

1



2

3

4 **Identity Assurance Framework:** 5 **Service Assessment Criteria**

6

7

8

9 **Version:** draft 0.9

10 **Date:** 2009-12-31

11 **Editor:** Richard G. Wilsher
12 Zygya LLC

13 **Contributors**

14 This document is a draft and not in final release form. The full list of contributors will be
15 added prior to the final release of this document.

16 **Abstract**

17 The Kantara Initiative Identity Assurance Work Group (IAWG) was formed to foster
18 adoption of identity trust services. The primary deliverable of the IAWG is the Identity
19 Assurance Framework (IAF), which is comprised of many different documents that detail
20 the levels of assurance and the certification program that bring the Framework to the
21 marketplace. The IAF is comprised of a set of documents that includes an Overview
22 publication, the IAF [Glossary](#), a summary [Assurance Levels](#) document, and an [Assurance](#)
23 [Assessment Scheme \(AAS\)](#), which encompasses the associated assessment and
24 certification program, as well as several subordinate documents, among them the [Service](#)
25 [Assessment Criteria \(SAC\)](#), which establishes baseline criteria for general organizational
26 conformity, identity proofing services, credential strength, and credential management
27 services against which all CSPs will be evaluated. The present document describes the
28 Service Assessment Criteria component of the IAF, including setting out the Assurance
29 Levels.

30

31 **Filename:** Kantara IAF-1400-Service Assessment Criteria.doc

32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56

Notice

This document has been prepared by Participants of Kantara Initiative. Permission is hereby granted to use the document solely for the purpose of implementing the Specification. No rights are granted to prepare derivative works of this Specification. Entities seeking permission to reproduce portions of this document for other uses must contact Kantara Initiative to determine whether an appropriate license for such use is available.

Implementation or use of certain elements of this document may require licenses under third party intellectual property rights, including without limitation, patent rights. The Participants of and any other contributors to the Specification are not and shall not be held responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights. This Specification is provided "AS IS," and no Participant in Kantara Initiative makes any warranty of any kind, expressed or implied, including any implied warranties of merchantability, non-infringement of third party intellectual property rights, and fitness for a particular purpose. Implementers of this Specification are advised to review Kantara Initiative's website (<http://www.kantarainitiative.org/>) for information concerning any Necessary Claims Disclosure Notices that have been received by the Kantara Initiative Board of Trustees.

Copyright: The content of this document is copyright of Kantara Initiative. © 2009 Kantara Initiative.

Contents

57		
58		
59	1 INTRODUCTION.....	4
60	2 ASSURANCE LEVELS.....	5
61	3 SERVICE ASSESSMENT CRITERIA.....	6
62	3.1 Context and Scope	6
63	3.2 Readership.....	6
64	3.3 Criteria Descriptions	7
65	3.4 Terminology.....	8
66	3.5 Common Organizational Service Assessment Criteria.....	9
67	3.5.1 Assurance Level 1.....	9
68	3.5.2 Assurance Level 2.....	12
69	3.5.3 Assurance Level 3.....	22
70	3.5.4 Assurance Level 4.....	32
71	3.5.5 Compliance Tables.....	42
72	3.6 Identity Proofing Service Assessment Criteria	49
73	3.6.1 Assurance Level 1.....	49
74	3.6.2 Assurance Level 2.....	51
75	3.6.3 Assurance Level 3.....	57
76	3.6.4 Assurance Level 4.....	63
77	3.6.5 Compliance Tables.....	68
78	3.7 Credential Management Service Assessment Criteria	72
79	3.7.1 Part A - Credential Operating Environment	72
80	3.7.2 Part B - Credential Issuing.....	85
81	3.7.3 Part C - Credential Renewal and Re-issuing.....	99
82	3.7.4 Part D - Credential Revocation	103
83	3.7.5 Part E - Credential Status Management.....	114
84	3.7.6 Part F - Credential Validation/Authentication	118
85	3.7.7 Compliance Tables.....	124
86	4 REFERENCES.....	132
87		
88		

89 1 INTRODUCTION

90 Kantara Initiative formed the Identity Assurance Work Group (IAWG) to foster adoption
91 of consistently managed identity trust services. Utilizing initial contributions from the
92 e-Authentication Partnership (EAP), the US E-Authentication Federation, and Liberty
93 Alliance, the IAWG's objective is to create a Framework of baseline policy requirements
94 (criteria) and rules against which identity trust services can be assessed and evaluated.
95 The goal is to facilitate trusted identity federation and to promote uniformity and
96 interoperability amongst identity service providers, with a specific focus on the level of
97 trust, or assurance, associated with identity assertions. The primary deliverable of IAWG
98 is the Identity Assurance Framework (IAF).

99 The IAF leverages the EAP Trust Framework [[EAPTrustFramework](#)] and the US
100 E-Authentication Federation Credential Assessment Framework ([[CAF](#)]) as baselines in
101 forming the criteria for a harmonized, best-of-breed, industry-recognized identity
102 assurance standard. The IAF is a Framework supporting mutual acceptance, validation,
103 and life cycle maintenance across identity federations. The IAF is composed of a set of
104 documents that includes an [Overview](#) publication, the IAF [Glossary](#), a [summary](#)
105 [document on Assurance Levels](#), and an [Assurance Assessment Scheme \(AAS\) document](#),
106 which encompasses the associated assessment and certification program, as well as
107 several subordinant documents. The present document, subordinant to the AAS,
108 describes the Service Assessment Criteria component of the IAF, including setting-out the
109 Assurance Levels.

110 Assurance Levels (ALs) are the levels of trust associated with a credential as measured by
111 the associated technology, processes, and policy and practice statements controlling the
112 operational environment. The IAF defers to the guidance provided by the U.S. National
113 Institute of Standards and Technology (NIST) Special Publication 800-63 version 1.0.1
114 [[NIST800-63](#)] which outlines four levels of assurance, ranging in confidence level from
115 low to very high. Use of ALs is determined by the level of confidence or trust (i.e.
116 assurance) necessary to mitigate risk in the transaction.

117 The Service Assessment Criteria part of the IAF establishes baseline criteria for general
118 organizational conformity, identity proofing services, credential strength, and credential
119 management services against which all CSPs will be evaluated. The IAF will initially
120 focus on baseline identity assertions and evolve to include attribute- and entitlement-
121 based assertions in future releases. The IAF will also establish a protocol for publishing
122 updates, as needed, to account for technological advances and preferred practice and
123 policy updates.

124 **2 ASSURANCE LEVELS**

125 The IAF has adopted four Assurance Levels (ALs), based on the four levels of assurance
126 posited by the U.S. Federal Government and described in OMB M-04-04 [[M-04-04](#)] and
127 NIST Special Publication 800-63 [[NIST800-63](#)]. These are further described in the IAF
128 publication [Assurance Levels](#).

129 **3 SERVICE ASSESSMENT CRITERIA**

130 **3.1 Context and Scope**

131 The Service Assessment Criteria (SAC) are prepared and maintained by the Identity
132 Assurance Work Group (IAWG) as part of its Identity Assurance Framework. These
133 criteria set out the requirements for credential services and their providers at all assurance
134 levels within the Framework. These criteria focus on the specific requirements for IAWG
135 assessment at each Assurance Level (AL) for the following:

- 136 • The general business and organizational conformity of services and their
137 providers;
- 138 • The functional conformity of identity proofing services; and
- 139 • The functional conformity of credential management services and their
140 providers.

141 These criteria (at the applicable level) must be complied with by all services that are
142 assessed for certification under the Identity Assurance Framework (IAF).

143 These criteria have been approved under the IAWG's governance rules as being suitable
144 for use by Kantara-Accredited Assessors in the performance of their assessments of trust
145 services whose providers are seeking recognition by IAWG.

146 In the context of the Identity Assurance Framework, the status of this document is
147 normative. An applicant's trust service shall comply with all applicable criteria within
148 this SAC at their nominated AL.

149 This document describes the specific criteria that must be met to achieve each of the four
150 ALs supported by the IAWG. To be certified under the IAF Accreditation and
151 Certification Scheme and earn the requisite Kantara Initiative Mark, services must
152 comply with all criteria at the appropriate level.

153 **3.2 Readership**

154 This description of Service Assessment Criteria is required reading for all Kantara-
155 Accredited Assessors, since it sets out the requirements with which service functions
156 must be independently verified as being in compliance in order to be granted Kantara
157 Recognition.

158 The description of criteria in Sections [3.5](#), [3.6](#) and [3.7](#) is required reading for all
159 organizations wishing to become Kantara-Recognized Service Providers, and also for
160 those wishing to become Kantara-Accredited Assessors. It is also recommended reading
161 for those involved in the governance and day-to-day administration of the Identity
162 Assurance Framework.

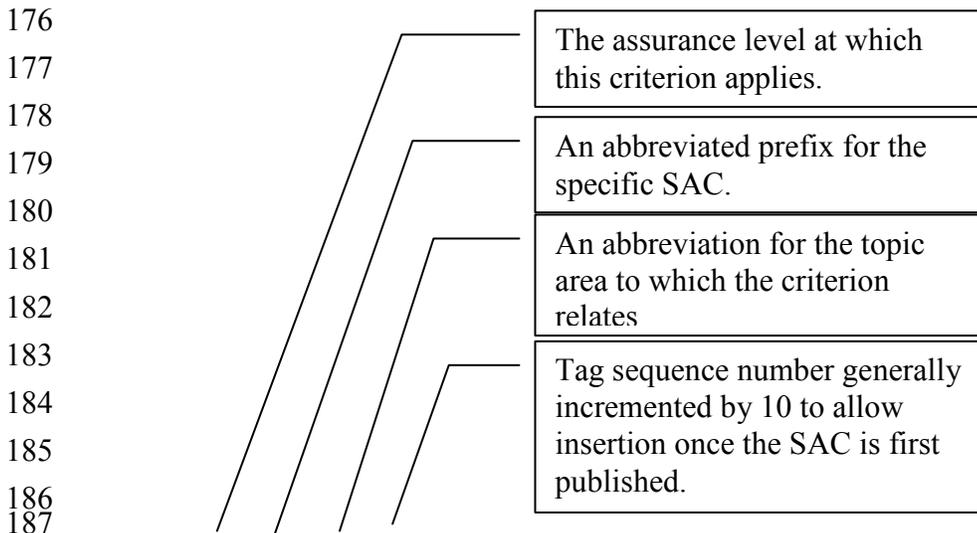
163 This document will also be of interest to those wishing to have a detailed understanding
164 of the operation of the Identity Assurance Framework but who are not actively involved
165 in its operations or in services that may fall within the scope of the Framework.

166 3.3 Criteria Descriptions

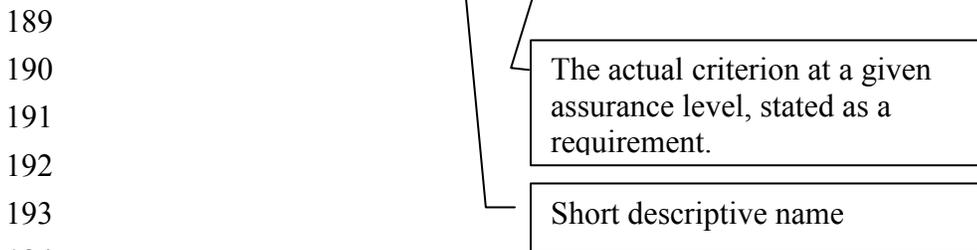
167 The Service Assessment Criteria are organized by AL. Subsections within each level
168 describe the criteria that apply to specific functions. The subsections are parallel.
169 Subsections describing the requirements for the same function at different levels of
170 assurance have the same title.

171 Each criterion consists of three components: a unique alphanumeric tag, a short name,
172 and the criterion (or criteria) associated with the tag. The tag provides a unique reference
173 for each criterion that assessors and service providers can use to refer to that criterion.
174 The name identifies the intended scope or purpose of the criterion.

175 The criteria are described as follows:



188 «ALn_CO_ZZZ#999»«name»Criterion ALn (i.e., AL1_CO_ESM#010)



195 When a given criterion changes (i.e. becomes more rigorous) at higher Assurance Levels
196 the new or revised text is **shown in bold** or '[Omitted]' is indicated where text has been

197 removed. With the obvious exception of AL1, when a criterion is first introduced it is
198 also shown in bold.

199 As noted in the above schematic, when originally prepared, the tags had numbers
200 incrementing in multiples of ten to permit the later insertion of additional criteria. Since
201 then there has been addition and withdrawal of criteria.

202 Where a criterion is not used in a given AL but is used at a higher AL its place is held by
203 the inclusion of a tag which is marked 'No stipulation'. A title and appropriate criteria
204 will be added at the higher AL which occupies that position. Since in general higher ALs
205 have a greater extent of criteria than lower ALs, where a given AL extends no further
206 through the numbering range, criteria beyond that value are by default omitted rather than
207 being included but marked 'No stipulation'.

208 Further, over time, some criteria have been removed, or withdrawn. In order to avoid the
209 re-use of that tag such tags are retained but marked 'Withdrawn'.

210 Not only do these editorial practices preserve continuity they also guard against possible
211 omission of a required criterion through an editing error.

212 **3.4 Terminology**

213 All special terms used in this description are defined in the [IAF Glossary](#).

214 Note that when, in these criteria, the term 'Subscriber' is used it applies equally to
215 'Subscriber' and 'Subject' as defined in the [IAF Glossary](#), according to the context in
216 which used. The term 'Subject' is used when the reference is explicitly toward that party.

217 **3.5 Common Organizational Service Assessment Criteria**

218 The Service Assessment Criteria in this section establish the general business and
219 organizational requirements for conformity of services and service providers at all ALs
220 defined in Section 2 and in the [Identity Assurance Framework: Levels of Assurance](#)
221 document. These criteria are generally referred to elsewhere within IAWG
222 documentation as CO-SAC.

223 These criteria may only be used in an assessment in combination with one or more other
224 SACs that address the technical functionality of specific service offerings.

225 **3.5.1 Assurance Level 1**

226 **3.5.1.1 Enterprise and Service Maturity**

227 These criteria apply to the establishment of the organization offering the service and its
228 basic standing as a legal and operational business entity within its respective jurisdiction
229 or country.

230 An enterprise and its specified service must:

231 AL1_CO_ESM#010 Established enterprise

232 Be a valid legal entity, and a person with the legal authority to commit the organization
233 must submit the signed assessment package.

234 AL1_CO_ESM#020 Established service

235 Be fully operational in all areas described in the assessment package submitted for
236 assessment.

237 **Guidance:** Kantara Initiative will not recognize a service which is not fully released for
238 the provision of services to its intended user/client community. Systems, or parts thereof,
239 which are not fully proven and released shall not be considered in an assessment and
240 therefore should not be included within the scope of the assessment package. Parts of
241 systems still under development, or even still being planned, are therefore ineligible for
242 inclusion within the scope of assessment.

243 AL1_CO_ESM#030 Legal & Contractual compliance

244 Demonstrate that it understands and complies with any legal requirements incumbent on
245 it in connection with operation and delivery of the specified service, accounting for all
246 jurisdictions and countries within which its services may be used.

247 **Guidance:** ‘Understanding’ is implicitly the correct understanding. Both it and
248 compliance are required because it could be that understanding is incomplete, incorrect or

249 even absent, even though compliance is apparent, and similarly, correct understanding
250 may not necessarily result in full compliance. The two are therefore complementary.

251 AL1_CO_ESM#040 No stipulation

252 AL1_CO_ESM#050 No stipulation

253 AL1_CO_ESM#055 Termination provisions

254 Define the practices in place for the protection of subscribers' private and secret
255 information related to their use of the service which must ensure the ongoing secure
256 preservation and protection of legally required records and for the secure destruction and
257 disposal of any such information whose retention is no longer legally required. Specific
258 details of these practices must be made available.

259 **Guidance:** Termination covers the cessation of the business activities, the service
260 provider itself ceasing business operations altogether, change of ownership of the service-
261 providing business, and other similar events which change the status and/or operations of
262 the service provider in any way which interrupts the continued provision of the specific
263 service.

264 **3.5.1.2 Notices and User information**

265 These criteria address the publication of information describing the service and the
266 manner of and any limitations upon its provision.

267 An enterprise and its specified service must:

268 AL1_CO_NUI#010 General Service Definition

269 Make available to the intended user community a Service Definition that includes all
270 applicable Terms, Conditions, and Fees, including any limitations of its usage. Specific
271 provisions are stated in further criteria in this section.

272 **Guidance:** The intended user community encompasses potential and actual subscribers,
273 subjects, and relying parties.

274 AL1_CO_NUI#020 Service Definition inclusions

275 Make available a Service Definition for the specified service containing clauses that
276 provide the following information:

277 a) a Privacy Policy
278

- 279 AL1_CO_NUI#030 Due notification
- 280 Have in place and follow appropriate policy and procedures to ensure that it notifies
281 Users in a timely and reliable fashion of any changes to the Service Definition and any
282 applicable Terms, Conditions, and Privacy Policy for the specified service.
- 283 AL1_CO_NUI#040 User Acceptance
- 284 Require subscribers and subjects to:
- 285 a) indicate, prior to receiving service, that they have read and accept the terms of
286 service as defined in the Service Definition;
- 287 b) at periodic intervals, determined by significant service provision events (e.g.
288 issuance, re-issuance, renewal), re-affirm their understanding and observance of
289 the terms of service;
- 290 c) always provide full and correct responses to requests for information.
- 291 AL1_CO_NUI#050 Record of User Acceptance
- 292 Obtain a record (hard-copy or electronic) of the subscriber's and subject's acceptance of
293 the terms and conditions of service, prior to initiating the service and thereafter at
294 periodic intervals, determined by significant service provision events (e.g. re-issuance,
295 renewal).
296
- 297 **3.5.1.3 Not used**
- 298 **3.5.1.4 Not used**
- 299 **3.5.1.5 Not used**
- 300 **3.5.1.6 Not used**
- 301 **3.5.1.7 Secure Communications**
- 302 AL1_CO_SCO#010 No stipulation
- 303 AL1_CO_SCO#020 Limited access to shared secrets
- 304 Ensure that:
- 305 a) access to shared secrets shall be subject to discretionary controls which permit
306 access to those roles/applications needing such access;
- 307 b) stored shared secrets are not held in their plaintext form unless given adequate
308 physical or logical protection;
- 309 c) any plaintext passwords or secrets are not transmitted across any public or
310 unsecured network.

311 **3.5.2 Assurance Level 2**

312 Criteria in this section address the establishment of the enterprise offering the service and
313 its basic standing as a legal and operational business entity within its respective
314 jurisdiction or country.

315 **3.5.2.1 Enterprise and Service Maturity**

316 These criteria apply to the establishment of the enterprise offering the service and its
317 basic standing as a legal and operational business entity.

318 An enterprise and its specified service must:

319 AL2_CO_ESM#010 Established enterprise

320 Be a valid legal entity, and a person with legal authority to commit the organization must
321 submit the signed assessment package.

322 AL2_CO_ESM#020 Established service

323 Be fully operational in all areas described in the assessment package submitted for
324 assessment.

325 AL2_CO_ESM#030 Legal & Contractual compliance

326 Demonstrate that it understands and complies with any legal requirements incumbent on
327 it in connection with operation and delivery of the specified service, accounting for all
328 jurisdictions within which its services may be offered. **Any specific contractual**
329 **requirements shall also be identified.**

330 **Guidance:** Kantara Initiative will not recognize a service which is not fully released for
331 the provision of services to its intended user/client community. Systems, or parts thereof,
332 which are not fully proven and released shall not be considered in an assessment and
333 therefore should not be included within the scope of the assessment package. Parts of
334 systems still under development, or even still being planned, are therefore ineligible for
335 inclusion within the scope of assessment.

