Controls	✓	✓	✓	✓	Account for the following system threats and apply appropriate	a) the introduction of malicious code;			F/P
15	SECURE-4.	PROTECTION CREDENTIAL	Entities that issue or manage credentials and tokens MUST	F/P	CM_CTR#030	System Threat Risk Assessment & Controls	✓	✓	✓	✓	Account for the following system threats and apply appropriate	b) compromised authentication arising from insider action:			F/P
16	SECURE-4.	PROTECTION CREDENTIAL	Entities that issue or manage credentials and tokens MUST	F/P	CM_CTR#030	System Threat Risk Assessment & Controls	✓	✓	✓	✓	Account for the following system threats and apply appropriate	c) out-of-band attacks by both users and system operators (e.g., the			F/P
17	SECURE-4.	PROTECTION CREDENTIAL	Entities that issue or manage credentials and tokens MUST	F/P	CM_CTR#030	System Threat Risk Assessment & Controls	✓	✓	✓	✓	Account for the following system threats and apply appropriate	d) spoofing of system elements/applications:			F/P
18	SECURE-4.	PROTECTION CREDENTIAL	Entities that issue or manage credentials and tokens MUST	F/P	CM_CTR#030	System Threat Risk Assessment & Controls	✓	✓	✓	✓	Account for the following system threats and apply appropriate	e) malfeasance on the part of subscribers and subjects:			F/P
19	SECURE-4.	PROTECTION CREDENTIAL	Entities that issue or manage credentials and tokens MUST	F/P	CM_CTR#030	System Threat Risk Assessment & Controls	✓	✓	✓	✓	Account for the following system threats in its risk assessment and	f) intrusions leading to information theft.			F/P
20	SECURE-4.	PROTECTION CREDENTIAL	Entities that issue or manage credentials and tokens MUST	F/P	CM_CTR#040	Specified Service's Key Management -	✓	✓	✓	✓	Specify and observe procedures and processes for the generation.	a) the physical security of the environment:			F/P
21	SECURE-4.	PROTECTION CREDENTIAL	Entities that issue or manage credentials and tokens MUST	F/P	CM_CTR#040	Specified Service's Key Management -	✓	✓	✓	✓	Specify and observe procedures and processes for the generation.	b) access control procedures limiting access to the minimum number of			F/P
22	SECURE-4.	PROTECTION CREDENTIAL	Entities that issue or manage credentials and tokens MUST	F/P	CM_CTR#040	Specified Service's Key Management -	✓	✓	✓	✓	Specify and observe procedures and processes for the generation.	c) public-key publication mechanisms:			F/P
23	SECURE-4.	PROTECTION CREDENTIAL	Entities that issue or manage credentials and tokens MUST	F/P	CM_CTR#040	Specified Service's Key Management -	✓	✓	✓	✓	Specify and observe procedures and processes for the generation.	d) application of controls deemed necessary as a result of the service's			F/P
24	SECURE-4.	PROTECTION CREDENTIAL	Entities that issue or manage credentials and tokens MUST	F/P	CM_CTR#040	Specified Service's Key Management -	✓	✓	✓	✓	Specify and observe procedures and processes for the generation.	e) destruction of expired or compromised private keys in a			F/P
25	SECURE-4.	PROTECTION CREDENTIAL	Entities that issue or manage credentials and tokens MUST	F/P	CM_CTR#040	Specified Service's Key Management -	✓	✓	✓	✓	Specify and observe procedures and processes for the generation.	f) applicable cryptographic module security requirements, quoting FIPS			F/P
1	SECURE-6.	UNIQUENESS CREDENTIAL	Entities that issue or manage credentials MUST ensure that each	F/P	CM_CTR#040	Specified Service's Key Management -	✓	✓	✓	✓	Specify and observe procedures and processes for the generation.	a) the physical security of the environment:			F/P
2	SECURE-6.	UNIQUENESS CREDENTIAL	Entities that issue or manage credentials MUST ensure that each	F/P	CM_CTR#040	Specified Service's Key Management -	✓	✓	✓	✓	Specify and observe procedures and processes for the generation.	b) access control procedures limiting access to the minimum number of			F/P
3	SECURE-6.	UNIQUENESS CREDENTIAL	Entities that issue or manage credentials MUST ensure that each	F/P	CM_CTR#040	Specified Service's Key Management -	✓	✓	✓	✓	Specify and observe procedures and processes for the generation.	c) public-key publication mechanisms:			F/P
4	SECURE-6.	UNIQUENESS CREDENTIAL	Entities that issue or manage credentials MUST ensure that each	F/P	CM_CTR#040	Specified Service's Key Management -	✓	✓	✓	✓	Specify and observe procedures and processes for the generation.	d) application of controls deemed necessary as a result of the service's			F/P
5	SECURE-6.	UNIQUENESS CREDENTIAL	Entities that issue or manage credentials MUST ensure that each	F/P	CM_CTR#040	Specified Service's Key Management -	✓	✓	✓	✓	Specify and observe procedures and processes for the generation.	e) destruction of expired or compromised private keys in a			F/P
6	SECURE-6.	UNIQUENESS CREDENTIAL	Entities that issue or manage credentials MUST ensure that each	F/P	CM_CTR#040	Specified Service's Key Management -	✓	✓	✓	✓	Specify and observe procedures and processes for the generation.	f) applicable cryptographic module security requirements, quoting FIPS			F/P
7	SECURE-6.	UNIQUENESS CREDENTIAL	Entities that issue or manage credentials MUST ensure that each	F/P	ID_POL#010	Unique service identity	✓	✓	✓	✓	Ensure that a unique identity is attributed to the specific service.				F/P
8	SECURE-6.	UNIQUENESS CREDENTIAL	Entities that issue or manage credentials MUST ensure that each	F/P	ID_POL#020	Unique Subject identity	✓	✓	✓	✓	Ensure that each applicant's identity is unique within the service's				F/P

9	SECURE-6.	CREDENTIAL UNIQUENESS	Entities that issue or manage credentials MUST ensure that each	F/P	ID_IDC#010	Authenticate Original Credential	✓	✓	✓	Prior to issuing any derived credential the original credential on	a) authenticated by a source trusted by the CSP as being valid and un-			F/P
10	SECURE-6.	CREDENTIAL UNIQUENESS	Entities that issue or manage credentials MUST ensure that each	F/P	ID_IDC#010	Authenticate Original Credential	✓	✓	✓	Prior to issuing any derived credential the original credential on	c) issued in the same name as that which the Applicant is claiming;			F/P
11	SECURE-6.	CREDENTIAL UNIQUENESS	Entities that issue or manage credentials MUST ensure that each	F/P	ID_IDC#010	Authenticate Original Credential		✓	✓	Prior to issuing any derived credential the original credential on	b) issued at Assurance Level 4;			F/P
12	SECURE-6.	CREDENTIAL UNIQUENESS	Entities that issue or manage credentials MUST ensure that each	F/P	ID_IDC#010	Authenticate Original Credential			✓	Prior to issuing any derived credential the original credential on	d) proven to be in the possession and under the control of the			F/P
13	SECURE-6.	CREDENTIAL UNIQUENESS	Entities that issue or manage credentials MUST ensure that each	F/P	ID_IDC#020	Record Original Credential			✓	Record the details of the original credential, the biometric sample				F/P
14	SECURE-6.	CREDENTIAL UNIQUENESS	Entities that issue or manage credentials MUST ensure that each	F/P	ID_IDC#030	Issue Derived Credential			✓	Only issue the derived credential in-person after performing biometric				F/P
15	SECURE-6.	CREDENTIAL UNIQUENESS	Entities that issue or manage credentials MUST ensure that each	F/P	CM_CRN#030	Credential uniqueness	✓	✓	✓	Allow the Subject to select a credential (e.g., UserID) that is				F/P
1	SECURE-7.	TOKEN CONTROL	Entities that authenticate a USER MUST employ industry-accepted	F/P	CO_SCO#020	Limited access to shared secrets			✓	Ensure that: These roles should be defined and documented by the CSP	a) access to shared secrets shall be subject to discretionary controls			F/P
2	SECURE-7.	TOKEN CONTROL	Entities that authenticate a USER MUST employ industry-accepted	F/P	CO_SCO#020	Limited access to shared secrets			✓	Ensure that: These roles should be defined and documented by the CSP	b) stored shared secrets are encrypted such that:			F/P
3	SECURE-7.	TOKEN CONTROL	Entities that authenticate a USER MUST employ industry-accepted	F/P	CO_SCO#020	Limited access to shared secrets			✓	Ensure that: These roles should be defined and documented by the CSP	b) stored shared secrets are encrypted such that:			F/P
4	SECURE-7.	TOKEN CONTROL	Entities that authenticate a USER MUST employ industry-accepted	F/P	CO_SCO#020	Limited access to shared secrets			✓	Ensure that: These roles should be defined and documented by the CSP	b) stored shared secrets are encrypted such that:			F/P
5	SECURE-7.	TOKEN CONTROL	Entities that authenticate a USER MUST employ industry-accepted	F/P	CO_SCO#020	Limited access to shared secrets			✓	Ensure that: These roles should be defined and documented by the CSP	c) any long-term (i.e., not session) shared secrets are revealed only to			F/P
6	SECURE-7.	TOKEN CONTROL	Entities that authenticate a USER MUST employ industry-accepted	F/P	CM_CRD#010	Notify Subject of Credential Issuance			✓	Notify the Subject of the credential's issuance and, if necessary, confirm	a) sending notice to the address of record confirmed during identity			F/P
7	SECURE-7.	TOKEN CONTROL	Entities that authenticate a USER MUST employ industry-accepted	F/P	CM_CRD#010	Notify Subject of Credential Issuance			✓	Notify the Subject of the credential's issuance and, if necessary, confirm	b) unless the Subject presented with a private key, issuing the hardware			F/P