336 AL2_CO_ESM#040 Financial Provisions

337 **Provide documentation of financial resources that allow for the continued operation**
338 **of the service and demonstrate appropriate liability processes and procedures that**
339 **satisfy the degree of liability exposure being carried.**

340 **Guidance:** The organization must show that it has a budgetary provision to operate the
341 service for at least a twelve-month period, with a clear review of the budgetary planning
342 within that period so as to keep the budgetary provisions extended. It must also show

343 how it has determined the degree of liability protection required, in view of its exposure
344 per ‘service’ and the number of users it has. This criterion helps ensure that Kantara
345 Initiative does not grant Recognition to services that are not likely to be sustainable over
346 at least this minimum period of time.

347 AL2_CO_ESM#050 Data Retention and Protection

348 **Specifically set out and demonstrate that it understands and complies with those**
349 **legal and regulatory requirements incumbent upon it concerning the retention and**
350 **destruction of private and identifiable information (personal and business)(i.e. its**
351 **secure storage and protection against loss, accidental public exposure, and/or**
352 **improper destruction) and the protection of subscribers’ private information**
353 **(against unlawful or unauthorized access, excepting that permitted by the**
354 **information owner or required by due process).**

355 **Guidance:** Note that whereas the criterion is intended to address unlawful or
356 unauthorized access arising from malicious or careless actions (or inaction) some access
357 may be unlawful UNLESS authorized by the subscriber or effected as a part of a
358 specifically-executed legal process.

359 AL2_CO_ESM#055 Termination provisions

360 Define the practices in place for the protection of subscribers’ private and secret
361 information related to their use of the service which must ensure the ongoing secure
362 preservation and protection of legally required records and for the secure destruction and
363 disposal of any such information whose retention is no longer legally required. Specific
364 details of these practices must be made available.

365 **Guidance:** Termination covers the cessation of the business activities, the service
366 provider itself ceasing business operations altogether, change of ownership of the service-
367 providing business, and other similar events which change the status and/or operations of
368 the service provider in any way which interrupts the continued provision of the specific
369 service.

370 **3.5.2.2 Notices and User Information/Agreements**

371 These criteria apply to the publication of information describing the service and the
372 manner of and any limitations upon its provision, and how users are required to accept
373 those terms.

374 An enterprise and its specified service must:

375 AL2_CO_NUI#010 General Service Definition

376 Make available to the intended user community a Service Definition that includes all
377 applicable Terms, Conditions, and Fees, including any limitations of its usage, **and**

378 **definitions of any terms having specific intention or interpretation. Specific**
379 **provisions are stated in further criteria in this section.**

380 **Guidance:** The intended user community encompasses potential and actual subscribers,
381 subjects, and relying parties.

382 AL2_CO_NUI#020 Service Definition inclusions

383 Make available a Service Definition for the specified service containing clauses that
384 provide the following information:

- 385 a) **Privacy, Identity Proofing & Verification, and Revocation and Termination**
386 **Policies;**
- 387 b) **the country in or legal jurisdiction under which the service is operated;**
- 388 c) **if different from the above, the legal jurisdiction under which subscriber and**
389 **any relying party agreements are entered into;**
- 390 d) **applicable legislation with which the service complies;**
- 391 e) **obligations incumbent upon the CSP;**
- 392 f) **obligations incumbent upon the subscriber;**
- 393 g) **notifications and guidance for relying parties, especially in respect of actions**
394 **they are expected to take should they choose to rely upon the service;**
- 395 h) **statement of warranties;**
- 396 i) **statement of liabilities toward both Subjects and Relying Parties;**
- 397 j) **procedures for notification of changes to terms and conditions;**
- 398 k) **steps the CSP will take in the event that it chooses or is obliged to terminate**
399 **the service;**
- 400 l) **availability of the specified service *per se* and of its help desk facility.**

401 AL2_CO_NUI#030 Due notification

402 Have in place and follow appropriate policy and procedures to ensure that it notifies
403 subscribers and subjects in a timely and reliable fashion of any changes to the Service
404 Definition and any applicable Terms, Conditions, Fees, and Privacy Policy for the
405 specified service, **and provide a clear means by which subscribers and subjects must**
406 **indicate that they wish to accept the new terms or terminate their subscription.**

407 AL2_CO_NUI#040 User Acceptance

408 Require subscribers and subjects to:

- 409 a) indicate, prior to receiving service, that they have read and accept the terms of
410 service as defined in the Service Definition;
- 411 b) at periodic intervals, determined by significant service provision events (e.g.
412 issuance, re-issuance, renewal) **and otherwise at least once every five years**, re-
413 affirm their understanding and observance of the terms of service;
- 414 c) always provide full and correct responses to requests for information.

- 415 AL2_CO_NUI#050 Record of User Acceptance
416 Obtain a record (hard-copy or electronic) of the subscriber's and subject's acceptance of
417 the terms and conditions of service, prior to initiating the service and thereafter at
418 periodic intervals, determined by significant service provision events (e.g. re-issuance,
419 renewal) **and otherwise at least once every five years.**
- 420 AL2_CO_NUI#060 Withdrawn
421 Withdrawn.
- 422 AL2_CO_NUI#070 Change of Subscriber Information
423 **Require and provide the mechanisms for subscribers and subjects to provide in a**
424 **timely manner full and correct amendments should any of their recorded**
425 **information change, as required under the terms of their use of the service, and only**
426 **after the subscriber's and/or subject's identity has been authenticated.**
- 427 AL2_CO_NUI#080 Withdrawn
428 Withdrawn.
- 429 **3.5.2.3 Information Security Management**
430 These criteria address the way in which the enterprise manages the security of its
431 business, the specified service, and information it holds relating to its user community.
432 This section focuses on the key components that comprise a well-established and
433 effective Information Security Management System (ISMS), or other IT security
434 management methodology recognized by a government or professional body.
435 An enterprise and its specified service must:
- 436 AL2_CO_ISM#010 Documented policies and procedures
437 **Have documented all security-relevant administrative, management, and technical**
438 **policies and procedures. The enterprise must ensure that these are based upon**
439 **recognized standards, published references or organizational guidelines, are**
440 **adequate for the specified service, and are implemented in the manner intended.**
- 441 AL2_CO_ISM#020 Policy Management and Responsibility
442 **Have a clearly defined managerial role, at a senior level, in which full responsibility**
443 **for the business's security policies is vested and from which review, approval, and**
444 **promulgation of policy and related procedures is applied and managed. The latest**
445 **approved versions of these policies must be applied at all times.**

- 446 AL2_CO_ISM#030 Risk Management
447 **Demonstrate a risk management methodology that adequately identifies and**
448 **mitigates risks related to the specified service and its user community.**
- 449 AL2_CO_ISM#040 Continuity of Operations Plan
450 **Have and keep updated a Continuity of Operations Plan that covers disaster**
451 **recovery and the resilience of the specified service.**
- 452 AL2_CO_ISM#050 Configuration Management
453 **Demonstrate that there is in place a configuration management system that at least**
454 **includes:**
455 **a) version control for software system components;**
456 **b) timely identification and installation of all organizationally-approved patches**
457 **for any software used in the provisioning of the specified service.**
- 458 AL2_CO_ISM#060 Quality Management
459 **Demonstrate that there is in place a quality management system that is appropriate**
460 **for the specified service.**
- 461 AL2_CO_ISM#070 System Installation and Operation Controls
462 **Apply controls during system development, procurement installation, and operation**
463 **that protect the security and integrity of the system environment, hardware,**
464 **software, and communications.**
- 465 AL2_CO_ISM#080 Internal Service Audit
466 **Be audited at least once every 12 months for effective provision of the specified**
467 **service by independent internal audit functions of the enterprise responsible for the**
468 **specified service, unless it can show that by reason of its organizational size or due to**
469 **other operational restrictions it is unreasonable to be so audited.**
- 470 AL2_CO_ISM#090 Independent Audit
471 **Be audited by an independent auditor at least every 24 months to ensure the**
472 **organization's security-related practices are consistent with the policies and**
473 **procedures for the specified service and the applicable SAC.**
474 **Guidance:** The appointed auditor should have appropriate accreditation or other
475 acceptable experience and qualification, comparable to that required of Kantara-
476 Accredited Assessors. It is expected that it will be cost-effective for the organization to

477 use the same Kantara-Accredited Assessor for the purposes of fulfilling this criterion as
478 they do for the maintenance of their grant of Kantara Recognition.

479 AL2_CO_ISM#100 Audit Records

480 **Retain records of all audits, both internal and independent, for a period which, as a**
481 **minimum, fulfills its legal obligations and otherwise for greater periods either as it**
482 **may have committed to in its Service Definition or required by any other obligations**
483 **it has with/to a subscriber, and which in any event is not less than 36 months. Such**
484 **records must be held securely and be protected against unauthorized access, loss,**
485 **alteration, public disclosure, or unapproved destruction.**

486 AL2_CO_ISM#110 Termination provisions

487 This is now AL2_CO_ESM#055.

488

489 **3.5.2.4 Security-relevant Event (Audit) Records**

490 These criteria apply to the need to provide an auditable log of all events that are pertinent
491 to the correct and secure operation of the service.

492 An enterprise and its specified service must:

493 AL2_CO_SER#010 Security event logging

494 **Maintain a log of all relevant security events concerning the operation of the service,**
495 **together with an accurate record of the time at which the event occurred (time-**
496 **stamp), and retain such records with appropriate protection and controls to ensure**
497 **successful retrieval, accounting for service definition, risk management**
498 **requirements, applicable legislation, and organizational policy.**

499 **Guidance:** It is sufficient that the accuracy of the time source is based upon an internal
500 computer/system clock synchronized to an internet time source. The time source need
501 not be authenticatable.

502

503 **3.5.2.5 Operational infrastructure**

504 These criteria apply to the infrastructure within which the delivery of the specified
505 service takes place. These criteria emphasize the personnel involved and their selection,
506 training, and duties.

507 An enterprise and its specified service must:

508 AL2_CO_OPN#010 Technical security

509 **Demonstrate that the technical controls employed will provide the level of security**
510 **protection required by the risk assessment and the ISMS, or other IT security**
511 **management methods recognized by a government or professional body, and that**
512 **these controls are effectively integrated with the applicable procedural and physical**
513 **security measures.**

514 **Guidance:** Appropriate technical controls, suited to this Assurance Level, should be
515 selected from [NIST800-63] or its equivalent, as established by a recognized national
516 technical authority.

517 AL2_CO_OPN#020 Defined security roles

518 **Define, by means of a job description, the roles and responsibilities for each service-**
519 **related security-relevant task, relating it to specific procedures, (which shall be set**
520 **out in the ISMS, or other IT security management methodology recognized by a**
521 **government or professional body) and other service-related job descriptions. Where**
522 **the role is security-critical or where special privileges or shared duties exist, these**
523 **must be specifically identified as such, including the applicable access privileges**
524 **relating to logical and physical parts of the service's operations.**

525 AL2_CO_OPN#030 Personnel recruitment

526 **Demonstrate that it has defined practices for the selection, evaluation, and**
527 **contracting of all service-related personnel, both direct employees and those whose**
528 **services are provided by third parties.**

529 AL2_CO_OPN#040 Personnel skills

530 **Ensure that employees are sufficiently trained, qualified, experienced, and current**
531 **for the roles they fulfill. Such measures must be accomplished either by recruitment**
532 **practices or through a specific training program. Where employees are undergoing**
533 **on-the-job training, they must only do so under the guidance of a mentor possessing**
534 **the defined service experiences for the training being provided.**

535 AL2_CO_OPN#050 Adequacy of Personnel resources

536 **Have sufficient staff to adequately operate and resource the specified service**
537 **according to its policies and procedures.**

538 AL2_CO_OPN#060 Physical access control

539 **Apply physical access control mechanisms to ensure that:**

540 a) **access to sensitive areas is restricted to authorized personnel;**

541 **b) all removable media and paper documents containing sensitive information**
542 **as plain-text are stored in secure containers.**

543 Require a minimum of two person physical access control when accessing any
544 cryptographic modules.

545 AL2_CO_OPN#070 Logical access control

546 **Employ logical access control mechanisms that ensure access to sensitive system**
547 **functions and controls is restricted to authorized personnel.**

548

549 **3.5.2.6 External Services and Components**

550 These criteria apply to the relationships and obligations upon contracted parties both to
551 apply the policies and procedures of the enterprise and also to be available for assessment
552 as critical parts of the overall service provision.

553 An enterprise and its specified service must:

554 AL2_CO_ESC#010 Contracted policies and procedures

555 **Where the enterprise uses external suppliers for specific packaged components of**
556 **the service or for resources that are integrated with its own operations and under its**
557 **control, ensure that those parties are engaged through reliable and appropriate**
558 **contractual arrangements which stipulate which critical policies, procedures, and**
559 **practices subcontractors are required to fulfill.**

560 AL2_CO_ESC#020 Visibility of contracted parties

561 **Where the enterprise uses external suppliers for specific packaged components of**
562 **the service or for resources that are integrated with its own operations and under its**
563 **control, ensure that the suppliers' compliance with contractually-stipulated policies**
564 **and procedures, and thus with IAF Service Assessment Criteria, can be**
565 **independently verified, and subsequently monitored if necessary.**

566

567 **3.5.2.7 Secure Communications**

568 An enterprise and its specified service must:

569 AL2_CO_SCO#010 Secure remote communications

570 **If the specific service components are located remotely from and communicate over**
571 **a public or unsecured network with other service components or other CSPs which**

572 **it services, the communications must be cryptographically authenticated, including**
573 **long-term and session tokens, by an authentication method that meets, at a**
574 **minimum, the requirements of AL2 and encrypted using a [FIPS140-2] Level 1-**
575 **compliant encryption method or equivalent, as established by a recognized national**
576 **technical authority.**

577 AL2_CO_SCO#015 Verification / Authentication confirmation messages

578 **Ensure that any verification or confirmation of authentication messages, which**
579 **asserts either that a weakly bound credential is valid or that a strongly bound**
580 **credential has not been subsequently revoked, is logically bound to the credential**
581 **and that the message, the logical binding, and the credential are all transmitted**
582 **within a single integrity-protected session between the service and the Verifier /**
583 **Relying Party.**

584 AL2_CO_SCO#016 Verification of Revoked Credential

585 **When a verification / authentication request results in notification of a revoked**
586 **credential one of the following measures shall be taken:**

- 587 a) **the confirmation message shall be time-stamped, or;**
588 b) **the session keys shall expire with an expiration time no longer than that of**
589 **the applicable revocation list, or;**
590 c) **the time-stamped message, binding, and credential shall all be signed by the**
591 **service.**

592 AL2_CO_SCO#020 Limited access to shared secrets

593 Ensure that:

- 594 a) access to shared secrets shall be subject to discretionary controls that only permit
595 access by those roles/applications requiring such access;
596 b) stored shared secrets are not held in their plaintext form unless given adequate
597 physical or logical protection;
598 c) **any long-term (i.e., not session) shared secrets are revealed only to the**
599 **subscriber or to the CSP's direct agents (bearing in mind item "a" in this**
600 **list).**

601
602 **These roles should be defined and documented by the CSP in accordance with**
603 **AL2_CO_OPN#020 above.**

604 AL2_CO_SCO#030 Logical protection of shared secrets

605 **Ensure that one of the alternative methods (below) is used to protect shared secrets:**

- 606 a) concatenation of the password to a salt and/or username which is then hashed
607 with an Approved algorithm such that the computations used to conduct a
608 dictionary or exhaustion attack on a stolen password file are not useful to
609 attack other similar password files, or;
- 610 b) encryption using an Approved algorithm and modes, and the shared secret
611 decrypted only when immediately required for authentication, or;
- 612 c) any secure method allowed to protect shared secrets at Level 3 or 4.
- 613

614 **3.5.3 Assurance Level 3**

615 Achieving AL3 requires meeting more stringent criteria in addition to all criteria required
616 to achieve AL2.

617 **3.5.3.1 Enterprise and Service Maturity**

618 Criteria in this section address the establishment of the enterprise offering the service and
619 its basic standing as a legal and operational business entity.

620 An enterprise and its specified service must:

621 AL3_CO_ESM#010 Established enterprise

622 Be a valid legal entity and a person with legal authority to commit the organization must
623 submit the signed assessment package.

624 AL3_CO_ESM#020 Established service

625 Be fully operational in all areas described in the assessment package submitted for
626 assessment.

627 AL3_CO_ESM#030 Legal & Contractual compliance

628 Demonstrate that it understands and complies with any legal requirements incumbent on
629 it in connection with operation and delivery of the specified service, accounting for all
630 jurisdictions within which its services may be offered. Any specific contractual
631 requirements shall also be identified.

632 **Guidance:** Kantara Initiative will not recognize a service which is not fully released for
633 the provision of services to its intended user/client community. Systems, or parts thereof,
634 which are not fully proven and released shall not be considered in an assessment and
635 therefore should not be included within the scope of the assessment package. Parts of
636 systems still under development, or even still being planned, are therefore ineligible for
637 inclusion within the scope of assessment.

638 AL3_CO_ESM#040 Financial Provisions

639 Provide documentation of financial resources that allow for the continued operation of the
640 service and demonstrate appropriate liability processes and procedures that satisfy the
641 degree of liability exposure being carried.

642 **Guidance:** The organization must show that it has a budgetary provision to operate the
643 service for at least a twelve-month period, with a clear review of the budgetary planning
644 within that period so as to keep the budgetary provisions extended. It must also show
645 how it has determined the degree of liability protection required, in view of its exposure

646 per 'service' and the number of users it has. This criterion helps ensure that Kantara
647 Initiative does not grant Recognition to services that are not likely to be sustainable over
648 at least this minimum period of time.

649 AL3_CO_ESM#050 Data Retention and Protection

650 Specifically set out and demonstrate that it understands and complies with those legal and
651 regulatory requirements incumbent upon it concerning the retention and destruction of
652 private and identifiable information (personal and business) (i.e. its secure storage and
653 protection against loss, accidental public exposure and/or improper destruction) and the
654 protection of private information (against unlawful or unauthorized access, excepting that
655 permitted by the information owner or required by due process).

656 AL3_CO_ESM#055 Termination provisions

657 Define the practices in place for the protection of subscribers' private and secret
658 information related to their use of the service which must ensure the ongoing secure
659 preservation and protection of legally required records and for the secure destruction and
660 disposal of any such information whose retention is no longer legally required. Specific
661 details of these practices must be made available.

662 **Guidance:** Termination covers the cessation of the business activities, the service
663 provider itself ceasing business operations altogether, change of ownership of the service-
664 providing business, and other similar events which change the status and/or operations of
665 the service provider in any way which interrupts the continued provision of the specific
666 service.

667 AL3_CO_ESM#060 Ownership

668 **If the enterprise named as the CSP is a part of a larger entity, the nature of the**
669 **relationship with its parent organization shall be disclosed to the assessors and, on**
670 **their request, to customers.**

671 AL3_CO_ESM#070 Independent management and operations

672 **Demonstrate that, for the purposes of providing the specified service, its**
673 **management and operational structures are distinct, autonomous, have discrete**
674 **legal accountability, and operate according to separate policies, procedures, and**
675 **controls.**

676

677 **3.5.3.2 Notices and User Information**

678 Criteria in this section address the publication of information describing the service and
679 the manner of and any limitations upon its provision, and how users are required to accept
680 those terms.

681 An enterprise and its specified service must:

682 AL3_CO_NUI#010 General Service Definition

683 Make available to the intended user community a Service Definition that includes all
684 applicable Terms, Conditions, and Fees, including any limitations of its usage, and
685 definitions of any terms having specific intention or interpretation. Specific provisions
686 are stated in further criteria in this section.

687 **Guidance:** The intended user community encompasses potential and actual subscribers,
688 subjects and relying parties.

689 AL3_CO_NUI#020 Service Definition inclusions

690 Make available a Service Definition for the specified service containing clauses that
691 provide the following information:

- 692 a) Privacy, Identity Proofing & Verification, and Revocation and Termination
693 Policies;
- 694 b) the country in or the legal jurisdiction under which the service is operated;
- 695 c) if different to the above, the legal jurisdiction under which subscriber and any
696 relying party agreements are entered into;
- 697 d) applicable legislation with which the service complies;
- 698 e) obligations incumbent upon the CSP;
- 699 f) obligations incumbent upon the subscriber;
- 700 g) notifications and guidance for relying parties, especially in respect of actions they
701 are expected to take should they choose to rely upon the service's product;
- 702 h) statement of warranties;
- 703 i) statement of liabilities toward both Subjects and Relying Parties;
- 704 j) procedures for notification of changes to terms and conditions;
- 705 k) steps the CSP will take in the event that it chooses or is obliged to terminate the
706 service;
- 707 l) availability of the specified service *per se* and of its help desk facility.

708 AL3_CO_NUI#030 Due notification

709 Have in place and follow appropriate policy and procedures to ensure that it notifies
710 subscribers and subjects in a timely and reliable fashion of any changes to the Service
711 Definition and any applicable Terms, Conditions, Fees, and Privacy Policy for the
712 specified service, and provide a clear means by which subscribers and subjects must
713 indicate that they wish to accept the new terms or terminate their subscription.

714 AL3_CO_NUI#040 User Acceptance

715 Require subscribers and subjects to:

- 716 a) indicate, prior to receiving service, that they have read and accept the terms of
717 service as defined in the Service Definition;
- 718 b) at periodic intervals, determined by significant service provision events (e.g.
719 issuance, re-issuance, renewal) and otherwise at least once every five years, re-
720 affirm their understanding and observance of the terms of service;
- 721 c) always provide full and correct responses to requests for information.

722 AL3_CO_NUI#050 Record of User Acceptance

723 Obtain a record (hard-copy or electronic) of the subscriber's and subject's acceptance of
724 the terms and conditions of service, prior to initiating the service and thereafter reaffirm
725 the agreement at periodic intervals, determined by significant service provision events
726 (e.g. re-issuance, renewal) and otherwise at least once every five years.

727 AL3_CO_NUI#060 Withdrawn

728 Withdrawn.

729 AL3_CO_NUI#070 Change of Subscriber Information

730 Require and provide the mechanisms for subscribers and subjects to provide in a timely
731 manner full and correct amendments should any of their recorded information change, as
732 required under the terms of their use of the service, and only after the subscriber's and/or
733 subject's identity has been authenticated.

734 AL3_CO_NUI#080 Withdrawn

735 Withdrawn.

736

737 **3.5.3.3 Information Security Management**

738 These criteria address the way in which the enterprise manages the security of its
739 business, the specified service, and information it holds relating to its user community.
740 This section focuses on the key components that make up a well-established and effective
741 Information Security Management System (ISMS), or other IT security management
742 methodology recognized by a government or professional body.

743 An enterprise and its specified service must:

- 744 AL3_CO_ISM#010 Documented policies and procedures
- 745 Have documented all security-relevant administrative management and technical policies
746 and procedures. The enterprise must ensure that these are based upon recognized
747 standards, published references or organizational guidelines, are adequate for the
748 specified service, and are implemented in the manner intended.
- 749 AL3_CO_ISM#020 Policy Management and Responsibility
- 750 Have a clearly defined managerial role, at a senior level, where full responsibility for the
751 business' security policies is vested and from which review, approval, and promulgation
752 of policy and related procedures is applied and managed. The latest approved versions of
753 these policies must be applied at all times.
- 754 AL3_CO_ISM#030 Risk Management
- 755 Demonstrate a risk management methodology that adequately identifies and mitigates
756 risks related to the specified service and its user community **and must show that a risk
757 assessment review is performed at least once every six months, such as adherence to
758 SAS 70 or [\[IS27001\]](#) method.**
- 759 AL3_CO_ISM#040 Continuity of Operations Plan
- 760 Have and keep updated a continuity of operations plan that covers disaster recovery and
761 the resilience of the specified service **and must show that a review of this plan is
762 performed at least once every six months.**
- 763 AL3_CO_ISM#050 Configuration Management
- 764 Demonstrate that there is in place a configuration management system that at least
765 includes:
- 766 a) version control for software system components;
767 b) timely identification and installation of all organizationally-approved patches for
768 any software used in the provisioning of the specified service;
769 c) **version control and managed distribution for all documentation associated
770 with the specification, management, and operation of the system, covering
771 both internal and publicly available materials.**
- 772 AL3_CO_ISM#060 Quality Management
- 773 Demonstrate that there is in place a quality management system that is appropriate for the
774 specified service.

775 AL3_CO_ISM#070 System Installation and Operation Controls

776 Apply controls during system development, procurement, installation, and operation that
777 protect the security and integrity of the system environment, hardware, software, and
778 communications **having particular regard to:**

- 779 a) **the software and hardware development environments, for customized**
- 780 **components;**
- 781 b) **the procurement process for commercial off-the-shelf (COTS) components;**
- 782 c) **contracted consultancy/support services;**
- 783 d) **shipment of system components;**
- 784 e) **storage of system components;**
- 785 f) **installation environment security;**
- 786 g) **system configuration;**
- 787 h) **transfer to operational status.**

788 AL3_CO_ISM#080 Internal Service Audit

789 Be audited at least once every 12 months for effective provision of the specified service
790 by independent internal audit functions of the enterprise responsible for the specified
791 service, unless it can show that by reason of its organizational size or due to other
792 **justifiable** operational restrictions it is unreasonable to be so audited.

793 AL3_CO_ISM#090 Independent Audit

794 Be audited by an independent auditor at least every 24 months to ensure the
795 organization's security-related practices are consistent with the policies and procedures
796 for the specified service.

797 **Guidance:** The appointed auditor should have appropriate accreditation or other
798 acceptable experience and qualification, comparable to that required of Kantara-
799 Accredited Assessors. It is expected that it will be cost-effective for the organization to
800 use the same Kantara-Accredited Assessor for the purposes of fulfilling this criterion as
801 they do for the maintenance of their grant of Kantara Recognition.

802 AL3_CO_ISM#100 Audit Records

803 Retain records of all audits, both internal and independent, for a period which, as a
804 minimum, fulfills its legal obligations and otherwise for greater periods either as it may
805 have committed to in its Service Definition or required by any other obligations it has
806 with/to a subscriber, and which in any event is not less than 36 months. Such records
807 must be held securely and be protected against unauthorized access, loss, alteration,
808 public disclosure, or unapproved destruction.

809 AL3_CO_ISM#110 Termination provisions

810 This is now AL3_CO_ESM#055.

811 AL3_CO_ISM#120 Best Practice Security Management

812 **Have in place an Information Security Management System (ISMS), or other IT**
813 **security management methodology recognized by a government or professional**
814 **body, that follows best practices as accepted by the information security industry**
815 **and that applies and is appropriate to the CSP in question. All requirements**
816 **expressed in preceding criteria in this section must *inter alia* fall wholly within the**
817 **scope of this ISMS or selected recognized alternative.**

818

819 **3.5.3.4 Security-Relevant Event (Audit) Records**

820 The criteria in this section are concerned with the need to provide an auditable log of all
821 events that are pertinent to the correct and secure operation of the service.

822 An enterprise and its specified service must:

823 AL3_CO_SER#010 Security Event Logging

824 Maintain a log of all relevant security events concerning the operation of the service,
825 together with an accurate record of the time at which the event occurred (time-stamp),
826 and retain such records with appropriate protection and controls to ensure successful
827 retrieval, accounting for Service Definition risk management requirements, applicable
828 legislation, and organizational policy.

829 **Guidance:** It is sufficient that the accuracy of the time source is based upon an internal
830 computer/system clock synchronized to an internet time source. The time source need
831 not be authenticatable.

832

833 **3.5.3.5 Operational Infrastructure**

834 The criteria in this section address the infrastructure within which the delivery of the
835 specified service takes place. It puts particular emphasis upon the personnel involved,
836 and their selection, training, and duties.

837 An enterprise and its specified service must:

838 AL3_CO_OPN#010 Technical security

839 Demonstrate that the technical controls employed will provide the level of security
840 protection required by the risk assessment and the ISMS, or other IT security
841 management methods recognized by a government or professional body, and that these

842 controls are effectively integrated with the applicable procedural and physical security
843 measures.

844 **Guidance:** Appropriate technical controls, suited to this Assurance Level, should be
845 selected from [[NIST800-63](#)] or its equivalent, as established by a recognized national
846 technical authority.

847 AL3_CO_OPN#020 Defined security roles

848 Define, by means of a job description, the roles and responsibilities for each service-
849 related security-relevant task, relating it to specific procedures (which shall be set out in
850 the ISMS, or other IT security management methodology recognized by a government or
851 professional body) and other service-related job descriptions. Where the role is security-
852 critical or where special privileges or shared duties exist, these must be specifically
853 identified as such, including the applicable access privileges relating to logical and
854 physical parts of the service's operations.

855 AL3_CO_OPN#030 Personnel recruitment

856 Demonstrate that it has defined practices for the selection, vetting, and contracting of all
857 service-related personnel, both direct employees and those whose services are provided
858 by third parties. **Full records of all searches and supporting evidence of qualifications
859 and past employment must be kept for the duration of the individual's employment
860 plus the longest lifespan of any credential issued under the Service Policy.**

861 AL3_CO_OPN#040 Personnel skills

862 Ensure that employees are sufficiently trained, qualified, experienced, and current for the
863 roles they fulfill. Such measures must be accomplished either by recruitment practices or
864 through a specific training program. Where employees are undergoing on-the-job
865 training, they must only do so under the guidance of a mentor possessing the defined
866 service experiences for the training being provided.

867 AL3_CO_OPN#050 Adequacy of Personnel resources

868 Have sufficient staff to adequately operate and resource the specified service according to
869 its policies and procedures.

870 AL3_CO_OPN#060 Physical access control

871 Apply physical access control mechanisms to ensure that:

- 872 a) access to sensitive areas is restricted to authorized personnel;
- 873 b) all removable media and paper documents containing sensitive information as
874 plain-text are stored in secure containers;

875 c) there is 24/7 monitoring for unauthorized intrusions.

876 AL3_CO_OPN#070 Logical access control

877 Employ logical access control mechanisms that ensure access to sensitive system
878 functions and controls is restricted to authorized personnel.

879

880 3.5.3.6 External Services and Components

881 This section addresses the relationships and obligations upon contracted parties both to
882 apply the policies and procedures of the enterprise and also to be available for assessment
883 as critical parts of the overall service provision.

884 An enterprise and its specified service must:

885 AL3_CO_ESC#010 Contracted policies and procedures

886 Where the enterprise uses external suppliers for specific packaged components of the
887 service or for resources which are integrated with its own operations and under its
888 control, ensure that those parties are engaged through reliable and appropriate contractual
889 arrangements which stipulate which critical policies, procedures, and practices sub-
890 contractors are required to fulfill.

891 AL3_CO_ESC#020 Visibility of contracted parties

892 Where the enterprise uses external suppliers for specific packaged components of the
893 service or for resources which are integrated with its own operations and under its
894 controls, ensure that the suppliers' compliance with contractually-stipulated policies and
895 procedures, and thus with the IAF Service Assessment Criteria, can be independently
896 verified, and subsequently monitored if necessary.

897

898 3.5.3.7 Secure Communications

899 An enterprise and its specified service must:

900 AL3_CO_SCO#010 Secure remote communications

901 If the specific service components are located remotely from and communicate over a
902 public or unsecured network with other service components or other CSPs it services, the
903 communications must be cryptographically authenticated, including long-term and
904 session tokens, by an authentication protocol that meets, at a minimum, the requirements
905 of AL3 and encrypted using **either a FIPS 140-2 [FIPS140-2] Level 2 (or higher)**
906 **validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 validated**

907 **cryptographic module**, or equivalent, as established by a recognized national technical
908 authority.

909 AL3_CO_SCO#020 Limited access to shared secrets

910 Ensure that:

- 911 a) access to shared secrets shall be subject to discretionary controls that permit
912 access to those roles/applications requiring such access;
- 913 b) stored shared secrets are **encrypted such that:**
- 914 i the encryption key for the shared secret file is encrypted under a key
915 held in either a FIPS 140-2 [FIPS140-2] Level 2 (or higher) validated
916 hardware cryptographic module or any FIPS 140-2 Level 3 or 4
917 validated cryptographic module, or equivalent, as established by a
918 recognized national technical authority, and decrypted only as
919 immediately required for an authentication operation;
- 920 ii they are protected as a key within the boundary of either a FIPS 140-2
921 Level 2 (or higher) validated hardware cryptographic module or any
922 FIPS 140-2 Level 3 or 4 validated cryptographic module, or
923 equivalent, as established by a recognized national technical
924 authority, and are not exported from the module in plaintext;
- 925 iii they are split by an "*n from m*" cryptographic secret-sharing method;
- 926 c) any long-term (i.e., not session) shared secrets are revealed only to the subscriber
927 and the CSP's direct agents (bearing in mind (a) above).
- 928

929 **These roles should be defined and documented by the CSP in accordance with**
930 **AL3_CO_OPN#020 above.**

931

932 **3.5.4 Assurance Level 4**

933 Achieving AL4 requires meeting even more stringent criteria in addition to the criteria
934 required to achieve AL3.

935 **3.5.4.1 Enterprise and Service Maturity**

936 Criteria in this section address the establishment of the enterprise offering the service and
937 its basic standing as a legal and operational business entity.

938 An enterprise and its specified service must:

939 AL4_CO_ESM#010 Established enterprise

940 Be a valid legal entity and a person with legal authority to commit the organization must
941 submit the signed assessment package.

942 AL4_CO_ESM#020 Established service

943 Be fully operational in all areas described in the assessment package submitted for
944 assessment.

945 AL4_CO_ESM#030 Legal & Contractual compliance

946 Demonstrate that it understands and complies with any legal requirements incumbent on
947 it in connection with operation and delivery of the specified service, accounting for all
948 jurisdictions within which its services may be offered. Any specific contractual
949 requirements shall also be identified.

950 **Guidance:** Kantara Initiative will not recognize a service which is not fully released for
951 the provision of services to its intended user/client community. Systems, or parts thereof,
952 which are not fully proven and released shall not be considered in an assessment and
953 therefore should not be included within the scope of the assessment package. Parts of
954 systems still under development, or even still being planned, are therefore ineligible for
955 inclusion within the scope of assessment.

956 AL4_CO_ESM#040 Financial Provisions

957 Provide documentation of financial resources that allow for the continued operation of the
958 service and demonstrate appropriate liability processes and procedures that satisfy the
959 degree of liability exposure being carried.

960 **Guidance:** The organization must show that it has a budgetary provision to operate the
961 service for at least a twelve-month period, with a clear review of the budgetary planning
962 within that period so as to keep the budgetary provisions extended. It must also show
963 how it has determined the degree of liability protection required, in view of its exposure

964 per ‘service’ and the number of users it has. This criterion helps ensure that Kantara
965 Initiative does not grant Recognition to services that are not likely to be sustainable over
966 at least this minimum period of time.

967 AL4_CO_ESM#050 Data Retention and Protection

968 Specifically set out and demonstrate that it understands and complies with those legal and
969 regulatory requirements incumbent upon it concerning the retention and destruction of
970 private and identifiable information (personal and business) (i.e. its secure storage and
971 protection against loss, accidental public exposure, and/or improper destruction) and the
972 protection of private information (against unlawful or unauthorized access excepting that
973 permitted by the information owner or required by due process).

974 Termination provisions

975 Define the practices in place for the protection of subscribers’ private and secret
976 information related to their use of the service which must ensure the ongoing secure
977 preservation and protection of legally required records and for the secure destruction and
978 disposal of any such information whose retention is no longer legally required. Specific
979 details of these practices must be made available.

980 **Guidance:** Termination covers the cessation of the business activities, the service
981 provider itself ceasing business operations altogether, change of ownership of the service-
982 providing business, and other similar events which change the status and/or operations of
983 the service provider in any way which interrupts the continued provision of the specific
984 service.

985 AL4_CO_ESM#060 Ownership

986 If the enterprise named as the CSP is a part of a larger entity, the nature of the relationship
987 with its parent organization, shall be disclosed to the assessors and, on their request, to
988 customers.

989 AL4_CO_ESM#070 Independent Management and Operations

990 Demonstrate that, for the purposes of providing the specified service, its management and
991 operational structures are distinct, autonomous, have discrete legal accountability, and
992 operate according to separate policies, procedures, and controls.

993

994 **3.5.4.2 Notices and Subscriber Information/Agreements**

995 Criteria in this section address the publication of information describing the service and
996 the manner of and any limitations upon its provision, and how users are required to accept
997 those terms.

998 An enterprise and its specified service must:

999 AL4_CO_NUI#010 General Service Definition

1000 Make available to the intended user community a Service Definition that includes all
1001 applicable Terms, Conditions, and Fees, including any limitations of its usage, and
1002 definitions of any terms having specific intention or interpretation. Specific provisions
1003 are stated in further criteria in this section.

1004 **Guidance:** The intended user community encompasses potential and actual subscribers,
1005 subjects, and relying parties.

1006 AL4_CO_NUI#020 Service Definition inclusions

1007 Make available a Service Definition for the specified service containing clauses that
1008 provide the following information:

- 1009 a) Privacy, Identity Proofing & Verification, and Revocation and Termination
1010 Policies;
- 1011 b) the country in or legal jurisdiction under which the service is operated;
- 1012 c) if different to the above, the legal jurisdiction under which subscriber and any
1013 relying party agreements are entered into;
- 1014 d) applicable legislation with which the service complies;
- 1015 e) obligations incumbent upon the CSP;
- 1016 f) obligations incumbent upon the subscriber;
- 1017 g) notifications and guidance for relying parties, especially in respect of actions they
1018 are expected to take should they choose to rely upon the service's product;
- 1019 h) statement of warranties;
- 1020 i) statement of liabilities toward both Subjects and Relying Parties;
- 1021 j) procedures for notification of changes to terms and conditions;
- 1022 k) steps the CSP will take in the event that it chooses or is obliged to terminate the
1023 service;
- 1024 l) availability of the specified service per se and of its help desk facility.

1025 AL4_CO_NUI#030 Due Notification

1026 Have in place and follow appropriate policy and procedures to ensure that it notifies
1027 subscribers and subjects in a timely and reliable fashion of any changes to the Service
1028 Definition and any applicable Terms, Conditions, Fees, and Privacy Policy for the
1029 specified service, and provide a clear means by which subscribers and subjects must
1030 indicate that they wish to accept the new terms or terminate their subscription.