8	SECURE-7.	TOKEN CONTROL	Entities that authenticate a USER MUST employ industry-accepted	F/P	CM_CRD#010	Notify Subject of Credential Issuance			✓	Notify the Subject of the credential's issuance and, if necessary, confirm	c) issuing the certificate to the Subject over a separate channel in a			F/P
9	SECURE-7.	TOKEN CONTROL	Entities that authenticate a USER MUST employ industry-accepted	F/P	CM_CRD#015	Confirm Applicant's identity (in person)			✓	Prior to delivering the credential, require the Applicant to identify				F/P
10	SECURE-7.	TOKEN CONTROL	Entities that authenticate a USER MUST employ industry-accepted	F/P	CM_CRD#020	Subject's acknowledgement			✓	Receive acknowledgement of receipt of the hardware token before				F/P
11	SECURE-7.	TOKEN CONTROL	Entities that authenticate a USER MUST employ industry-accepted	F/P	CM_ASS#018	Ensure token validity			✓	Ensure that tokens are either still valid or have been issued within the				F/P
1	SECURE-9.	AUTHENTICATION RISK ASSESSMENT	Entities MUST have a risk assessment process in place for the	F/P	CO_ISM#030	Risk Management			✓	Demonstrate a risk management methodology that adequately				F/P
1	SECURE-10.	UPTIME	Entities that provide and conduct digital identity management	F/P	CO_ISM#040	Continuity of Operations Plan			✓	Have and keep updated a continuity of operations plan that covers				F/P
1	SECURE-11.	KEY MANAGEMENT	Entities that use cryptographic solutions as part of identity	F/P	CO_SCO#010	Secure remote communications		✓	✓	If the specific service components are located remotely from and	a) implementing mutually-authenticated protected sessions: or			F/P
2	SECURE-11.	KEY MANAGEMENT	Entities that use cryptographic solutions as part of identity	F/P	CO_SCO#010	Secure remote communications		✓	✓	If the specific service components are located remotely from and	b) time-stamped or sequenced messages signed by their source and			F/P
3	SECURE-11.	KEY MANAGEMENT	Entities that use cryptographic solutions as part of identity	F/P	CM_CTR#040	Specified Service's Key Management -		✓	✓	Specify and observe procedures and processes for the generation.	a) the physical security of the environment;			F/P
4	SECURE-11.	KEY MANAGEMENT	Entities that use cryptographic solutions as part of identity	F/P	CM_CTR#040	Specified Service's Key Management -		✓	✓	Specify and observe procedures and processes for the generation.	b) access control procedures limiting access to the minimum number of			F/P
5	SECURE-11.	KEY MANAGEMENT	Entities that use cryptographic solutions as part of identity	F/P	CM_CTR#040	Specified Service's Key Management -		✓	✓	Specify and observe procedures and processes for the generation.	c) public-key publication mechanisms;			F/P
6	SECURE-11.	KEY MANAGEMENT	Entities that use cryptographic solutions as part of identity	F/P	CM_CTR#040	Specified Service's Key Management -		✓	✓	Specify and observe procedures and processes for the generation.	d) application of controls deemed necessary as a result of the service's			F/P
7	SECURE-11.	KEY MANAGEMENT	Entities that use cryptographic solutions as part of identity	F/P	CM_CTR#040	Specified Service's Key Management -		✓	✓	Specify and observe procedures and processes for the generation.	e) destruction of expired or compromised private keys in a			F/P
8	SECURE-11.	KEY MANAGEMENT	Entities that use cryptographic solutions as part of identity	F/P	CM_CTR#040	Specified Service's Key Management -		✓	✓	Specify and observe procedures and processes for the generation.	f) applicable cryptographic module security requirements, quoting FIPS			F/P
9	SECURE-11.	KEY MANAGEMENT	Entities that use cryptographic solutions as part of identity	F/P	CM_STS#020	Stored Secret Encryption			✓	Encrypt such shared secret files so that:	a) the encryption key for the shared secret file is encrypted under			F/P
10	SECURE-11.	KEY MANAGEMENT	Entities that use cryptographic solutions as part of identity	F/P	CM_STS#020	Stored Secret Encryption			✓	Encrypt such shared secret files so that:	b) the shared secret file is decrypted only as immediately			F/P
11	SECURE-11.	KEY MANAGEMENT	Entities that use cryptographic solutions as part of identity	F/P	CM_STS#020	Stored Secret Encryption			✓	Encrypt such shared secret files so that:	c) shared secrets are protected as a key within the boundary of a			F/P
12	SECURE-11.	KEY MANAGEMENT	Entities that use cryptographic solutions as part of identity	F/P	CM_STS#020	Stored Secret Encryption			✓	Encrypt such shared secret files so that:	d) shared secrets are split by an "n from m" cryptographic secret			F/P