1031 AL4_CO_NUI#040 User Acceptance

1032 Require subscribers and subjects to:

- 1033 a) indicate, prior to receiving service, that they have read and accept the terms of
1034 service as defined in the Service Definition, thereby indicating their properly-
1035 informed opt-in;
1036 b) at periodic intervals, determined by significant service provision events (e.g.
1037 issuance, re-issuance, renewal) and otherwise at least once every five years, re-
1038 affirm their understanding and observance of the terms of service;
1039 c) always provide full and correct responses to requests for information.

1040 AL4_CO_NUI#050 Record of User Acceptance

1041 Obtain a record (hard-copy or electronic) of the subscriber's and subject's acceptance of
1042 the terms and conditions of service, prior to initiating the service and thereafter reaffirm
1043 the agreement at periodic intervals, determined by significant service provision events
1044 (e.g. issuance, re-issuance, renewal) and otherwise at least once every five years.

1045 AL4_CO_NUI#060 Withdrawn

1046 Withdrawn.

1047 AL4_CO_NUI#070 Change of Subscriber Information

1048 Require and provide the mechanisms for subscribers and subjects to provide in a timely
1049 manner full and correct amendments should any of their recorded information change, as
1050 required under the terms of their use of the service, and only after the subscriber's and/or
1051 subject's identity has been authenticated.

1052 AL4_CO_NUI#080 Withdrawn

1053 Withdrawn.

1054

1055 3.5.4.3 Information Security Management

1056 These criteria address the way in which the enterprise manages the security of its
1057 business, the specified service, and information it holds relating to its user community.

1058 This section focuses on the key components that comprise a well-established and
1059 effective Information Security Management System (ISMS), or other IT security
1060 management methodology recognized by a government or professional body.

1061 An enterprise and its specified service must:

1062 AL4_CO_ISM#010 Documented policies and procedures

1063 Have documented all security-relevant administrative, management, and technical
1064 policies and procedures. The enterprise must ensure that these are based upon recognized

1065 standards, published references, or organizational guidelines, are adequate for the
1066 specified service, and are implemented in the manner intended.

1067 AL4_CO_ISM#020 Policy Management and Responsibility

1068 Have a clearly defined managerial role, at a senior level, where full responsibility for the
1069 business' security policies is vested and from which review, approval, and promulgation
1070 of policy and related procedures is applied and managed. The latest approved versions of
1071 these policies must be applied at all times.

1072 AL4_CO_ISM#030 Risk Management

1073 Demonstrate a risk management methodology that adequately identifies and mitigates
1074 risks related to the specified service and its user community and must show that on-going
1075 risk assessment review is conducted as a part of the business' procedures, such as
1076 adherence to SAS 70 or [\[IS27001\]](#) methods.

1077 AL4_CO_ISM#040 Continuity of Operations Plan

1078 Have and keep updated a continuity of operations plan that covers disaster recovery and
1079 the resilience of the specified service and must show that **on-going review of this plan is**
1080 **conducted as a part of the business' procedures.**

1081 AL4_CO_ISM#050 Configuration Management

1082 Demonstrate that there is in place a configuration management system that at least
1083 includes:

- 1084 a) version control for software system components;
- 1085 b) timely identification and installation of all organizationally-approved patches for
1086 any software used in the provisioning of the specified service;
- 1087 c) version control and managed distribution for all documentation associated with
1088 the specification, management, and operation of the system, covering both
1089 internal and publicly available materials.

1090 AL4_CO_ISM#060 Quality Management

1091 Demonstrate that there is in place a quality management system that is appropriate for the
1092 specified service.

1093 AL4_CO_ISM#070 System Installation and Operation Controls

1094 Apply controls during system development, procurement, installation, and operation that
1095 protect the security and integrity of the system environment, hardware, software, and
1096 communications having particular regard to:

- 1097 a) the software and hardware development environments, for customized
1098 components;
- 1099 b) the procurement process for commercial off-the-shelf (COTS) components;
- 1100 c) contracted consultancy/support services;
- 1101 d) shipment of system components;
- 1102 e) storage of system components;
- 1103 f) installation environment security;
- 1104 g) system configuration;
- 1105 h) transfer to operational status.
- 1106 AL4_CO_ISM#080 Internal Service Audit
- 1107 Be audited at least once every 12 months for effective provision of the specified service
1108 by independent internal audit functions of the enterprise responsible for the specified
1109 service, unless it can show that by reason of its organizational size or due to other
1110 justifiable operational restrictions it is unreasonable to be so audited.
- 1111 AL4_CO_ISM#090 Independent Audit
- 1112 Be audited by an independent auditor at least every 24 months to ensure the
1113 organization's security-related practices are consistent with the policies and procedures
1114 for the specified service.
- 1115 **Guidance:** The appointed auditor should have appropriate accreditation or other
1116 acceptable experience and qualification, comparable to that required of Kantara-
1117 Accredited Assessors. It is expected that it will be cost-effective for the organization to
1118 use the same Kantara-Accredited Assessor for the purposes of fulfilling this criterion as
1119 they do for the maintenance of their grant of Kantara Recognition.
- 1120 AL4_CO_ISM#100 Audit Records
- 1121 Retain records of all audits, both internal and independent, for a period which, as a
1122 minimum, fulfills its legal obligations and otherwise for greater periods either as it may
1123 have committed to in its Service Definition or required by any other obligations it has
1124 with/to a subscriber, and which in any event is not less than 36 months. Such records
1125 must be held securely and be protected against unauthorized access loss, alteration, public
1126 disclosure, or unapproved destruction.
- 1127 AL4_CO_ISM#110 Termination provisions
- 1128 This is now AL4_CO_ESM#055.

1129 AL4_CO_ISM#120 Best Practice Security Management

1130 Have in place a certified Information Security Management System (ISMS), or other IT
1131 security management methodology recognized by a government or professional body,
1132 that **has been assessed and found to be in compliance with the requirements of**
1133 **ISO/IEC 27001 [IS27001] and which applies and is appropriate to the CSP in**
1134 **question.** All requirements expressed in preceding criteria in this section must *inter alia*
1135 fall wholly within the scope of this ISMS, or the selected recognized alternative.

1136

1137 3.5.4.4 Security-Related (Audit) Records

1138 The criteria in this section are concerned with the need to provide an auditable log of all
1139 events that are pertinent to the correct and secure operation of the service.

1140 An enterprise and its specified service must:

1141 AL4_CO_SER#010 Security Event Logging

1142 Maintain a log of all relevant security events concerning the operation of the service,
1143 together with a **precise** record of the time at which the event occurred (time-stamp)
1144 **provided by a trusted time-source** and retain such records with appropriate protection
1145 and controls to ensure successful retrieval, accounting for service definition, risk
1146 management requirements, applicable legislation, and organizational policy.

1147 **Guidance:** The trusted time source could be an external trusted service or a network time
1148 server or other hardware timing device. The time source must be not only precise but
1149 authenticatable as well.

1150

1151 3.5.4.5 Operational Infrastructure

1152 The criteria in this section address the infrastructure within which the delivery of the
1153 specified service takes place. It puts particular emphasis upon the personnel involved,
1154 and their selection, training, and duties.

1155 An enterprise and its specified service must:

1156 AL4_CO_OPN#010 Technical Security

1157 Demonstrate that the technical controls employed will provide the level of security
1158 protection required by the risk assessment and the ISMS, or other IT security
1159 management methods recognized by a government or professional body, and that these
1160 controls are effectively integrated with the applicable procedural and physical security
1161 measures.

1162 **Guidance:** Appropriate technical controls, suited to this Assurance Level, should be
1163 selected from [NIST800-63] or its equivalent, as established by a recognized national
1164 technical authority.

1165 AL4_CO_OPN#020 Defined Security Roles

1166 Define, by means of a job description, the roles and responsibilities for each service-
1167 related security-relevant task, relating it to specific procedures (which shall be set out in
1168 the ISMS, or other IT security management methodology recognized by a government or
1169 professional body) and other service-related job descriptions. Where the role is security-
1170 critical or where special privileges or shared duties exist, these must be specifically
1171 identified as such, including the applicable access privileges relating to logical and
1172 physical parts of the service's operations.

1173 AL4_CO_OPN#030 Personnel Recruitment

1174 Demonstrate that it has defined practices for the selection, vetting, and contracting of all
1175 service-related personnel, both direct employees and those whose services are provided
1176 by third parties. Full records of all searches and supporting evidence of qualifications and
1177 past employment must be kept for the duration of the individual's employment plus the
1178 longest lifespan of any credential issued under the Service Policy.

1179 AL4_CO_OPN#040 Personnel skills

1180 Ensure that employees are sufficiently trained, qualified, experienced, and current for the
1181 roles they fulfill. Such measures must be accomplished either by recruitment practices or
1182 through a specific training program. Where employees are undergoing on-the-job
1183 training, they must only do so under the guidance of a mentor possessing the defined
1184 service experiences for the training being provided.

1185 AL4_CO_OPN#050 Adequacy of Personnel resources

1186 Have sufficient staff to adequately operate and resource the specified service according to
1187 its policies and procedures.

1188 AL4_CO_OPN#060 Physical access control

1189 Apply physical access control mechanisms to ensure that:

- 1190 a) access to sensitive areas is restricted to authorized personnel;
- 1191 b) all removable media and paper documents containing sensitive information as
1192 plain-text are stored in secure containers;
- 1193 c) there is 24/7 monitoring for unauthorized intrusions.

1194

1195 AL4_CO_OPN#070 Logical access control

1196 Employ logical access control mechanisms that ensure access to sensitive system
1197 functions and controls is restricted to authorized personnel.

1198

1199 **3.5.4.6 External Services and Components**

1200 This section addresses the relationships and obligations upon contracted parties both to
1201 apply the policies and procedures of the enterprise and also to be available for assessment
1202 as critical parts of the overall service provision.

1203 An enterprise and its specified service must:

1204 AL4_CO_ESC#010 Contracted Policies and Procedures

1205 Where the enterprise uses external suppliers for specific packaged components of the
1206 service or for resources which are integrated with its own operations and under its
1207 control, ensure that those parties are engaged through reliable and appropriate contractual
1208 arrangements which stipulate which critical policies, procedures, and practices sub-
1209 contractors are required to fulfill.

1210 AL4_CO_ESC#020 Visibility of Contracted Parties

1211 Where the enterprise uses external suppliers for specific packaged components of the
1212 service or for resources which are integrated with its own operations and under its
1213 control, ensure that the suppliers' compliance with contractually-stipulated policies and
1214 procedures, and thus with the IAF Service Assessment Criteria, can be independently
1215 verified, and subsequently monitored if necessary.

1216

1217 **3.5.4.7 Secure Communications**

1218 An enterprise and its specified service must:

1219 AL4_CO_SCO#010 Secure remote communications

1220 If the specific service components are located remotely from and communicate over a
1221 public or unsecured network with other service components or other CSPs it services, the
1222 communications must be cryptographically authenticated, including long-term and
1223 session tokens, by an authentication protocol that meets the requirements of AL4 and
1224 encrypted using either a FIPS 140-2 [FIPS140-2] Level 2 (or higher) validated hardware
1225 cryptographic module or any FIPS 140-2 Level 3 or 4 validated cryptographic module, or
1226 equivalent, as established by a recognized national technical authority.

- 1227 AL4_CO_SCO#020 Limited access to shared secrets
- 1228 Ensure that:
- 1229 a) access to shared secrets shall be subject to discretionary controls which permit
1230 access to those roles/applications which need such access;
- 1231 b) stored shared secrets are encrypted such that:
- 1232 i the encryption key for the shared secret file is encrypted under a key held
1233 in a FIPS 140-2 [FIPS140-2] Level 2 (or higher) validated hardware
1234 cryptographic module, or equivalent, as established by a recognized
1235 national technical authority, or any FIPS 140-2 Level 3 or 4 validated
1236 cryptographic module, or equivalent, as established by a recognized
1237 national technical authority, and decrypted only as immediately required
1238 for an authentication operation;
- 1239 ii they are protected as a key within the boundary of a FIPS 140-2 Level 2
1240 (or higher) validated hardware cryptographic module, or equivalent, as
1241 established by a recognized national technical authority, or any
1242 FIPS 140-2 Level 3 or 4 cryptographic module, or equivalent, as
1243 established by a recognized national technical authority, and are not
1244 exported in plaintext from the module;
- 1245 iii they are split by an "*n from m*" cryptographic secret-sharing method;
- 1246 c) any long-term (i.e., not session) shared secrets are revealed only to the subscriber
1247 and the CSP's direct agents (bearing in mind (a) above).
- 1248

1249 **3.5.5 Compliance Tables**

1250 Use the following tables to correlate criteria for a particular Assurance Level (AL) and
1251 the evidence offered to support compliance.

1252 Service providers preparing for an assessment can use the table appropriate to the AL at
1253 which they are seeking approval to correlate evidence with criteria or to justify non-
1254 applicability (e.g., "specific service types not offered").

1255 Assessors can use the tables to record the steps in their assessment and their
1256 determination of compliance or failure.

1257 **Table 3-1. CO-SAC - AL1 Compliance**

Clause	Description	Compliance
AL1_CO_ESM#010	Established enterprise	
AL1_CO_ESM#020	Established service	
AL1_CO_ESM#030	Legal & Contractual compliance	
AL1_CO_ESM#040	No stipulation	
AL1_CO_ESM#040	No stipulation	
AL1_CO_ESM#055	Termination provisions	
AL1_CO_NUI#010	General Service Definition	
AL1_CO_NUI#020	Service Definition inclusions	
AL1_CO_NUI#030	Due notification	
AL1_CO_NUI#040	User Acceptance	
AL1_CO_NUI#050	Record of User Acceptance	
AL1_CO_SCO#020	Limited access to shared secrets	

1258

1259

Table 3-2. CO-SAC - AL2 Compliance

Clause	Description	Compliance
AL2_CO_ESM#010	Established enterprise	
AL2_CO_ESM#020	Established service	
AL2_CO_ESM#030	Legal & Contractual compliance	
AL2_CO_ESM#040	Financial Provisions	
AL2_CO_ESM#050	Data Retention and Protection	
AL2_CO_ESM#055	Termination provisions	
AL2_CO_NUI#010	General Service Definition	
AL2_CO_NUI#020	Service Definition inclusions	
AL2_CO_NUI#030	Due notification	
AL2_CO_NUI#040	User Acceptance	
AL2_CO_NUI#050	Record of User Acceptance	
AL2_CO_NUI#060	Withdrawn	No conformity requirement
AL2_CO_NUI#070	Change of Subscriber Information	
AL2_CO_NUI#080	Withdrawn	No conformity requirement
AL2_CO_ISM#010	Documented policies and procedures	
AL2_CO_ISM#020	Policy Management and Responsibility	
AL2_CO_ISM#030	Risk Management	
AL2_CO_ISM#040	Continuity of Operations Plan	
AL2_CO_ISM#050	Configuration Management	
AL2_CO_ISM#060	Quality Management	
AL2_CO_ISM#070	System Installation and Operation Controls	
AL2_CO_ISM#080	Internal Service Audit	
AL2_CO_ISM#090	Independent Audit	
AL2_CO_ISM#100	Audit Records	
AL2_CO_ISM#110	Termination provisions	Re-assigned as AL2_CO_ESM#055
AL2_CO_SER#010	Security event logging	
AL2_CO_OPN#010	Technical security	
AL2_CO_OPN#020	Defined security roles	
AL2_CO_OPN#030	Personnel recruitment	
AL2_CO_OPN#040	Personnel skills	
AL2_CO_OPN#050	Adequacy of Personnel resources	
AL2_CO_OPN#060	Physical access control	

AL2_CO_OPN#070	Logical access control	
AL2_CO_ESC#010	Contracted policies and procedures	
AL2_CO_ESC#020	Visibility of contracted parties	
AL2_CO_SCO#010	Secure remote communications	
AL2_CO_SCO#015	Verification / Authentication confirmation messages	
AL2_CO_SCO#016	Verification of Revoked Credential	
AL2_CO_SCO#020	Limited access to shared secrets	
AL2_CO_SCO#030	Logical protection of shared secrets	

1260

1261

Table 3-3. CO-SAC - AL3 compliance

Clause	Description	Compliance
AL3_CO_ESM#010	Established enterprise	
AL3_CO_ESM#020	Established service	
AL3_CO_ESM#030	Legal & Contractual compliance	
AL3_CO_ESM#040	Financial Provisions	
AL3_CO_ESM#050	Data Retention and Protection	
AL3_CO_ESM#055	Termination provisions	
AL3_CO_ESM#060	Ownership	
AL3_CO_ESM#070	Independent management and operations	
AL3_CO_NUI#010	General Service Definition	
AL3_CO_NUI#020	Service Definition inclusions	
AL3_CO_NUI#030	Due notification	
AL3_CO_NUI#040	User Acceptance	
AL3_CO_NUI#050	Record of User Acceptance	
AL3_CO_NUI#060	Withdrawn	No conformity requirement
AL3_CO_NUI#070	Change of Subscriber Information	
AL3_CO_NUI#080	Withdrawn	No conformity requirement
AL3_CO_ISM#010	Documented policies and procedures	
AL3_CO_ISM#020	Policy Management and Responsibility	
AL3_CO_ISM#030	Risk Management	
AL3_CO_ISM#040	Continuity of Operations Plan	
AL3_CO_ISM#050	Configuration Management	
AL3_CO_ISM#060	Quality Management	
AL3_CO_ISM# 070	System Installation and Operation Controls	
AL3_CO_ISM#080	Internal Service Audit	
AL3_CO_ISM#090	Independent Audit	
AL3_CO_ISM#100	Audit Records	
AL3_CO_ISM#110	Termination provisions	Re-assigned as AL3_CO_ESM#055
AL3_CO_ISM#120	Best Practice Security Management	
AL3_CO_SER#010	Security Event Logging	
AL3_CO_OPN#010	Technical security	
AL3_CO_OPN#020	Defined security roles	
AL3_CO_OPN#030	Personnel recruitment	

AL3_CO_OPN#040	Personnel skills	
AL3_CO_OPN#050	Adequacy of Personnel resources	
AL3_CO_OPN#060	Physical access control	
AL3_CO_OPN#070	Logical access control	
AL3_CO_ESC#010	Contracted policies and procedures	
AL3_CO_ESC#020	Visibility of contracted parties	
AL3_CO_SCO#010	Secure remote communications	
AL3_CO_SCO#020	Limited access to shared secrets	

1262

1263

Table 3-4. CO-SAC - AL4 compliance

Clause	Description	Compliance
AL4_CO_ESM#010	Established enterprise	
AL4_CO_ESM#020	Established service	
AL4_CO_ESM#030	Legal & Contractual compliance	
AL4_CO_ESM#040	Financial Provisions	
AL4_CO_ESM#050	Data Retention and Protection	
AL4_CO_ESM#055	Termination provisions	
AL4_CO_ESM#060	Ownership	
AL4_CO_ESM#070	Independent Management and Operations	
AL4_CO_NUI#010	General Service Definition	
AL4_CO_NUI#020	Service Definition inclusions	
AL4_CO_NUI#030	Due Notification	
AL4_CO_NUI#040	User Acceptance	
AL4_CO_NUI#050	Record of User Acceptance	
AL4_CO_NUI#060	Withdrawn	No conformity requirement
AL4_CO_NUI#070	Change of Subscriber Information	
AL4_CO_NUI#080	Withdrawn	No conformity requirement
AL4_CO_ISM#010	Documented policies and procedures	
AL4_CO_ISM#020	Policy Management and Responsibility	
AL4_CO_ISM#030	Risk Management	
AL4_CO_ISM#040	Continuity of Operations Plan	
AL4_CO_ISM#050	Configuration Management	
AL4_CO_ISM#060	Quality Management	
AL4_CO_ISM#070	System Installation and Operation Controls	
AL4_CO_ISM#080	Internal Service Audit	
AL4_CO_ISM#090	Independent Audit	
AL4_CO_ISM#100	Audit Records	
AL4_CO_ISM#110	Termination provisions	Re-assigned as AL4_CO_ESM#055
AL4_CO_ISM#120	Best Practice Security Management	
AL4_CO_SER#010	Security Event Logging	
AL4_CO_OPN#010	Technical Security	
AL4_CO_OPN#020	Defined Security Roles	
AL4_CO_OPN#030	Personnel Recruitment	

AL4_CO_OPN#040	Personnel skills	
AL4_CO_OPN#050	Adequacy of Personnel resources	
AL4_CO_OPN#060	Physical access control	
AL4_CO_OPN#070	Logical access control	
AL4_CO_ESC#010	Contracted Policies and Procedures	
AL4_CO_ESC#020	Visibility of Contracted Parties	
AL4_CO_SCO#010	Secure remote communications	
AL4_CO_SCO#020	Limited access to shared secrets	

1264

1265 **3.6 Identity Proofing Service Assessment Criteria**

1266 The Service Assessment Criteria in this section establish the requirements for the
1267 technical conformity of identity proofing services at all ALs defined in Section 2 and in
1268 the [Identity Assurance Framework: Levels of Assurance](#) document. These criteria apply
1269 to a particular kind of electronic trust service (ETS) recognized by the IAWG and to the
1270 related credential service provider (CSP)—an identity proofing service for both
1271 individual identity and institutional identity credentials¹. (For definitions of terms used in
1272 this section, see the [Identity Assurance Framework: Glossary](#) document). These criteria
1273 are generally referred to elsewhere within IAWG documentation as ID-SAC [ID-SAC].