13	SECURE-11.	KEY MANAGEMENT	Entities that use cryptographic solutions as part of identity	F/P	CM_SKP#010	Key generation by Specified Service			✓	If the specified service generates the Subject's keys:	a) use a FIPS AL140-2 (FIPSAL140-2) compliant algorithm.			F/P
14	SECURE-11.	KEY MANAGEMENT	Entities that use cryptographic solutions as part of identity	F/P	CM_SKP#010	Key generation by Specified Service			✓	If the specified service generates the Subject's keys:	b) only create keys of a key length and for use with a			F/P
15	SECURE-11.	KEY MANAGEMENT	Entities that use cryptographic solutions as part of identity	F/P	CM_SKP#010	Key generation by Specified Service			✓	If the specified service generates the Subject's keys:	c) generate and store the keys securely until delivery to and			F/P
16	SECURE-11.	KEY MANAGEMENT	Entities that use cryptographic solutions as part of identity	F/P	CM_SKP#010	Key generation by Specified Service			✓	If the specified service generates the Subject's keys:	d) deliver the Subject's private key in a manner that ensures that the			F/P
17	SECURE-11.	KEY MANAGEMENT	Entities that use cryptographic solutions as part of identity	F/P	CM_SKP#020	Key generation by Subject			✓	If the Subject generates and presents its own keys, obtain the	a) used a FIPS AL140-2 (FIPSAL140-2) compliant algorithm.			F/P
18	SECURE-11.	KEY MANAGEMENT	Entities that use cryptographic solutions as part of identity	F/P	CM_SKP#020	Key generation by Subject			✓	If the Subject generates and presents its own keys, obtain the	b) created keys of a key length and for use with a FIPS AL140-2			F/P

1	USABLE-3.	PLAIN LANGUAGE	Information presented to USERS in digital identity management	F/P	CO_NUI#010	General Service Definition	X	✓	✓	✓	Make available to the intended user community a Service Definition that			F/P
2	USABLE-3.	PLAIN LANGUAGE	Information presented to USERS in digital identity management	F/P	CO_NUI#030	Due notification		✓	✓	✓	Have in place and follow appropriate policy and procedures to ensure that it			F/P
1	INTEROP-2.	THIRD-PARTY CREDENTIALS	Entities who issue credentials or assertions MUST issue them using	P	CM_CPP#020	Certificate Policy/Certification Certificate		✓		✓	Include in its Service Definition its full Certificate Policy and the	a) applicable OIDs for each certificate type issued;		P
2	INTEROP-2.	THIRD-PARTY CREDENTIALS	Entities who issue credentials or assertions MUST issue them using	P	CM_CPP#020	Certificate Policy/Certification Certificate		✓		✓	Include in its Service Definition its full Certificate Policy and the	b) how users may subscribe to the service/apply for certificates, and		P
3	INTEROP-2.	THIRD-PARTY CREDENTIALS	Entities who issue credentials or assertions MUST issue them using	P	CM_CPP#020	Certificate Policy/Certification Certificate		✓		✓	Include in its Service Definition its full Certificate Policy and the	c) if users present their own keys, how they will be required to		P
4	INTEROP-2.	THIRD-PARTY CREDENTIALS	Entities who issue credentials or assertions MUST issue them using	P	CM_CPP#020	Certificate Policy/Certification Certificate		✓		✓	Include in its Service Definition its full Certificate Policy and the	d) if users' keys are generated for them, how the private keys will be		P
5	INTEROP-2.	THIRD-PARTY CREDENTIALS	Entities who issue credentials or assertions MUST issue them using	P	CM_CPP#020	Certificate Policy/Certification Certificate		✓		✓	Include in its Service Definition its full Certificate Policy and the	e) how Subjects acknowledge receipt of tokens and credentials and what		P
6	INTEROP-2.	THIRD-PARTY CREDENTIALS	Entities who issue credentials or assertions MUST issue them using	P	CM_CPP#020	Certificate Policy/Certification Certificate		✓		✓	Include in its Service Definition its full Certificate Policy and the	f) how certificates may be renewed, re-keyed, modified, revoked, and		P
7	INTEROP-2.	THIRD-PARTY CREDENTIALS	Entities who issue credentials or assertions MUST issue them using	P	CM_CPP#020	Certificate Policy/Certification Certificate		✓		✓	Include in its Service Definition its full Certificate Policy and the	g) what actions a Subject must take to terminate their subscription.		P
8	INTEROP-2.	THIRD-PARTY CREDENTIALS	Entities who issue credentials or assertions MUST issue them using	P	CM_CRN#035	Convey credential	✓	✓	✓	✓	Be capable of conveying the unique identity information associated with			P
9	INTEROP-2.	THIRD-PARTY CREDENTIALS	Entities who issue credentials or assertions MUST issue them using	P	CM_CSM#030	Revision to Published Status		✓	✓	✓	Process authenticated requests for revised status information and have			P
10	INTEROP-2.	THIRD-PARTY CREDENTIALS	Entities who issue credentials or assertions MUST issue them using	P	CM_CSM#040	Status Information Availability			✓	✓	Provide, with 99% availability, a secure automated mechanism to			P
11	INTEROP-2.	THIRD-PARTY CREDENTIALS	Entities who issue credentials or assertions MUST issue them using	P	CM_CSM#050	Inactive Credentials		✓	✓	✓	Disable any credential that has not been successfully used for			P
1	INTEROP-4.	STANDARDIZED DATA EXCHANGES	Entities that conduct digital identity management functions MUST use	P	CM_CPP#020	Certificate Policy/Certification Certificate				✓	Include in its Service Definition its full Certificate Policy and the	a) applicable OIDs for each certificate type issued;		P
2	INTEROP-4.	STANDARDIZED DATA EXCHANGES	Entities that conduct digital identity management functions MUST use	P	CM_CPP#020	Certificate Policy/Certification Certificate				✓	Include in its Service Definition its full Certificate Policy and the	b) how users may subscribe to the service/apply for certificates, and		P
3	INTEROP-4.	STANDARDIZED DATA EXCHANGES	Entities that conduct digital identity management functions MUST use	P	CM_CPP#020	Certificate Policy/Certification Certificate				✓	Include in its Service Definition its full Certificate Policy and the	c) if users present their own keys, how they will be required to		P
4	INTEROP-4.	STANDARDIZED DATA EXCHANGES	Entities that conduct digital identity management functions MUST use	P	CM_CPP#020	Certificate Policy/Certification Certificate				✓	Include in its Service Definition its full Certificate Policy and the	d) if users' keys are generated for them, how the private keys will be		P
5	INTEROP-4.	STANDARDIZED DATA EXCHANGES	Entities that conduct digital identity management functions MUST use	P	CM_CPP#020	Certificate Policy/Certification Certificate				✓	Include in its Service Definition its full Certificate Policy and the	e) how Subjects acknowledge receipt of tokens and credentials and what		P
6	INTEROP-4.	STANDARDIZED DATA EXCHANGES	Entities that conduct digital identity management functions MUST use	P	CM_CPP#020	Certificate Policy/Certification Certificate				✓	Include in its Service Definition its full Certificate Policy and the	f) how certificates may be renewed, re-keyed, modified, revoked, and		P
7	INTEROP-4.	STANDARDIZED DATA EXCHANGES	Entities that conduct digital identity management functions MUST use	P	CM_CPP#020	Certificate Policy/Certification Certificate				✓	Include in its Service Definition its full Certificate Policy and the	g) what actions a Subject must take to terminate their subscription.		P
1	INTEROP-5.	DOCUMENTED PROCESSES	Entities MUST employ documented business policies and processes in	P	CO_NUI#010	General Service Definition	X	✓	✓	✓	Make available to the intended user community a Service Definition that			P
2	INTEROP-5.	DOCUMENTED PROCESSES	Entities MUST employ documented business policies and processes in	P	CO_NUI#050	Record of User Acceptance		✓	✓	✓	Obtain a record (hard-copy or electronic) of the Subscriber's and			P
3	INTEROP-5.	DOCUMENTED PROCESSES	Entities MUST employ documented business policies and processes in	P	ID_POL#030	Published Proofing Policy		✓	✓	✓	Make available the Identity Proofing Policy under which it verifies the			P
1	INTEROP-6.	THIRD-PARTY COMPLIANCE	Entities that act as THIRD-PARTY service providers for another entity.	P	CO_ESC#010	Contracted policies and procedures		✓	✓	✓	Where the enterprise uses external suppliers for specific packaged			P
2	INTEROP-6.	THIRD-PARTY COMPLIANCE	Entities that act as THIRD-PARTY service providers for another entity.	P	CO_ESC#020	Visibility of contracted parties		✓	✓	✓	Where the enterprise uses external suppliers for specific packaged			P
1	INTEROP-7.	USER REDRESS	Entities MUST provide effective mechanisms for redress of	P	CO_NUI#040	User Acceptance		✓	✓	✓	Require Subscribers and Subjects to:	c) always provide full and correct responses to requests for		P
1	PRIVACY-1.	DATA MINIMIZATION	Entities MUST limit the collection, use, transmission and storage of	P	CO_ESM#030	Legal & Contractual compliance		✓	✓	✓	Demonstrate that it understands and complies with any legal			P
1	PRIVACY-6.	USAGE NOTICE	Entities MUST provide concise, meaningful, and timely	P	CO_NUI#010	General Service Definition	X	✓	✓	✓	Make available to the intended user community a Service Definition that			P