1274 These criteria do not address the delivery of a credential to the applicant/subscriber,
1275 which is dealt with by the Credential Management SAC (CM-SAC), described in Section
1276 3.7.

1277 These criteria may only be used in an assessment in one of the following circumstances:

- 1278 • In conjunction with the Common Organizational SAC (CO-SAC), described in
1279 Section 3.5, for a standalone identity proofing service.
- 1280 • In combination with one or more other SACs that must include the CO-SAC and
1281 where the identity proofing functions that these criteria address form part of a
1282 larger service offering.

1283 **3.6.1 Assurance Level 1**

1284 **3.6.1.1 Policy**

1285 An enterprise or specified service must:

1286 AL1_ID_POL#010 Unique service identity

1287 Ensure that a unique identity is attributed to the specific service, such that credentials
1288 issued by it can be distinguishable from those issued by other services, including services
1289 operated by the same enterprise.

1290 AL1_ID_POL#020 Unique subject identity

1291 Ensure that each applicant's identity is unique within the service's community of subjects
1292 and uniquely associable with tokens and/or credentials issued to that identity.

¹ Identity proofing processes for entities that are not human persons will vary by assurance level and will utilize existing SSL and EV SSL issuance requirements from the CA Browser Forum for the appropriate level of assurance. Non-individual verification requirements will be attached as an appendix to this document.

1293

1294 **3.6.1.2 Identity Verification**

1295 **3.6.1.2.1 In-Person Public Verification**

1296 An enterprise or specified service must:

1297 AL1_ID_IPV#010 Required evidence

1298 Accept a self-assertion of identity.

1299 AL1_ID_IPV#020 Evidence checks

1300 Accept self-attestation of evidence.

1301

1302 **3.6.1.2.2 Remote Public Verification**

1303 If the specific service offers remote identity proofing to applicants with whom it has no
1304 previous relationship, then it must comply with the criteria in this section.

1305 An enterprise or specified service must:

1306 AL1_ID_RPV#010 Required evidence

1307 Require the applicant to provide a contact telephone number or email address.

1308 AL1_ID_RPV#020 Evidence checks

1309 Verify the provided information by either:

1310 a) confirming the request by calling the number;

1311 b) successfully sending a confirmatory email and receiving a positive
1312 acknowledgement.

1313

1314 **3.6.1.2.3 Secondary Verification**

1315 In each of the above cases, an enterprise or specified service must:

1316 AL1_ID_SCV#010 Secondary checks

1317 Have in place additional measures (e.g., require additional documentary evidence, delay
1318 completion while out-of-band checks are undertaken) to deal with any anomalous
1319 circumstances that can be reasonably anticipated (e.g., a legitimate and recent change of
1320 address that has yet to be established as the address of record).

1321

1322 **3.6.2 Assurance Level 2**

1323 **3.6.2.1 Policy**

1324 The specific service must show that it applies identity proofing policies and procedures
1325 and that it retains appropriate records of identity proofing activities and evidence.

1326 The enterprise or specified service must:

1327 AL2_ID_POL#010 Unique service identity

1328 Ensure that a unique identity is attributed to the specific service, such that credentials
1329 issued by it can be distinguishable from those issued by other services, including services
1330 operated by the same enterprise.

1331 AL2_ID_POL#020 Unique subject identity

1332 Ensure that each applicant's identity is unique within the service's community of subjects
1333 and uniquely associable with tokens and/or credentials issued to that identity.

1334 AL2_ID_POL#030 Published Proofing Policy

1335 **For each service it offers, make available the Identity Proofing Policy under which it**
1336 **verifies the identity of applicants² in form, language, and media accessible to the**
1337 **declared community of Users.**

1338 AL2_ID_POL#040 Adherence to Proofing Policy

1339 **Perform all identity proofing strictly in accordance with its published Identity**
1340 **Proofing Policy.**

1341

1342 **3.6.2.2 Identity Verification**

1343 The enterprise or specific service must:

² For an identity proofing service that is within the management scope of a credential management service provider, this should be the credential management service's definitive policy; for a stand-alone identity proofing service, the policy may be either that of a client who has imposed one through contract, the ID service's own policy, or a separate policy that explains how the client's policies will be complied with.

- 1344 AL2_ID_IDV#000 Identity Proofing classes
- 1345 a) include in its Service Definition **at least one** of the following classes of identity
1346 proofing service, and;
- 1347 b) may offer any additional classes of identity proofing service it chooses,
1348 subject to the nature and the entitlement of the CSP concerned;
- 1349 c) Fulfill the applicable assessment criteria according to its choice of identity
1350 proofing service, i.e. conform to at least one of the criteria sets defined in:
- 1351 i) §3.6.2.2.1, “[In-Person Public Verification](#)”;
- 1352 ii) §3.6.2.2.2, “[Remote Public Verification](#)”;
- 1353 iii) §3.6.2.2.3, “[Current Relationship Verification](#)”;
- 1354 iv) §3.6.2.2.4, “[Affiliation Verification](#)”.

1355 **3.6.2.2.1 In-Person Public Verification**

1356 If the specific service offers in-person identity proofing to applicants with whom it has no
1357 previous relationship, then it must comply with the criteria in this section.

1358 The enterprise or specified service must:

1359 AL2_ID_IPV#010 Required evidence

1360 **Ensure that the applicant is in possession of a primary Government Picture ID**
1361 **document that bears a photographic image of the holder.**

1362 AL2_ID_IPV#020 Evidence checks

1363 **Have in place and apply processes which ensure that the presented document:**

- 1364 a) **appears to be a genuine document properly issued by the claimed issuing**
1365 **authority and valid at the time of application;**
- 1366 b) **bears a photographic image of the holder that matches that of the applicant;**
- 1367 c) **provides all reasonable certainty that the identity exists and that it uniquely**
1368 **identifies the applicant.**
- 1369

1370 **3.6.2.2.2 Remote Public Verification**

1371 If the specific service offers remote identity proofing to applicants with whom it has no
1372 previous relationship, then it must comply with the criteria in this section.

1373 An enterprise or specified service must:

1374 AL2_ID_RPV#010 Required evidence

1375 **Ensure that the applicant submits the references of and attests to current possession**
1376 **of a primary Government Picture ID document, and one of:**

- 1377 a) a second Government ID;
1378 b) an employee or student ID number;
1379 c) a financial account number (e.g., checking account, savings account, loan or
1380 credit card) or;
1381 d) a utility service account number (e.g., electricity, gas, or water) for an address
1382 matching that in the primary document.

1383 **Ensure that the applicant provides additional verifiable personal information that at**
1384 **a minimum must include:**

- 1385 a) a name that matches the referenced photo-ID;
1386 b) date of birth and;
1387 c) current address or personal telephone number.

1388 **Additional information may be requested so as to ensure a unique identity, and**
1389 **alternative information may be sought where the enterprise can show that it leads to**
1390 **at least the same degree of certitude when verified.**

1391 AL2_ID_RPV#020 Evidence checks

1392 **Inspection and analysis of records against the provided identity references with the**
1393 **specified issuing authorities/institutions or through similar databases:**

- 1394 a) the existence of such records with matching name and reference numbers;
1395 b) corroboration of date of birth, current address of record, and other personal
1396 information sufficient to ensure a unique identity.

1397
1398

1399 **Confirm address of record by at least one of the following means:**

- 1400 a) RA sends notice to an address of record confirmed in the records check and
1401 receives a mailed or telephonic reply from applicant;
1402 b) RA issues credentials in a manner that confirms the address of record
1403 supplied by the applicant, for example by requiring applicant to enter on-line
1404 some information from a notice sent to the applicant;
1405 c) RA issues credentials in a manner that confirms ability of the applicant to
1406 receive telephone communications at telephone number or email at email
1407 address associated with the applicant in records. Any secret sent over an
1408 unprotected channel shall be reset upon first use.

1409
1410
1411

**Additional checks should be performed so as to establish the uniqueness of the
claimed identity.**

1412 **Alternative checks may be performed where the enterprise can show that they lead**
1413 **to at least the same degree of certitude.**

1414

1415 **3.6.2.2.3 Current Relationship Verification**

1416 If the specific service offers identity proofing to applicants with whom it has a current
1417 relationship, then it must comply with the criteria in this section.

1418 The enterprise or specified service must:

1419 AL2_ID_CRV#010 Required evidence

1420 **Ensure that it has previously exchanged with the applicant a shared secret (e.g., a**
1421 **PIN or password) that meets AL2 (or higher) entropy requirements³.**

1422 AL2_ID_CRV#020 Evidence checks

1423 **Ensure that it has:**

- 1424 a) **only issued the shared secret after originally establishing the applicant’s**
1425 **identity with a degree of rigor equivalent to that required under either the**
1426 **AL2 (or higher) requirements for in-person or remote public verification;**
1427 b) **an ongoing business relationship sufficient to satisfy the enterprise of the**
1428 **applicant’s continued personal possession of the shared secret.**

1429

1430 **3.6.2.2.4 Affiliation Verification**

1431 If the specific service offers identity proofing to applicants on the basis of some form of
1432 affiliation, then it must comply with the criteria in this section for the purposes of
1433 establishing that affiliation, in addition to the previously stated requirements for the
1434 verification of the individual’s identity.

1435 The enterprise or specified service must:

1436 AL2_ID_AFV#000 Meet preceding criteria

1437 **Meet all the criteria set out above, under §3.6.2.2.3, “[Current Relationship](#)**
1438 **[Verification](#)”.**

1439 AL2_ID_AFV#010 Required evidence

1440 **Ensure that the applicant possesses:**

³ Refer to NIST SP 800-63 “Appendix A: Estimating Entropy and Strength” or similar recognized sources of such information.

- 1441 a) **identification from the organization with which it is claiming affiliation;**
1442 b) **agreement from the organization that the applicant may be issued a**
1443 **credential indicating that an affiliation exists.**

1444 AL2_ID_AFV#020 Evidence checks

1445 **Have in place and apply processes which ensure that the presented documents:**

- 1446 a) **each appear to be a genuine document properly issued by the claimed issuing**
1447 **authorities and valid at the time of application;**
1448 b) **refer to an existing organization with a contact address;**
1449 c) **indicate that the applicant has some form of recognizable affiliation with the**
1450 **organization;**
1451 d) **appear to grant the applicant an entitlement to obtain a credential indicating**
1452 **its affiliation with the organization.**
1453

1454 **3.6.2.2.5 Secondary Verification**

1455 In each of the above cases, the enterprise or specified service must:

1456 AL2_ID_SCV#010 Secondary checks

1457 Have in place additional measures (e.g., require additional documentary evidence, delay
1458 completion while out-of-band checks are undertaken) to deal with any anomalous
1459 circumstances that can be reasonably anticipated (e.g., a legitimate and recent change of
1460 address that has yet to be established as the address of record).

1461

1462 **3.6.2.3 Verification Records**

1463 The specific service must retain records of the identity proofing (verification) that it
1464 undertakes and provide them to qualifying parties when so required.

1465 An enterprise or specified service must:

1466 AL2_ID_VRC#010 Verification Records for Personal Applicants

1467 **Log, taking account of all applicable legislative and policy obligations, a record of**
1468 **the facts of the verification process, including a reference relating to the verification**
1469 **processes and the date and time of verification.**

1470 **Guidance:** The facts of the verification process should include the specific record
1471 information (source, unique reference, value/content) used in establishing the applicant's
1472 identity, and will be determined by the specific processes used and documents accepted
1473 by the CSP. The CSP need not retain these records itself if it uses a third-party service
1474 which retains such records securely and to which the CSP has access when required, in

1475 which case it must retain a record of the identity of the third-party service providing the
1476 verification service or the location at which the (in-house) verification was performed.

1477 AL2_ID_VRC#020 Verification Records for Affiliated Applicants

1478 **In addition to the foregoing, log, taking account of all applicable legislative and**
1479 **policy obligations, a record of the additional facts of the verification process must be**
1480 **performed. At a minimum, records of identity information must include:**

- 1481 a) the subscriber's full name;
- 1482 b) the subscriber's current address of record;
- 1483 c) the subscriber's current telephone or email address of record;
- 1484 d) the subscriber's acknowledgement for issuing the subject with a credential;
- 1485 e) type, issuing authority, and reference number(s) of all documents checked in
1486 the identity proofing process.

1487 AL2_ID_VRC#030 Record Retention

1488 **Either retain, securely, the record of the verification process for the duration of the**
1489 **subscriber account plus 7.5 years, or submit same record to a client CSP that has**
1490 **undertaken to retain the record for the requisite period or longer.**

1491

1492 **3.6.3 Assurance Level 3**

1493 **3.6.3.1 Policy**

1494 The specific service must show that it applies identity proofing policies and procedures
1495 and that it retains appropriate records of identity proofing activities and evidence.

1496 The enterprise or specified service must:

1497 AL3_ID_POL#010 Unique service identity

1498 Ensure that a unique identity is attributed to the specific service, such that credentials
1499 issued by it can be distinguishable from those issued by other services, including services
1500 operated by the same enterprise.

1501 AL3_ID_POL#020 Unique subject identity

1502 Ensure that each applicant's identity is unique within the service's community of subjects
1503 and uniquely associable with tokens and/or credentials issued to that identity.

1504 AL3_ID_POL#030 Published Proofing Policy

1505 Make available the Identity Proofing Policy under which it verifies the identity of
1506 applicants⁴ in form, language, and media accessible to the declared community of Users.

1507 AL3_ID_POL#040 Adherence to Proofing Policy

1508 Perform all identity proofing strictly in accordance with its published Identity Proofing
1509 Policy, through application of the procedures and processes set out in its Identity Proofing
1510 Practice Statement.

1511

1512 **3.6.3.2 Identity Verification**

1513 The enterprise or specific service must:

⁴ For an identity proofing service that is within the management scope of a Credential Management service provider, this should be the Credential Management service's definitive policy; for a stand-alone identity proofing service, the policy may be either that of a client who has defined one through contract, the ID service's own policy or a separate policy that explains how the client's policies will be complied with.

- 1514 AL3_ID_IDV#000 Identity Proofing classes
- 1515 a) include in its Service Definition at least one of the following classes of identity
1516 proofing services, and;
- 1517 b) may offer any additional classes of identity proofing service it chooses, subject to
1518 the nature and the entitlement of the CSP concerned;
- 1519 c) Fulfill the applicable assessment criteria according to its choice of identity
1520 proofing service, i.e. conform to at least one of the criteria sets defined in:
- 1521 i) §3.6.3.2.1, “[In-Person Public Verification](#)”;
- 1522 ii) §3.6.3.2.2, “[Remote Public Verification](#)”;
- 1523 iii) §3.6.3.2.4, “[Affiliation Verification](#)”.
- 1524

1525 **3.6.3.2.1 In-Person Public Verification**

1526 A specific service that offers identity proofing to applicants with whom it has no previous
1527 relationship must comply with the criteria in this section.

1528 The enterprise or specified service must:

- 1529 AL3_ID_IPV#010 Required evidence
- 1530 Ensure that the applicant is in possession of a primary Government Picture ID document
1531 that bears a photographic image of the holder.

1532 AL3_ID_IPV#020 Evidence checks

1533 **Have in place and apply processes which ensure** that the presented document:

- 1534 a) appears to be a genuine document properly issued by the claimed issuing
1535 authority and valid at the time of application;
- 1536 b) bears a photographic image of the holder that matches that of the applicant;
- 1537 c) **is electronically verified by a record check with the specified issuing
1538 authority or through similar databases that:**
- 1539 i) **establishes the existence of such records with matching name and
1540 reference numbers;**
- 1541 ii) **corroborates date of birth, current address of record, and other
1542 personal information sufficient to ensure a unique identity;**
- 1543 d) provides all reasonable certainty that the identity exists and that it uniquely
1544 identifies the applicant.
- 1545

1546 **3.6.3.2.2 Remote Public Verification**

1547 A specific service that offers remote identity proofing to applicants with whom it has no
1548 previous relationship must comply with the criteria in this section.

1549 The enterprise or specified service must:

1550 AL3_ID_RPV#010 Required evidence

1551 Ensure that the applicant submits the references of and attests to current possession of a
1552 primary Government Picture ID document, and one of:

- 1553 a) a second Government ID;
- 1554 b) an employee or student ID number;
- 1555 c) a financial account number (e.g., checking account, savings account, loan, or
1556 credit card), or;
- 1557 d) a utility service account number (e.g., electricity, gas, or water) for an address
1558 matching that in the primary document.

1559 Ensure that the applicant provides additional verifiable personal information that at a
1560 minimum must include:

- 1561 e) a name that matches the referenced photo-ID;
- 1562 f) date of birth;
- 1563 g) current address or personal telephone number.

1564 Additional information may be requested so as to ensure a unique identity, and alternative
1565 information may be sought where the enterprise can show that it leads to at least the same
1566 degree of certitude when verified.