2	PRIVACY-6.	USAGE NOTICE	Entities MUST provide concise, meaningful, and timely	P	CO_NUI#020	Service Definition inclusions		✓	✓	✓	Make available a Service Definition for the specified service containing	a) Privacy, Identity Proofing & Verification, Renewal/Re-issuance,		P
3	PRIVACY-6.	USAGE NOTICE	Entities MUST provide concise, meaningful, and timely	P	CO_NUI#020	Service Definition inclusions		✓	✓	✓	Make available a Service Definition for the specified service containing	b) the country in or the legal jurisdiction under which the service		P
4	PRIVACY-6.	USAGE NOTICE	Entities MUST provide concise, meaningful, and timely	P	CO_NUI#020	Service Definition inclusions		✓	✓	✓	Make available a Service Definition for the specified service containing	c) if different to the above, the legal jurisdiction under which Subscriber		P
5	PRIVACY-6.	USAGE NOTICE	Entities MUST provide concise, meaningful, and timely	P	CO_NUI#020	Service Definition inclusions		✓	✓	✓	Make available a Service Definition for the specified service containing	d) applicable legislation with which the service complies;		P
6	PRIVACY-6.	USAGE NOTICE	Entities MUST provide concise, meaningful, and timely	P	CO_NUI#020	Service Definition inclusions		✓	✓	✓	Make available a Service Definition for the specified service containing	e) obligations incumbent upon the CSP;		P
7	PRIVACY-6.	USAGE NOTICE	Entities MUST provide concise, meaningful, and timely	P	CO_NUI#020	Service Definition inclusions		✓	✓	✓	Make available a Service Definition for the specified service containing	f) obligations incumbent upon each class of user of the service, e.a.		P
8	PRIVACY-6.	USAGE NOTICE	Entities MUST provide concise, meaningful, and timely	P	CO_NUI#020	Service Definition inclusions		✓	✓	✓	Make available a Service Definition for the specified service containing	g) notifications and guidance for relying parties, especially in respect		P
9	PRIVACY-6.	USAGE NOTICE	Entities MUST provide concise, meaningful, and timely	P	CO_NUI#020	Service Definition inclusions		✓	✓	✓	Make available a Service Definition for the specified service containing	h) statement of warranties;		P
10	PRIVACY-6.	USAGE NOTICE	Entities MUST provide concise, meaningful, and timely	P	CO_NUI#020	Service Definition inclusions		✓	✓	✓	Make available a Service Definition for the specified service containing	i) statement of liabilities toward both Subjects and Relying Parties;		P
11	PRIVACY-6.	USAGE NOTICE	Entities MUST provide concise, meaningful, and timely	P	CO_NUI#020	Service Definition inclusions		✓	✓	✓	Make available a Service Definition for the specified service containing	j) procedures for notification of changes to terms and conditions;		P

12	PRIVACY-6.	USAGE NOTICE	Entities MUST provide concise, meaningful, and timely	P	CO_NUI#020	Service Definition inclusions	✓	✓	✓	Make available a Service Definition for the specified service containing	k) steps the CSP will take in the event that it chooses or is obliged to			P
13	PRIVACY-6.	USAGE NOTICE	Entities MUST provide concise, meaningful, and timely	P	CO_NUI#020	Service Definition inclusions	✓	✓	✓	Make available a Service Definition for the specified service containing	l) availability of the specified service			P
14	PRIVACY-6.	USAGE NOTICE	Entities MUST provide concise, meaningful, and timely	P	CO_NUI#030	Due notification	✓	✓	✓	Have in place and follow appropriate policy and procedures to ensure	per se and of its help desk facility.			P
15	PRIVACY-6.	USAGE NOTICE	Entities MUST provide concise, meaningful, and timely	P	CO_NUI#040	User Acceptance	✓	✓	✓	Require Subscribers and Subjects to:	a) indicate, prior to receiving service, that they have read and accept the			P
16	PRIVACY-6.	USAGE NOTICE	Entities MUST provide concise, meaningful, and timely	P	CO_NUI#040	User Acceptance	✓	✓	✓	Require Subscribers and Subjects to:	b) at periodic intervals, determined by significant service provision			P
17	PRIVACY-6.	USAGE NOTICE	Entities MUST provide concise, meaningful, and timely	P	CO_NUI#040	User Acceptance	✓	✓	✓	Require Subscribers and Subjects to:	c) always provide full and correct responses to requests for			P
18	PRIVACY-6.	USAGE NOTICE	Entities MUST provide concise, meaningful, and timely	P	ID_POL#030	Published Proofing Policy		✓	✓	✓	Make available the Identity Proofing Policy under which it verifies the			P
1	PRIVACY-14.	DATA RETENTION AND DISPOSAL	Entities MUST limit the retention of personal information to the time	P	CO_ESM#050	Data Retention and Protection	✓	✓	✓	Specifically set out and demonstrate that it understands and complies				P
2	PRIVACY-14.	DATA RETENTION AND DISPOSAL	Entities MUST limit the retention of personal information to the time	P	CO_ESM#055	Termination provisions	✓	✓	✓	Define the practices in place for the protection of Subjects' private and				P
1	USABLE-5.	ACCESSIBILITY	All digital identity management functions MUST make reasonable	P	CO_ESM#030	Legal & Contractual compliance	✓	✓	✓	Demonstrate that it understands and complies with any legal				P
1	USABLE-7.	USER REQUESTS	Wherever public open STANDARDS or legal requirements exist for	P	CO_ESM#030	Legal & Contractual compliance	✓	✓	✓	Demonstrate that it understands and complies with any legal				P
1	PRIVACY-12.	ANONYMITY	Wherever feasible, entities MUST utilize identity systems and	NE	ID_POL#010	Unique service identity	ü	ü	ü	ü	Ensure that a unique identity is attributed to the specific service.			NE
2	PRIVACY-12.	ANONYMITY	Wherever feasible, entities MUST utilize identity systems and	NE	ID_POL#020	Unique Subject identity	ü	ü	ü	ü	Ensure that each applicant's identity is unique within the			NE
3	PRIVACY-12.	ANONYMITY	Wherever feasible, entities MUST utilize identity systems and	NE	CM_CRN#090	Nature of Subject	ü	ü			Record the nature of the Subject of the credential (which must			NE
4	PRIVACY-12.	ANONYMITY	Wherever feasible, entities MUST utilize identity systems and	NE	CM_VAS#040	No pseudonyms	ü	ü			Create assertions which indicate only verified Subscriber names in			NE
1	PRIVACY-15.	ATTRIBUTE SEGREGATION	Wherever feasible, identifier data MUST be segregated from	NE	CM_CRN#090	Nature of Subject	ü	ü			Record the nature of the Subject of the credential (which must			NE
1	SECURE-8.	MULTIFACTOR AUTHENTICATION	Entities that authenticate a USER MUST offer authentication	NE	ID_IPV#010	Required evidence	ü			ü	Ensure that the applicant is in possession of:	a) a primary Government Picture ID document that bears a	account	NE
2	SECURE-8.	MULTIFACTOR AUTHENTICATION	Entities that authenticate a USER MUST offer authentication	NE	ID_IPV#010	Required evidence	ü			ü	Ensure that the applicant is in possession of:	a) a primary Government Picture ID document that bears a	utility	NE
3	SECURE-8.	MULTIFACTOR AUTHENTICATION	Entities that authenticate a USER MUST offer authentication	NE	ID_IPV#030	Evidence checks – primary ID	ü			ü	Ensure that the presented document:	a) appears to be a genuine document properly issued by the	y	NE
4	SECURE-8.	MULTIFACTOR AUTHENTICATION	Entities that authenticate a USER MUST offer authentication	NE	ID_IPV#030	Evidence checks – primary ID	ü			ü	Ensure that the presented document:	b) bears a photographic image of the holder which matches that of		NE
5	SECURE-8.	MULTIFACTOR AUTHENTICATION	Entities that authenticate a USER MUST offer authentication	NE	ID_IPV#030	Evidence checks – primary ID	ü			ü	Ensure that the presented document:	c) is electronically verified by a record check with the specified	records and other	NE
6	SECURE-8.	MULTIFACTOR AUTHENTICATION	Entities that authenticate a USER MUST offer authentication	NE	ID_IPV#030	Evidence checks – primary ID	ü			ü	Ensure that the presented document:	c) is electronically verified by a record check with the specified		NE
7	SECURE-8.	MULTIFACTOR AUTHENTICATION	Entities that authenticate a USER MUST offer authentication	NE	ID_IPV#030	Evidence checks – primary ID	ü			ü	Ensure that the presented document:	d) provides all reasonable certainty, at AL4, that the identity		NE
8	SECURE-8.	MULTIFACTOR AUTHENTICATION	Entities that authenticate a USER MUST offer authentication	NE	ID_IPV#040	Evidence checks – secondary ID	✓			ü	Ensure that the presented document meets the following conditions:	a) If it is secondary Government Picture ID:	the claim holder with the records with and other properly telephone	NE
9	SECURE-8.	MULTIFACTOR AUTHENTICATION	Entities that authenticate a USER MUST offer authentication	NE	ID_IPV#040	Evidence checks – secondary ID	✓			ü	Ensure that the presented document meets the following conditions:	a) If it is secondary Government Picture ID:		NE
10	SECURE-8.	MULTIFACTOR AUTHENTICATION	Entities that authenticate a USER MUST offer authentication	NE	ID_IPV#040	Evidence checks – secondary ID	✓			ü	Ensure that the presented document meets the following conditions:	a) If it is secondary Government Picture ID:		NE
11	SECURE-8.	MULTIFACTOR AUTHENTICATION	Entities that authenticate a USER MUST offer authentication	NE	ID_IPV#040	Evidence checks – secondary ID	✓			ü	Ensure that the presented document meets the following conditions:	b) If it is a financial institution account number, is verified by a		NE