1567

1568 AL3_ID_RPV#020 Evidence checks

1569 **Electronically verify by a record check against the provided identity references with**
1570 **the specified issuing authorities/institutions or through similar databases:**

- 1571 a) the existence of such records with matching name and reference numbers;
- 1572 b) corroboration of date of birth, current address of record, **or personal telephone**
1573 **number**, and other personal information sufficient to ensure a unique identity;
- 1574 c) **dynamic verification of personal information previously provided by or**
1575 **likely to be known only by the applicant.**

1576

1577

1578 Confirm address of record by at least one of the following means:

- 1579 a) RA sends notice to an address of record confirmed in the records check and
1580 receives a mailed or telephonic reply from applicant;

- 1581 b) RA issues credentials in a manner that confirms the address of record supplied by
1582 the applicant, for example by requiring applicant to enter on-line some
1583 information from a notice sent to the applicant;
1584 c) RA issues credentials in a manner that confirms ability of the applicant to receive
1585 telephone communications at telephone number or email at email address
1586 associated with the applicant in records. Any secret sent over an unprotected
1587 channel shall be reset upon first use.
1588
1589 Additional checks may be performed so as to establish the uniqueness of the claimed
1590 identity, and alternative checks may be performed where the enterprise can show that they
1591 lead to at least the same degree of certitude.

1592 **3.6.3.2.3 Current Relationship Verification**

1593 No stipulation.

1594

1595 **3.6.3.2.4 Affiliation Verification**

1596 A specific service that offers identity proofing to applicants on the basis of some form of
1597 affiliation must comply with the criteria in this section to establish that affiliation and
1598 with the previously stated requirements to verify the individual's identity.

1599 The enterprise or specified service must:

1600 AL3_ID_AFV#000 Meet preceding criteria

1601 Meet all the criteria set out above, under §3.6.3.2.2, "[Remote Public Verification](#)".

1602 AL3_ID_AFV#010 Required evidence

1603 Ensure that the applicant possesses:

- 1604 a) identification from the organization with which it is claiming affiliation;
1605 b) agreement from the organization that the applicant may be issued a credential
1606 indicating that an affiliation exists.

1607 AL3_ID_AFV#020 Evidence checks

1608 Have in place and apply processes which ensure that the presented documents:

- 1609 a) each appear to be a genuine document properly issued by the claimed issuing
1610 authorities and valid at the time of application;
1611 b) refer to an existing organization with a contact address;
1612 c) indicate that the applicant has some form of recognizable affiliation with the
1613 organization;

- 1614 d) appear to grant the applicant an entitlement to obtain a credential indicating an
1615 affiliation with the organization.
1616

1617 **3.6.3.2.5 Secondary Verification**

1618 In each of the above cases, the enterprise or specified service must also meet the
1619 following criteria:

1620 AL3_ID_SCV#010 Secondary checks

1621 Have in place additional measures (e.g., require additional documentary evidence, delay
1622 completion while out-of-band checks are undertaken) to deal with any anomalous
1623 circumstance that can reasonably be anticipated (e.g., a legitimate and recent change of
1624 address that has yet to be established as the address of record).

1625 **3.6.3.3 Verification Records**

1626 The specific service must retain records of the identity proofing (verification) that it
1627 undertakes and provide them to qualifying parties when so required.

1628 The enterprise or specified service must:

1629 AL3_ID_VRC#010 Verification Records for Personal Applicants

1630 Log, taking account of all applicable legislative and policy obligations, a record of the
1631 facts of the verification process **and the identity of the registrar**, including a reference
1632 relating to the verification processes and the date and time of verification.

1633 **Guidance:** The facts of the verification process should include the specific record
1634 information (source, unique reference, value/content) used in establishing the applicant's
1635 identity, and will be determined by the specific processes used and documents accepted
1636 by the CSP. The CSP need not retain these records itself if it uses a third-party service
1637 which retains such records securely and to which the CSP has access when required, in
1638 which case it must retain a record of the identity of the third-party service providing the
1639 verification service or the location at which the (in-house) verification was performed.

1640 AL3_ID_VRC#020 Verification Records for Affiliated Applicants

1641 In addition to the foregoing, log, taking account of all applicable legislative and policy
1642 obligations, a record of the additional facts of the verification process must be performed.
1643 At a minimum, records of identity information must include:

- 1644 a) the 'full name;
1645 b) the subscriber's current address of record;
1646 c) the subscriber's current telephone or email address of record;
1647 d) the subscriber's acknowledgement of issuing the subject with a credential;

- 1648 e) type, issuing authority, and reference number(s) of all documents checked in the
1649 identity proofing process;
1650 f) **where required, a telephone or email address for related contact and/or**
1651 **delivery of credentials/notifications.**

1652 AL3_ID_VRC#030 Record Retention

1653 Either retain, securely, the record of the verification/revocation process for the duration of
1654 the subscriber account plus 7.5 years, or submit the same record to a client CSP that has
1655 undertaken to retain the record for the requisite period or longer.

1656

1657 **3.6.4 Assurance Level 4**

1658 Identity proofing at Assurance Level 4 requires the physical presence of the applicant in
1659 front of the registration officer with photo ID or other readily verifiable biometric identity
1660 information, as well as the requirements set out by the following criteria.

1661 **3.6.4.1 Policy**

1662 The specific service must show that it applies identity proofing policies and procedures
1663 and that it retains appropriate records of identity proofing activities and evidence.

1664 The enterprise or specified service must:

1665 AL4_ID_POL#010 Unique service identity

1666 Ensure that a unique identity is attributed to the specific service, such that credentials
1667 issued by it can be distinguishable from those issued by other services, including services
1668 operated by the same enterprise.

1669 AL4_ID_POL#020 Unique subject identity

1670 Ensure that each applicant's identity is unique within the service's community of subjects
1671 and uniquely associable with tokens and/or credentials issued to that identity.

1672 AL4_ID_POL#030 Published Proofing Policy

1673 Make available the Identity Proofing Policy under which it verifies the identity of
1674 applicants⁵ in form, language, and media accessible to the declared community of users.

1675 AL4_ID_POL#040 Adherence to Proofing Policy

1676 Perform all identity proofing strictly in accordance with its published Identity Proofing
1677 Policy, through application of the procedures and processes set out in its Identity Proofing
1678 Practice Statement.

1679

1680 **3.6.4.2 Identity Verification**

1681 The enterprise or specific service may:

⁵ For an identity proofing service that is within the management scope of a credential management service provider, this should be the credential management service's definitive policy; for a stand-alone identity proofing service, the policy may be either that of a client which has defined one through contract, the ID service's own policy or a separate policy that explains how the client's policies will be complied with.

- 1682 AL4_ID_IDV#000 Identity Proofing classes
- 1683 **[Omitted] offer only face-to-face identity proofing service. Remote verification is not**
1684 **allowed at this assurance level;**
- 1685
- 1686 The enterprise or specified service must:
- 1687 **3.6.4.2.1 In-Person Public Verification**
- 1688 AL4_ID_IPV#010 Required evidence
- 1689 Ensure that the applicant is in possession of:
- 1690 a) a primary Government Picture ID document that bears a photographic image of
1691 the **holder and either:**
- 1692 i) **secondary Government Picture ID or an account number issued by a**
1693 **regulated financial institution or;**
- 1694 ii) **two items confirming name, and address or telephone number, such**
1695 **as: utility bill, professional license or membership, or other evidence**
1696 **of equivalent standing.**
- 1697 AL4_ID_IPV#020 No stipulation
- 1698 AL4_ID_IPV#030 Evidence checks – primary ID
- 1699 **Ensure that the presented document:**
- 1700 a) **appears to be a genuine document properly issued by the claimed issuing**
1701 **authority and valid at the time of application;**
- 1702 b) **bears a photographic image of the holder which matches that of the**
1703 **applicant;**
- 1704 c) **is electronically verified by a record check with the specified issuing**
1705 **authority or through similar databases that:**
- 1706 i) **establishes the existence of such records with matching name and**
1707 **reference numbers;**
- 1708 ii) **corroborates date of birth, current address of record, and other**
1709 **personal information sufficient to ensure a unique identity;**
- 1710 d) **provides all reasonable certainty, at AL4, that the identity exists and that it**
1711 **uniquely identifies the applicant.**
- 1712 AL4_ID_IPV#040 Evidence checks – secondary ID
- 1713 **Ensure that the presented document meets the following conditions:**
- 1714 a) **If it is secondary Government Picture ID:**

- 1715 i) appears to be a genuine document properly issued by the claimed
1716 issuing authority and valid at the time of application;
1717 ii) bears a photographic image of the holder which matches that of the
1718 applicant;
1719 iii) states an address at which the applicant can be contacted.
1720 b) If it is a financial institution account number, is verified by a record check
1721 with the specified issuing authority or through similar databases that:
1722 i) establishes the existence of such records with matching name and
1723 reference numbers;
1724 ii) corroborates date of birth, current address of record, and other
1725 personal information sufficient to ensure a unique identity.
1726 c) If it is two utility bills or equivalent documents:
1727 i) each appears to be a genuine document properly issued by the
1728 claimed issuing authority;
1729 ii) corroborates current address of record or telephone number
1730 sufficient to ensure a unique identity.

1731 AL4_ID_IPV#050 Applicant knowledge checks

1732 Where the applicant is unable to satisfy any of the above requirements, that the
1733 applicant can provide a unique identifier, such as a Social Security Number (SSN),
1734 that matches the claimed identity.

1735

1736 3.6.4.2.2 Remote Public Verification

1737 Not permitted

1738 3.6.4.2.3 Affiliation Verification

1739 A specific service that offers identity proofing to applicants on the basis of some form of
1740 affiliation must comply with the criteria in this section to establish that affiliation, in
1741 addition to complying with the previously stated requirements for verifying the
1742 individual's identity.

1743 The enterprise or specified service must:

1744 AL4_ID_AFV#000 Meet preceding criteria

1745 Meet all the criteria set out above, under §3.6.4.2.1, "[In-Person Public Verification](#)".

1746 AL4_ID_AFV#010 Required evidence

1747 Ensure that the applicant possesses:

1748 a) identification from the organization with which it is claiming affiliation;

1749 b) agreement from the organization that the applicant may be issued a credential
1750 indicating that an affiliation exists.

1751 AL4_ID_AFV#020 Evidence checks

1752 Have in place and apply processes which ensure that the presented documents:

- 1753 a) each appear to be a genuine document properly issued by the claimed issuing
1754 authorities and valid at the time of application;
1755 b) refer to an existing organization with a contact address;
1756 c) indicate that the applicant has some form of recognizable affiliation with the
1757 organization;
1758 d) appear to grant the applicant an entitlement to obtain a credential indicating an
1759 affiliation with the organization.
1760

1761 **3.6.4.2.4 Secondary Verification**

1762 In each of the above cases, the enterprise or specified service must also meet the
1763 following criteria:

1764 AL4_ID_SCV#010 Secondary checks

1765 Have in place additional measures (e.g., require additional documentary evidence, delay
1766 completion while out-of-band checks are undertaken) to deal with any anomalous
1767 circumstances that can reasonably be anticipated (e.g., a legitimate and recent change of
1768 address that has yet to be established as the address of record).
1769

1770 **3.6.4.3 Verification Records**

1771 The specific service must retain records of the identity proofing (verification) that it
1772 undertakes and provide them to qualifying parties when so required.

1773 The enterprise or specified service must:

1774 AL4_ID_VRC#010 Verification Records for Personal Applicants

1775 Log, taking account of all applicable legislative and policy obligations, a record of the
1776 facts of the verification process and the identity of the registrar, including a reference
1777 relating to the verification processes and the date and time of verification **issued by a**
1778 **trusted time-source**.

1779 **Guidance:** The facts of the verification process should include the specific record
1780 information (source, unique reference, value/content) used in establishing the applicant's
1781 identity, and will be determined by the specific processes used and documents accepted
1782 by the CSP. The CSP need not retain these records itself if it uses a third-party service

1783 which retains such records securely and to which the CSP has access when required, in
1784 which case it must retain a record of the identity of the third-party service providing the
1785 verification service or the location at which the (in-house) verification was performed.

1786 AL4_ID_VRC#020 Verification Records for Affiliated Applicants

1787 In addition to the foregoing, log, taking account of all applicable legislative and policy
1788 obligations, a record of the additional facts of the verification process must be performed.
1789 At a minimum, records of identity information must include:

- 1790 a) the subscriber's full name;
- 1791 b) the subscriber's current address of record;
- 1792 c) the subscriber's current telephone or email address of record;
- 1793 d) the subscriber's authorization for issuing the subject a credential;
- 1794 e) type, issuing authority, and reference number(s) of all documents checked in the
1795 identity proofing process;
- 1796 **f) a biometric record of each required representative of the affiliating**
1797 **organization (e.g., a photograph, fingerprint, voice recording), as determined**
1798 **by that organization's governance rules/charter.**

1799 AL4_ID_VRC#030 Record Retention

1800 Either retain, securely, the record of the verification/revocation process for the duration of
1801 the subscriber account plus **10.5** years, or submit the record to a client CSP that has
1802 undertaken to retain the record for the requisite period or longer.

1803

1804 **3.6.5 Compliance Tables**

1805 Use the following tables to correlate criteria for a particular Assurance Level (AL) and
1806 the evidence offered to support compliance.

1807 Service providers preparing for an assessment can use the table appropriate to the AL at
1808 which they are seeking approval to correlate evidence with criteria or to justify non-
1809 applicability (e.g., "specific service types not offered").

1810 Assessors can use the tables to record the steps in their assessment and their
1811 determination of compliance or failure.

1812 **Table 3-5. ID-SAC - AL1 Compliance**

Clause	Description	Compliance
AL1_ID_POL#010	Unique service identity	
AL1_ID_POL#020	Unique subject identity	
AL1_ID_IPV#010	Required evidence	
AL1_ID_IPV#020	Evidence checks	
AL1_ID_RPV#010	Required evidence	
AL1_ID_RPV#020	Evidence checks	
AL1_ID_SCV#010	Secondary checks	

1813

1814

Table 3-6. ID-SAC - AL2 Compliance

Clause	Description	Compliance
AL2_ID_POL#010	Unique service identity	
AL2_ID_POL#020	Unique subject identity	
AL2_ID_POL#030	Published Proofing Policy	
AL2_ID_POL#040	Adherence to Proofing Policy	
AL2_ID_IDV#000	Identity Proofing classes	
AL2_ID_IPV#010	Required evidence	
AL2_ID_IPV#020	Evidence checks	
AL2_ID_RPV#010	Required evidence	
AL2_ID_RPV#020	Evidence checks	
AL2_ID_CRV#010	Required evidence	
AL2_ID_CRV#020	Evidence checks	
AL2_ID_AFV#000	Meet preceding criteria	
AL2_ID_AFV#010	Required evidence	
AL2_ID_AFV#020	Evidence checks	
AL2_ID_SCV#010	Secondary checks	
AL2_ID_VRC#010	Verification Records for Personal Applicants	
AL2_ID_VRC#020	Verification Records for Affiliated Applicants	
AL2_ID_VRC#030	Record Retention	

1815

1816

Table 3-7. ID-SAC - AL3 compliance

Clause	Description	Compliance
AL3_ID_POL#010	Unique service identity	
AL3_ID_POL#020	Unique subject identity	
AL3_ID_POL#030	Published Proofing Policy	
AL3_ID_POL#040	Adherence to Proofing Policy	
AL3_ID_IDV#000	Identity Proofing classes	
AL3_ID_IPV#010	Required evidence	
AL3_ID_IPV#020	Evidence checks	
AL3_ID_RPV#010	Required evidence	
AL3_ID_RPV#020	Evidence checks	
AL3_ID_AFV#000	Meet preceding criteria	
AL3_ID_AFV#010	Required evidence	
AL3_ID_AFV#020	Evidence checks	
AL3_ID_SCV#010	Secondary checks	
AL3_ID_VRC#010	Verification Records for Personal Applicants	
AL3_ID_VRC#020	Verification Records for Affiliated Applicants	
AL3_ID_VRC#030	Record Retention	

1817

1818

Table 3-8. ID-SAC - AL4 compliance

Clause	Description	Compliance
AL4_ID_POL#010	Unique service identity	
AL4_ID_POL#020	Unique subject identity	
AL4_ID_POL#030	Published Proofing Policy	
AL4_ID_POL#040	Adherence to Proofing Policy	
AL3_ID_IDV#000	Identity Proofing classes	
AL4_ID_IPV#010	Required evidence	
AL4_ID_IPV#020	No stipulation	No conformity requirement
AL4_ID_IPV#030	Evidence checks – primary ID	
AL4_ID_IPV#040	Evidence checks – secondary ID	
AL4_ID_IPV#050	Applicant knowledge checks	
AL4_ID_AFV#000	Meet preceding criteria	
AL4_ID_AFV#010	Required evidence	
AL4_ID_AFV#020	Evidence checks	
AL4_ID_SCV#010	Secondary checks	
AL4_ID_VRC#010	Verification Records for Personal Applicants	
AL4_ID_VRC#020	Verification Records for Affiliated Applicants	
AL4_ID_VRC#030	Record Retention	

1819

1820 **3.7 Credential Management Service Assessment Criteria**

1821 The Service Assessment Criteria in this section establish requirements for the functional
1822 conformity of credential management services and their providers at all ALs defined in
1823 Section 2 and in the [Identity Assurance Framework: Levels of Assurance](#) document.

1824 These criteria are generally referred to elsewhere within IAF documentation as CM-SAC.

1825 The criteria are divided into five parts. Each part deals with a specific functional aspect
1826 of the overall credential management process.

1827 This SAC must be used in conjunction with the Common Organizational SAC
1828 (CO-SAC), described in Section 3.5, and, in addition, must either:

- 1829 • explicitly include the criteria of the Identity Proofing SAC ([ID-SAC]) described
1830 in Section 3.6, or
- 1831 • rely upon the criteria of the ID-SAC [ID-SAC] being fulfilled by the use of a
1832 Kantara-approved ID-proofing service.

1833 **3.7.1 Part A - Credential Operating Environment**

1834 The criteria in this part deal with the overall operational environment in which the
1835 credential life-cycle management is conducted. The credential management service
1836 assessment criteria must be used in conjunction with the Common Organizational criteria
1837 described in Section 3.5. In addition, they must either explicitly include the identity
1838 proofing service assessment criteria described in Section 3.6 or rely upon those criteria
1839 being fulfilled by the use of a Kantara-approved identity proofing service.

1840 These criteria describe requirements for the overall operational environment in which
1841 credential lifecycle management is conducted. The common organizational criteria
1842 describe broad requirements. The criteria in this section describe implementation
1843 specifics. Implementation depends on the AL. The procedures and processes required to
1844 create a secure environment for management of credentials and the particular
1845 technologies that are considered strong enough to meet the assurance requirements differ
1846 considerably from level to level.

1847 **3.7.1.1 Assurance Level 1**

1848 These criteria apply to PINs and passwords, as well as SAML assertions.

1849 **3.7.1.1.1 Not used**

1850 No stipulation.

1851

1852 **3.7.1.1.2 Security Controls**

1853 An enterprise and its specified service must:

- 1854 AL1_CM_CTR#010 No stipulation
- 1855 AL1_CM_CTR#020 Protocol threat risk assessment and controls
- 1856 Account for at least the following protocol threats and apply appropriate controls:
- 1857 a) password guessing, such that the resistance to an on-line guessing attack against a
1858 selected user/password is at least 1 in 2^{10} (1,024);
- 1859 b) message replay.
- 1860 AL1_CM_CTR#025 No stipulation
- 1861 AL1_CM_CTR#030 System threat risk assessment and controls
- 1862 Account for the following system threats and apply appropriate controls:
- 1863 a) the introduction of malicious code;
- 1864 b) compromised authentication arising from insider action;
- 1865 c) out-of-band attacks by other users and system operators (e.g., the ubiquitous
1866 shoulder-surfing);
- 1867 d) spoofing of system elements/applications;
- 1868 e) malfeasance on the part of subscribers and subjects.
- 1869
- 1870 **3.7.1.1.3 Storage of Long-term Secrets**
- 1871 AL1_CM_STS#010 Withdrawn
- 1872 Withdrawn (AL1_CO_SCO#020 (a) & (b) enforce this requirement)
- 1873
- 1874 **3.7.1.1.4 Not used**
- 1875 **3.7.1.1.5 Subject Options**
- 1876 AL1_CM_OPN#010 Withdrawn
- 1877 Withdrawn – see AL1_CM_RNR#010.

1878 **3.7.1.2 Assurance Level 2**

1879 These criteria apply to passwords, as well as acceptable SAML assertions.

1880 **3.7.1.2.1 Credential Policy and Practices**

1881 These criteria apply to the policy and practices under which credentials are managed.

1882 An enterprise and its specified service must:

1883 AL2_CM_CPP#010 Credential Policy and Practice Statement

1884 **Include in its Service Definition a description of the policy against which it issues**
1885 **credentials and the corresponding practices it applies in their management. At a**
1886 **minimum, the Credential Policy and Practice Statement must specify:**

- 1887 a) **if applicable, any OIDs related to the Practice and Policy Statement;**
1888 b) **how users may subscribe to the service/apply for credentials and how users'**
1889 **credentials will be delivered to them;**
1890 c) **how subscribers acknowledge receipt of tokens and credentials and what**
1891 **obligations they accept in so doing (including whether they consent to**
1892 **publication of their details in credential status directories);**
1893 d) **how credentials may be renewed, modified, revoked, and suspended,**
1894 **including how requestors are authenticated or their identity re-proven;**
1895 e) **what actions a subscriber must take to terminate a subscription;**
1896 f) **how records are retained and archived.**

1897 AL2_CM_CPP#020 No stipulation

1898 AL2_CM_CPP#030 Management Authority

1899 **Have a nominated management body with authority and responsibility for**
1900 **approving the Credential Policy and Practice Statement and for its implementation.**

1901

1902 **3.7.1.2.2 Security Controls**

1903 An enterprise and its specified service must:

1904 AL2_CM_CTR#010 Secret revelation

1905 **Withdrawn.**

1906 AL2_CM_CTR#020 Protocol threat risk assessment and controls

1907 Account for at least the following protocol threats **in its risk assessment** and apply
1908 **[omitted] controls that reduce them to acceptable risk levels:**

- 1909 a) password guessing, such that the resistance to an on-line guessing attack against a
1910 selected user/password is at least 1 in 2^{14} **(16,384)**;
1911 b) message replay, **showing that it is impractical**;
1912 c) **eavesdropping, showing that it is impractical.**

1913 AL2_CM_CTR#025 Permitted authentication protocols

1914 **Permit only the following authentication protocols:**

- 1915 a) **tunneled password**;
1916 b) **zero knowledge-base password**;
1917 c) **SAML assertions.**

1918 AL2_CM_CTR#028 One-time passwords

1919 **Use only one-time passwords which:**

- 1920 a) **are generated using an approved block-cipher or hash function to combine a**
1921 **symmetric key, stored on the device, with a nonce**;
1922 b) **derive the nonce from a date and time, or a counter generated on the device**;
1923 c) **have a limited lifetime, in the order of minutes.**
1924

1925 AL2_CM_CTR#030 System threat risk assessment and controls

1926 Account for the following system threats **in its risk assessment** and apply **[omitted]**
1927 controls **that reduce them to acceptable risk levels:**

- 1928 a) the introduction of malicious code;
1929 b) compromised authentication arising from insider action;
1930 c) out-of-band attacks by both users and system operators (e.g., the ubiquitous
1931 shoulder-surfing);
1932 d) spoofing of system elements/applications;
1933 e) malfeasance on the part of subscribers and subjects;
1934 f) **intrusions leading to information theft.**

1935 AL2_CM_CTR#040 Specified Service's Key Management

1936 **Specify and observe procedures and processes for the generation, storage, and**
1937 **destruction of its own cryptographic keys used for securing the specific service's**
1938 **assertions and other publicized information. At a minimum, these should address:**

- 1939 a) **the physical security of the environment**;
1940 b) **access control procedures limiting access to the minimum number of**
1941 **authorized personnel**;
1942 c) **public-key publication mechanisms**;
1943 d) **application of controls deemed necessary as a result of the service's risk**
1944 **assessment**;

- 1945 e) **destruction of expired or compromised private keys in a manner that**
1946 **prohibits their retrieval, or their archival in a manner that prohibits their**
1947 **reuse;**
1948 f) **applicable cryptographic module security requirements, quoting FIPS 140-2**
1949 **[FIPS140-2] or equivalent, as established by a recognized national technical**
1950 **authority.**
1951

1952 **3.7.1.2.3 Storage of Long-term Secrets**

- 1953 AL2_CM_STS#010 Withdrawn
1954 Withdrawn (AL2_CO_SCO#020 (a) & (b) enforce this requirement).
1955

1956 **3.7.1.2.4 Security-Relevant Event (Audit) Records**

1957 **3.7.1.2.5 No stipulation**

- 1958 AL2_CM_OPN#010 Withdrawn
1959 Withdrawn – see AL2_CM_RNR#010.
1960

1961 **3.7.1.3 Assurance Level 3**

1962 These criteria apply to one-time password devices and soft crypto applications protected
1963 by passwords or biometric controls, as well as cryptographically-signed SAML
1964 assertions.

1965 **3.7.1.3.1 Credential Policy and Practices**

1966 These criteria apply to the policy and practices under which credentials are managed.

1967 An enterprise and its specified service must:

1968 AL3_CM_CPP#010 Credential Policy and Practice Statement

1969 Include in its Service Definition a full description of the policy against which it issues
1970 credentials and the corresponding practices it applies in their issuance. At a minimum,
1971 the Credential Policy and Practice Statement must specify:

- 1972 a) if applicable, any OIDs related to the Credential Policy and Practice Statement;
1973 b) how users may subscribe to the service/apply for credentials and how the users'
1974 credentials will be delivered to them;
1975 c) how subscribers acknowledge receipt of tokens and credentials and what
1976 obligations they accept in so doing (including whether they consent to publication
1977 of their details in credential status directories);
1978 d) how credentials may be renewed, modified, revoked, and suspended, including
1979 how requestors are authenticated or their identity proven;
1980 e) what actions a subscriber must take to terminate a subscription;
1981 f) how records are retained and archived.

1982 AL3_CM_CPP#020 No stipulation

1983 AL3_CM_CPP#030 Management Authority

1984 Have a nominated or appointed high-level management body with authority and
1985 responsibility for approving the Certificate Policy and Certification Practice Statement,
1986 including ultimate responsibility for their proper implementation.

1987

1988 **3.7.1.3.2 Security Controls**

1989 AL3_CM_CTR#010 No stipulation

1990 AL3_CM_CTR#020 Protocol threat risk assessment and controls

1991 Account for at least the following protocol threats in its risk assessment and apply
1992 controls that reduce them to acceptable risk levels:

- 1993 a) password guessing, such that the resistance to an on-line guessing attack against a
1994 selected user/password is at least 1 in 2^{14} **(16,384)**;
1995 b) message replay, showing that it is impractical;
1996 c) eavesdropping, showing that it is impractical;
1997 **d) relying party (verifier) impersonation, showing that it is impractical;**
1998 **e) man-in-the-middle attack, showing that it is impractical.**
1999 **The above list shall not be considered to be a complete list of threats to be addressed**
2000 **by the risk assessment.**

2001 AL3_CM_CTR#025 Permitted authentication protocols

2002 For non-PKI credentials, permit only the following authentication protocols:

- 2003 a) tunneled password;
2004 b) zero knowledge-base password;
2005 c) SAML assertions.

2006 AL3_CM_CTR#030 System threat risk assessment and controls

2007 Account for the following system threats in its risk assessment and apply controls that
2008 reduce them to acceptable risk levels:

- 2009 a) the introduction of malicious code;
2010 b) compromised authentication arising from insider action;
2011 c) out-of-band attacks by both users and system operators (e.g., shoulder-surfing);
2012 d) spoofing of system elements/applications;
2013 e) malfeasance on the part of subscribers and subjects;
2014 f) intrusions leading to information theft.

2015 The above list shall not be considered to be a complete list of threats to be addressed by
2016 the risk assessment.

2017 AL3_CM_CTR#040 Specified Service's Key Management

2018 Specify and observe procedures and processes for the generation, storage, and destruction
2019 of its own cryptographic keys used for securing the specific service's assertions and other
2020 publicized information. At a minimum, these should address:

- 2021 a) the physical security of the environment;
2022 b) access control procedures limiting access to the minimum number of authorized
2023 personnel;
2024 c) public-key publication mechanisms;
2025 d) application of controls deemed necessary as a result of the service's risk
2026 assessment;
2027 e) destruction of expired or compromised private keys in a manner that prohibits
2028 their retrieval or their archival in a manner that prohibits their reuse;

- 2029 f) applicable cryptographic module security requirements, quoting FIPS 140-2
2030 [FIPS140-2] or equivalent, as established by a recognized national technical
2031 authority.
2032

2033 **3.7.1.3.3 Storage of Long-term Secrets**

2034 An enterprise and its specified service must:

2035 AL3_CM_STS#010 Withdrawn

2036 Withdrawn (AL3_CO_SCO#020 (a) & (b) enforce this requirement).

2037 AL3_CM_STS#020 Stored Secret Encryption

2038 Encrypt such shared secret files so that:

- 2039 a) the encryption key for the shared secret file is encrypted under a key held in a
2040 FIPS 140-2 [FIPS140-2] Level 2 or higher validated hardware or software
2041 cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module, or
2042 equivalent, as established by a recognized national technical authority;
2043 b) the shared secret file is decrypted only as immediately required for an
2044 authentication operation;
2045 c) shared secrets are protected as a key within the boundary of a FIPS 140-2 Level 2
2046 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or
2047 4 cryptographic module and are not exported from the module in plain text, or
2048 equivalent, as established by a recognized national technical authority;
2049 d) shared secrets are split by an "*n from m*" cryptographic secret sharing method.
2050

2051 **3.7.1.3.4 Security-relevant Event (Audit) Records**

2052 These criteria describe the need to provide an auditable log of all events that are pertinent
2053 to the correct and secure operation of the service. The common organizational criteria
2054 applying to provision of an auditable log of all security-related events pertinent to the
2055 correct and secure operation of the service must also be considered carefully. These
2056 criteria carry implications for credential management operations.

2057 In the specific context of a certificate management service, an enterprise and its specified
2058 service must:

2059 AL3_CM_SER#010 Security event logs

2060 Ensure that such audit records include:

- 2061 a) the identity of the point of registration (irrespective of whether internal or
2062 outsourced);

- 2063 b) generation of the subscriber's keys or the evidence that the subscriber was in
2064 possession of both parts of their own key-pair;
2065 c) generation of the subscriber's certificate;
2066 d) dissemination of the subscriber's certificate;
2067 e) any revocation or suspension associated with the subscriber's certificate.
2068

2069 **3.7.1.3.5 Subject options**

2070 AL3_CM_OPN#010 Changeable PIN/Password

2071 Withdrawn – see AL3_CM_RNR#010.

2072 **3.7.1.4 Assurance Level 4**

2073 These criteria apply exclusively to cryptographic technology deployed through a Public
2074 Key Infrastructure. This technology requires hardware tokens protected by password or
2075 biometric controls. No other forms of credential are permitted at AL4.

2076 **3.7.1.4.1 Certification Policy and Practices**

2077 These criteria apply to the policy and practices under which certificates are managed.

2078 An enterprise and its specified service must:

2079 AL4_CM_CPP#010 No stipulation

2080 AL4_CM_CPP#020 Certificate Policy/Certification Practice Statement

2081 **Include in its Service Definition its full Certificate Policy and the corresponding**
2082 **Certification and Practice Statement. The Certificate Policy and Certification**
2083 **Practice Statement must conform to IETF RFC 3647 (2003-11) [RFC 3647] in their**
2084 **content and scope or be demonstrably consistent with the content or scope of that**
2085 **RFC. At a minimum, the Certificate Policy must specify:**

- 2086 a) **applicable OIDs for each certificate type issued;**
2087 b) **how users may subscribe to the service/apply for certificates, and how**
2088 **certificates will be issued to them;**
2089 c) **if users present their own keys, how they will be required to demonstrate**
2090 **possession of the private key;**
2091 d) **if users' keys are generated for them, how the private keys will be delivered**
2092 **to them;**
2093 e) **how subscribers acknowledge receipt of tokens and credentials and what**
2094 **obligations they accept in so doing (including whether they consent to**
2095 **publication of their details in certificate status directories);**
2096 f) **how certificates may be renewed, re-keyed, modified, revoked, and**
2097 **suspended, including how requestors are authenticated or their identity**
2098 **proven;**
2099 g) **what actions a subscriber must take to terminate their subscription.**

2100 AL4_CM_CPP#030 Management Authority

2101 Have a nominated or appointed high-level management body with authority and
2102 responsibility for approving the Certificate Policy and Certification Practice Statement,
2103 including ultimate responsibility for their proper implementation.

2104

2105 **3.7.1.4.2 Security Controls**

2106 An enterprise and its specified service must:

- 2107 AL4_CM_CTR#010 No stipulation
- 2108 AL4_CM_CTR#020 Protocol threat risk assessment and controls
- 2109 Account for at least the following protocol threats in its risk assessment and apply
2110 controls that reduce them to acceptable risk levels:
- 2111 a) password guessing, showing that there is sufficient entropy;
2112 b) message replay, showing that it is impractical;
2113 c) eavesdropping, showing that it is impractical;
2114 d) relying party (verifier) impersonation, showing that it is impractical;
2115 e) man-in-the-middle attack, showing that it is impractical;
2116 **f) session hijacking, showing that it is impractical.**
- 2117 The above list shall not be considered to be a complete list of threats to be addressed by
2118 the risk assessment.
- 2119 AL4_CM_CTR#025 No stipulation
- 2120 AL4_CM_CTR#030 System threat risk assessment and controls
- 2121 Account for the following system threats in its risk assessment and apply controls that
2122 reduce them to acceptable risk levels:
- 2123 a) the introduction of malicious code;
2124 b) compromised authentication arising from insider action;
2125 c) out-of-band attacks by both users and system operators (e.g., shoulder-surfing);
2126 d) spoofing of system elements/applications;
2127 e) malfeasance on the part of subscribers and subjects;
2128 f) intrusions leading to information theft.
- 2129 The above list shall not be considered to be a complete list of threats to be addressed by
2130 the risk assessment.
- 2131 AL4_CM_CTR#040 Specified Service's Key Management
- 2132 Specify and observe procedures and processes for the generation, storage, and destruction
2133 of its own cryptographic keys used for securing the specific service's assertions and other
2134 publicized information. At a minimum, these should address:
- 2135 a) the physical security of the environment;
2136 b) access control procedures limiting access to the minimum number of authorized
2137 personnel;
2138 c) public-key publication mechanisms;
2139 d) application of controls deemed necessary as a result of the service's risk
2140 assessment;

- 2141 e) destruction of expired or compromised private keys in a manner that prohibits
2142 their retrieval, or their archival in a manner which prohibits their reuse;
2143 f) applicable cryptographic module security requirements, quoting FIPS 140-2
2144 [FIPS140-2] or equivalent, as established by a recognized national technical
2145 authority.
2146

2147 **3.7.1.4.3 Storage of Long-term Secrets**

2148 The enterprise and its specified service must meet the following criteria:

2149 AL4_CM_STS#010 Stored Secrets

- 2150 a) Withdrawn (AL4_CO_SCO#020 (a) & (b) enforce this requirement)
2151 b) **apply discretionary access controls that limit access to trusted administrators**
2152 **and to those applications that require access.**

2153 AL4_CM_STS#020 Stored Secret Encryption

2154 Encrypt such [omitted] secret files so that:

- 2155 a) the encryption key for the [omitted] secret file is encrypted under a key held in a
2156 FIPS 140-2 [FIPS140-2] Level 2 or higher validated hardware cryptographic
2157 module or any FIPS 140-2 Level 3 or 4 cryptographic module, or equivalent, as
2158 established by a recognized national technical authority;
2159 b) the [omitted] secret file is decrypted only as immediately required for a key
2160 recovery operation;
2161 c) [omitted] secrets are protected as a key within the boundary of a FIPS 140-2
2162 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2
2163 Level 3 or 4 cryptographic module and are not exported from the module in
2164 plaintext, or equivalent, as established by a recognized national technical
2165 authority;
2166 d) escrowed secrets are split by an "n from m" cryptographic secret **storing** method.
2167

2168 **3.7.1.4.4 Security-relevant Event (Audit) Records**

2169 These criteria describe the need to provide an auditable log of all events that are pertinent
2170 to the correct and secure operation of the service. The common organizational criteria
2171 relating to the recording of all security-related events must also be considered carefully.
2172 These criteria carry implications for credential management operations.

2173 In the specific context of a certificate management service, an enterprise and its specified
2174 service must:

- 2175 AL4_CM_SER#010 Security event logs
- 2176 Ensure that such audit records include:
- 2177 a) the identity of the point of registration (irrespective of whether internal or
2178 outsourced);
- 2179 b) generation of the subscriber's keys or evidence that the subscriber was in
2180 possession of both parts of the key-pair;
- 2181 c) generation of the subscriber's certificate;
- 2182 d) dissemination of the subscriber's certificate;
- 2183 e) any revocation or suspension associated with the subscriber's credential.
2184

2185 **3.7.1.4.5 Subject Options**

- 2186 AL4_CM_OPN#010 Changeable PIN/Password
- 2187 Withdrawn – see AL4_CM_RNR#010.

2188 **3.7.2 Part B - Credential Issuing**

2189 These criteria apply to the verification of the identity of the subject of a credential and
2190 with token strength and credential delivery mechanisms. They address requirements
2191 levied by the use of various technologies to achieve the appropriate AL⁶. These criteria
2192 include by reference all applicable criteria in Section 3.6.

2193 **3.7.2.1 Assurance Level 1**

2194 **3.7.2.1.1 Identity Proofing**

2195 These criteria determine how the enterprise shows compliance with the criteria for
2196 fulfilling identity proofing functions.

2197 The enterprise and its specified service must:

2198 AL1_CM_IDP#010 Self-managed Identity Proofing

2199 If the enterprise assumes direct responsibility for identity proofing functions, show, by
2200 direct inclusion, compliance with all applicable identity proofing service assessment
2201 criteria⁷ ([ID-SAC]) for AL1 or higher.

2202 AL1_CM_IDP#020 Kantara-Recognized outsourced service

2203 If the enterprise outsources responsibility for identity proofing functions and uses a
2204 service already Kantara-Recognized, show that the service in question has been approved
2205 at AL1 or higher.

2206 AL1_CM_IDP#030 Non-recognized outsourced service

2207 If the enterprise outsources responsibility for identity proofing functions, ensure that each
2208 provider of such a service demonstrates compliance with all applicable identity proofing
2209 service assessment criteria for AL1 or higher, and that the enterprise, itself, has in place
2210 controls to ensure the continued fulfillment of those criteria by the provider to which the
2211 functions have been outsourced.