12	SECURE-8.	MULTIFACTOR AUTHENTICATION	Entities that authenticate a USER MUST offer authentication	NE	ID_IPV#040	Evidence checks – secondary ID	✓			ü	Ensure that the presented document meets the following conditions:	b) If it is a financial institution account number, is verified by a		NE
13	SECURE-8.	MULTIFACTOR AUTHENTICATION	Entities that authenticate a USER MUST offer authentication	NE	ID_IPV#040	Evidence checks – secondary ID	✓			ü	Ensure that the presented document meets the following conditions:	c) If it is two utility bills or equivalent documents:		NE
14	SECURE-8.	MULTIFACTOR AUTHENTICATION	Entities that authenticate a USER MUST offer authentication	NE	ID_IPV#040	Evidence checks – secondary ID	✓			ü	Ensure that the presented document meets the following conditions:	c) If it is two utility bills or equivalent documents:		NE
15	SECURE-8.	MULTIFACTOR AUTHENTICATION	Entities that authenticate a USER MUST offer authentication	NE	ID_IPV#050	Applicant knowledge checks	✓			ü	Where the applicant is unable to satisfy any of the above			NE
16	SECURE-8.	MULTIFACTOR AUTHENTICATION	Entities that authenticate a USER MUST offer authentication	NE	ID_AFV#010	Required evidence	✓			ü	Ensure that the applicant possesses:	a) identification from the organization with which it is claiming affiliation;		NE
17	SECURE-8.	MULTIFACTOR AUTHENTICATION	Entities that authenticate a USER MUST offer authentication	NE	ID_AFV#010	Required evidence	✓			ü	Ensure that the applicant possesses:	b) agreement from the organization that the applicant may be issued a		NE
18	SECURE-8.	MULTIFACTOR AUTHENTICATION	Entities that authenticate a USER MUST offer authentication	NE	ID_AFV#020	Evidence checks	✓			ü	Have in place and apply processes which ensure that the presented	a) each appear to be a genuine document properly issued by the		NE
19	SECURE-8.	MULTIFACTOR AUTHENTICATION	Entities that authenticate a USER MUST offer authentication	NE	ID_AFV#020	Evidence checks	✓			ü	Have in place and apply processes which ensure that the presented	b) refer to an existing organization with a contact address;		NE
20	SECURE-8.	MULTIFACTOR AUTHENTICATION	Entities that authenticate a USER MUST offer authentication	NE	ID_AFV#020	Evidence checks	✓			ü	Have in place and apply processes which ensure that the presented	c) indicate that the applicant has some form of recognizable affiliation		NE

21	SECURE-8.	MULTIFACTOR AUTHENTICATION	Entities that authenticate a USER MUST offer authentication	NE	ID_AFV#020	Evidence checks	✓	✓	Have in place and apply processes which ensure that the presented d) appear to grant the applicant an entitlement to obtain a credential			NE
22	SECURE-8.	MULTIFACTOR AUTHENTICATION	Entities that authenticate a USER MUST offer authentication	NE	CM_ASS#030	Proof of Possession	✓	✓	Use an authentication protocol that requires the claimant to prove			NE
23	SECURE-8.	MULTIFACTOR AUTHENTICATION	Entities that authenticate a USER MUST offer authentication	NE	CM_AGC#010	Entropy level	✓	✓	Create authentication secrets to be used during the authentication			NE
1	INTEROP-1.	THIRD PARTY AUTHENTICATION	Entities MUST be capable of accepting external USERS	NCR								NCR
1	INTEROP-3.	STANDARDIZED CREDENTIALS	Entities that issue credentials or assertions MUST issue them in a	NCR								NCR
1	PRIVACY-2.	PURPOSE LIMITATION	Entities MUST limit the use of personal information that is	NCR								NCR
1	PRIVACY-3.	ATTRIBUTE MINIMIZATION	Entities requesting attributes MUST evaluate the need to collect specific	NCR								NCR
1	PRIVACY-4.	CREDENTIAL LIMITATION	Entities MUST NOT request USERS' credentials unless necessary for	NCR								NCR
1	PRIVACY-5.	DATA AGGREGATION RISK	Entities MUST assess the privacy risk of aggregating personal	NCR								NCR
1	PRIVACY-10.	USER OPTION TO DECLINE	USERS MUST have the opportunity to decline registration: decline	NCR								NCR
1	PRIVACY-11.	OPTIONAL INFORMATION	Entities MUST clearly indicate to USERS what personal information	NCR								NCR
1	USABLE-1.	USABILITY PRACTICES	Entities conducting digital identity management functions MUST apply	NCR								NCR
1	USABLE-2.	USABILITY ASSESSMENT	Entities MUST assess the usability of the communications, interfaces.	NCR								NCR
1	USABLE-4.	NAVIGATION	All choices, pathways, interfaces, and offerings provided to USERS in	NCR								NCR
1	USABLE-6.	USABILITY FEEDBACK	All communications, interfaces, policies, data transactions, and	NCR								NCR

[illegible]

[illegible]

[illegible]

Reminders that covers initial "proofing" rather than later
Reminders that authentication protocol
does not require alternative to
Reminders that authentication protocol
does not require alternative to
password