2212 AL1_CM_IDP#040 Revision to subscriber information

2213 Provide a means for subscribers to amend their stored information after registration.

2214

⁶ Largely driven by the guidance in NIST SP 800-63 [NIST800-63].

⁷ Not all criteria may be applicable – the precise scope (definition) of the identity proofing performed by a particular service may exclude certain functionality and therefore certain criteria.

2215 **3.7.2.1.2 Credential Creation**

2216 These criteria address the requirements for creation of credentials that can only be used at
2217 AL1. Any credentials/tokens that comply with the criteria stipulated for AL2 and higher
2218 are acceptable at AL1.

2219 An enterprise and its specified service must:

2220 AL1_CM_CRN#010 Authenticated Request

2221 Only accept a request to generate a credential and bind it to an identity if the source of the
2222 request can be authenticated as being authorized to perform identity proofing at AL1 or
2223 higher.

2224 AL1_CM_CRN#020 No stipulation

2225 AL1_CM_CRN#030 Credential uniqueness

2226 Allow the subscriber to select a credential (e.g., UserID) that is verified to be unique
2227 within the specified service's community and assigned uniquely to a single identity
2228 subject.

2229 **3.7.2.1.3 Not used**

2230 **3.7.2.1.4 Not used**

2231

2232 **3.7.2.2 Assurance Level 2**

2233 **3.7.2.2.1 Identity Proofing**

2234 These criteria determine how the enterprise shows compliance with the criteria for
2235 fulfilling identity proofing functions.

2236 The enterprise and its specified service must:

2237 AL2_CM_IDP#010 Self-managed Identity Proofing

2238 If the enterprise assumes direct responsibility for identity proofing functions, show, by
2239 direct inclusion, compliance with all applicable identity proofing service assessment
2240 criteria ([ID-SAC]) for AL2 or higher.

2241 AL2_CM_IDP#020 Kantara-Recognized outsourced service

2242 If the enterprise outsources responsibility for identity proofing functions and uses a
2243 service already Kantara-Recognized, show that the service in question has been approved
2244 at AL2 or higher **and that its approval has at least six months of remaining validity.**

2245 AL2_CM_IDP#030 Non- Kantara-Recognized outsourced service

2246 If the enterprise outsources responsibility for identity proofing functions, ensure that each
2247 provider of such a service demonstrates compliance with all applicable identity proofing
2248 service assessment criteria for AL2 or higher, and that the enterprise, itself, has in place
2249 controls to ensure the continued fulfillment of those criteria by the provider to which the
2250 functions have been outsourced.

2251 AL2_CM_IDP#040 Revision to subscriber information

2252 Provide a means for subscribers to **securely** amend their stored information after
2253 registration, **either by re-proving their identity, as in the initial registration process,**
2254 **or by using their credentials to authenticate their revision.**

2255

2256 **3.7.2.2.2 Credential Creation**

2257 These criteria define the requirements for creation of credentials whose highest use is at
2258 AL2. Credentials/tokens that comply with the criteria stipulated at AL3 and higher are
2259 also acceptable at AL2 and below.

2260 Note, however, that a token and credential required by a higher AL but created according
2261 to these criteria may not necessarily provide that higher level of assurance for the claimed
2262 identity of the subscriber. Authentication can only be provided at the assurance level at
2263 which the identity is proven.

- 2264 An enterprise and its specified service must:
- 2265 AL2_CM_CRN#010 Authenticated Request
- 2266 Only accept a request to generate a credential and bind it to an identity if the source of the
2267 request can be authenticated, **i.e., Registration Authority, as being authorized to**
2268 **perform identity proofing at AL2 or higher.**
- 2269 AL2_CM_CRN#020 Unique identity
- 2270 **Ensure that the identity which relates to a specific applicant is unique within the**
2271 **specified service, including identities previously used and that are now cancelled,**
2272 **other than its re-assignment to the same applicant.**
- 2273 Guidance: This requirement is intended to prevent identities that may exist in a Relying
2274 Party's access control list from possibly representing a different physical person.
- 2275 AL2_CM_CRN#030 Credential uniqueness
- 2276 Allow the subscriber to select a credential (e.g., UserID) that is verified to be unique
2277 within the specified service's community and assigned uniquely to a single identity
2278 subject.
- 2279 AL2_CM_CRN#035 Convey credential
- 2280 **Be capable of conveying the unique identity information associated with a credential**
2281 **to Verifiers and Relying Parties.**
- 2282 AL2_CM_CRN#040 Password strength
- 2283 **Only allow passwords that, over the life of the password, have resistance to an on-**
2284 **line guessing attack against a selected user/password of at least 1 in 2^{14} (16,384),**
2285 **accounting for state-of-the-art attack strategies, and at least 10 bits of min-entropy⁸.**
- 2286 AL2_CM_CRN#050 One-time password strength
- 2287 **Only allow password tokens that have a resistance to online guessing attack against**
2288 **a selected user/password of at least 1 in 2^{14} (16,384), accounting for state-of-the-art**
2289 **attack strategies, and at least 10 bits of min-entropy⁸.**

⁸ Refer to NIST SP 800-63 "Appendix A: Estimating Entropy and Strength" or similar recognized sources of such information.

- 2290 AL2_CM_CRN#060 Software cryptographic token strength
- 2291 **Ensure that software cryptographic keys stored on general-purpose devices:**
- 2292 a) **are protected by a key and cryptographic protocol that are evaluated against**
- 2293 **FIPS 140-2 [[FIPS140-2](#)] Level 2, or equivalent, as established by a recognized**
- 2294 **national technical authority;**
- 2295 b) **require password or biometric activation by the subscriber or employ a**
- 2296 **password protocol when being used for authentication.**
- 2297 AL2_CM_CRN#070 Hardware token strength
- 2298 **Ensure that hardware tokens used to store cryptographic keys:**
- 2299 a) **employ a cryptographic module that is evaluated against FIPS 140-2**
- 2300 **[[FIPS140-2](#)] Level 1 or higher, or equivalent, as established by a recognized**
- 2301 **national technical authority;**
- 2302 b) **require password or biometric activation by the subscriber or also employ a**
- 2303 **password when being used for authentication.**
- 2304 AL2_CM_CRN#080 No stipulation
- 2305 AL2_CM_CRN#090 Nature of subject
- 2306 **Record the nature of the subject of the credential (which must correspond to the**
- 2307 **manner of identity proofing performed), i.e., physical person, a named person acting**
- 2308 **on behalf of a corporation or other legal entity, corporation or legal entity, or**
- 2309 **corporate machine entity, in a manner that can be unequivocally associated with the**
- 2310 **credential and the identity that it asserts. If the credential is based upon a**
- 2311 **pseudonym this must be indicated in the credential.**
- 2312 **3.7.2.2.3 Subject Key Pair Generation**
- 2313 No stipulation.
- 2314 **3.7.2.2.4 Credential Delivery**
- 2315 An enterprise and its specified service must:
- 2316 AL2_CM_CRD#010 Notify Subject of Credential Issuance
- 2317 **Notify the subject of the credential's issuance and, if necessary, confirm the**
- 2318 **Subject's contact information by:**
- 2319 a) **sending notice to the address of record confirmed during identity proofing**
- 2320 **or;**
- 2321 b) **issuing the credential(s) in a manner that confirms the address of record**
- 2322 **supplied by the applicant during identity proofing or;**

2323 c) **issuing the credential(s) in a manner that confirms the ability of the applicant**
2324 **to receive telephone communications at a fixed-line telephone number or**
2325 **postal address supplied by the applicant during identity proofing.**

2326 AL2_CM_CRD#015 Confirm Applicant's identity (in person)

2327 **Prior to delivering the credential, require the Applicant to identify themselves in**
2328 **person in any new electronic transaction (beyond the first transaction or encounter)**
2329 **by either:**

2330 (a) **using a secret which was established during a prior transaction or**
2331 **encounter, or sent to the Applicant's phone number, email address, or**
2332 **physical address of record, or;**

2333 (b) **through the use of a biometric that was recorded during a prior**
2334 **encounter.**

2335 AL2_CM_CRD#016 Confirm Applicant's identity (remotely)

2336 **Prior to delivering the credential, require the Applicant to identify themselves in any**
2337 **new electronic transaction (beyond the first transaction or encounter) by presenting**
2338 **a temporary secret which was established during a prior transaction or encounter,**
2339 **or sent to the Applicant's phone number, email address, or physical address of**
2340 **record.**

2341

2342 **3.7.2.3 Assurance Level 3**

2343 **3.7.2.3.1 Identity Proofing**

2344 These criteria in this section determine how the enterprise shows compliance with the
2345 criteria for fulfilling identity proofing functions.

2346 The enterprise and its specified service must:

2347 AL3_CM_IDP#010 Self-managed Identity Proofing

2348 If the enterprise assumes direct responsibility for identity proofing functions, show, by
2349 direct inclusion, compliance with all applicable identity proofing service assessment
2350 criteria for **AL3 or AL4**.

2351 AL3_CM_IDP#020 Kantara-Recognized outsourced service

2352 If the enterprise outsources responsibility for identity proofing functions and uses a
2353 service already Kantara-Recognized, show that the service in question has been certified
2354 at **AL3 or AL4** and that its approval has at least six months of remaining validity.

2355 AL3_CM_IDP#030 Non- Kantara-Recognized outsourced service

2356 **Not use any non- Kantara-Recognized services for identity proofing unless they can**
2357 **be demonstrated to have satisfied equivalently rigorous requirements established by**
2358 **another scheme recognized by IAWG.**

2359 AL3_CM_IDP#040 Revision to subscriber information

2360 Provide a means for subscribers to securely amend their stored information after
2361 registration, either by re-proving their identity as in the initial registration process or by
2362 using their credentials to authenticate their revision. **Successful revision must, where**
2363 **necessary, instigate the re-issuance of the credential.**

2364

2365 **3.7.2.3.2 Credential Creation**

2366 These criteria define the requirements for creation of credentials whose highest use is
2367 AL3. Any credentials/tokens that comply with the criteria stipulated at AL4 are also
2368 acceptable at AL3 and below.

2369 Note, however, that a token and credential type required by a higher AL but created
2370 according to these criteria may not necessarily provide that higher level of assurance for
2371 the claimed identity of the subscriber. Authentication can only be provided at the
2372 assurance level at which the identity is proven.

2373 An enterprise and its specified service must:

- 2374 AL3_CM_CRN#010 Authenticated Request
- 2375 Only accept a request to generate a credential and bind it to an identity if the source of the
2376 request, i.e., Registration Authority, can be authenticated as being authorized to perform
2377 identity proofing at AL3 or higher.
- 2378 AL3_CM_CRN#020 Unique identity
- 2379 Ensure that the identity which relates to a specific applicant is unique within the specified
2380 service, including identities previously used and that are now cancelled other than its re-
2381 assignment to the same applicant.
- 2382 **Guidance:** This requirement is intended to prevent identities that may exist in a Relying
2383 Party's access control lists from possibly representing a different physical person.
2384
- 2385 AL3_CM_CRN#030 Credential uniqueness
- 2386 Allow the subscriber to select a credential (e.g., UserID) that is verified to be unique
2387 within the specified service's community and assigned uniquely to a single identity
2388 subject.
- 2389 AL3_CM_CRN#035 Convey credential
- 2390 Be capable of conveying the unique identity information associated with a credential to
2391 Verifiers and Relying Parties.
- 2392 AL3_CM_CRN#040 PIN/Password strength
- 2393 **Not use PIN/password tokens.**
- 2394 AL3_CM_CRN#050 One-time password strength
- 2395 Only allow one-time password tokens that:
- 2396 a) **depend on a symmetric key stored on a personal hardware device evaluated**
2397 **against FIPS 140-2 [FIPS140-2] Level 1 or higher, or equivalent, as**
2398 **established by a recognized national technical authority;**
2399 b) **permit at least 10⁶ possible password values;**
2400 c) **require password or biometric activation by the subscriber.**
- 2401 AL3_CM_CRN#060 Software cryptographic token strength
- 2402 Ensure that software cryptographic keys stored on general-purpose devices:

- 2403 a) are protected by a key and cryptographic protocol that are evaluated against
2404 FIPS 14-2 [FIPS140-2] Level 2, or equivalent, as established by a recognized
2405 national technical authority;
2406 b) require password or biometric activation by the subscriber or employ a password
2407 protocol when being used for authentication.

2408 AL3_CM_CRN#070 Hardware token strength

2409 Ensure that hardware tokens used to store cryptographic keys:

- 2410 a) employ a cryptographic module that is evaluated against FIPS 140-2 [FIPS140-2]
2411 Level 1 or higher, or equivalent, as established by a recognized national technical
2412 authority;
2413 b) require password or biometric activation by the subscriber or also employ a
2414 password when being used for authentication.

2415 AL3_CM_CRN#080 Binding of key

2416 **If the specified service generates the subject's key pair, that the key generation**
2417 **process securely and uniquely binds that process to the certificate generation and**
2418 **maintains at all times the secrecy of the private key, until it is accepted by the**
2419 **subject.**

2420 AL3_CM_CRN#090 Nature of subject

2421 Record the nature of the subject of the credential (which must correspond to the manner
2422 of identity proofing performed), i.e., private person, a named person acting on behalf of a
2423 corporation or other legal entity, corporation or legal entity, or corporate machine entity,
2424 in a manner that can be unequivocally associated with the credential and the identity that
2425 it asserts. **[Omitted]**

2426

2427 **3.7.2.3.3 Subject Key Pair Generation**

2428 An enterprise and its specified service must:

2429 AL3_CM_SKP#010 Key generation by Specified Service

2430 **If the specified service generates the subject's keys:**

- 2431 a) use a FIPS 140-2 [FIPS140-2] compliant algorithm, or equivalent, as
2432 established by a recognized national technical authority, that is recognized as
2433 being fit for the purposes of the service;
2434 b) only create keys of a key length and for use with a FIPS 140-2 [FIPS140-2]
2435 compliant public key algorithm, or equivalent, as established by a recognized

- 2436 **national technical authority, recognized as being fit for the purposes of the**
2437 **service;**
2438 c) **generate and store the keys securely until delivery to and acceptance by the**
2439 **subject;**
2440 d) **deliver the subject’s private key in a manner that ensures that the privacy of**
2441 **the key is not compromised and only the subject has access to the private**
2442 **key.**

2443 AL3_CM_SKP#020 Key generation by Subject

2444 **If the subject generates and presents its own keys, obtain the subject’s written**
2445 **confirmation that it has:**

- 2446 a) **used a FIPS 140-2 [FIPS140-2] compliant algorithm, or equivalent, as**
2447 **established by a recognized national technical authority, that is recognized as**
2448 **being fit for the purposes of the service;**
2449 b) **created keys of a key length and for use with a FIPS 140-2 [FIPS140-2]**
2450 **compliant public key algorithm, or equivalent, as established by a recognized**
2451 **national technical authority, recognized as being fit for the purposes of the**
2452 **service.**
2453

2454 **3.7.2.3.4 Credential Delivery**

2455 An enterprise and its specified service must:

2456 AL3_CM_CRD#010, Notify Subject of Credential Issuance

2457 Notify the subject of the credential’s issuance and, if necessary, confirm Subject’s contact
2458 information by:

- 2459 a) sending notice to the address of record confirmed during identity proofing, **and**
2460 **either:**
2461 i) **issuing the credential(s) in a manner that confirms the address of**
2462 **record supplied by the applicant during identity proofing, or;**
2463 ii) **issuing the credential(s) in a manner that confirms the ability of the**
2464 **applicant to receive telephone communications at a phone number**
2465 **supplied by the applicant during identity proofing, while recording**
2466 **the applicant’s voice.**

2467 AL3_CM_CRD#020 Subject’s acknowledgement

2468 **Receive acknowledgement of receipt of the credential before it is activated and its**
2469 **directory status record is published (and thereby the subscription becomes active or**
2470 **re-activated, depending upon the circumstances of issue).**

2471

2472 **3.7.2.4 Assurance Level 4**

2473 **3.7.2.4.1 Identity Proofing**

2474 These criteria determine how the enterprise shows compliance with the criteria for
2475 fulfilling identity proofing functions.

2476 An enterprise and its specified service must:

2477 AL4_CM_IDP#010 Self-managed Identity Proofing

2478 If the enterprise assumes direct responsibility for identity proofing functions, show, by
2479 direct inclusion, compliance with all applicable identity proofing service assessment
2480 criteria for **[omitted]** AL4.

2481 AL4_CM_IDP#020 Kantara-Recognized outsourced service

2482 If the enterprise outsources responsibility for identity proofing functions and uses a
2483 service already Kantara-Recognized, show that the service in question has been certified
2484 at **[omitted]** AL4 and that its approval has at least **12** months of remaining validity.

2485 AL4_CM_IDP#030 Non- Kantara-Recognized outsourced service

2486 Not use any non- Kantara-Recognized outsourced services for identity proofing unless
2487 they can be demonstrated to have satisfied equivalently rigorous requirements established
2488 by another scheme recognized by IAWG.

2489 AL4_CM_IDP#040 Revision to subscriber information

2490 Provide a means for subscribers to securely amend their stored information after
2491 registration, either by re-proving their identity as in the initial registration process or by
2492 using their credentials to authenticate their revision. Successful revision must, where
2493 necessary, instigate the re-issuance of the credential.

2494

2495 **3.7.2.4.2 Credential Creation**

2496 These criteria define the requirements for creation of credentials whose highest use is
2497 AL4.

2498 Note, however, that a token and credential created according to these criteria may not
2499 necessarily provide that level of assurance for the claimed identity of the subscriber.
2500 Authentication can only be provided at the assurance level at which the identity is proven.

2501 An enterprise and its specified service must:

-
- 2502 AL4_CM_CRN#010 Authenticated Request
- 2503 Only accept a request to generate a credential and bind it to an identity if the source of the
2504 request, i.e., Registration Authority, can be authenticated as being authorized to perform
2505 identity proofing at AL4.
- 2506 AL4_CM_CRN#020 Unique identity
- 2507 Ensure that the identity which relates to a specific applicant is unique within the specified
2508 service, including identities previously used and that are now cancelled, other than its re-
2509 assignment to the same applicant.
- 2510 **Guidance:** This requirement is intended to prevent identities that may exist in a Relying
2511 Party's access control lists from possibly representing a different physical person.
- 2512 AL4_CM_CRN#030 Credential uniqueness
- 2513 Allow the subscriber to select a credential (e.g., UserID) that is verified to be unique
2514 within the specified service's community and assigned uniquely to a single identity
2515 subject.
- 2516 AL4_CM_CRN#035 Convey credential
- 2517 Be capable of conveying the unique identity information associated with a credential to
2518 Verifiers and Relying Parties.
- 2519 AL4_CM_CRN#040 PIN/Password strength
- 2520 *Not* use PIN/password tokens.
- 2521 AL4_CM_CRN#050 One-time password strength
- 2522 ***Not* use one-time password tokens.**
- 2523 AL4_CM_CRN#060 Software cryptographic token strength
- 2524 ***Not* use software cryptographic tokens.**
- 2525 AL4_CM_CRN#070 Hardware token strength
- 2526 Ensure that hardware tokens used to store cryptographic keys:
- 2527 a) employ a cryptographic module that is validated against FIPS 140-2 [FIPS140-2]
2528 Level 2 or higher, or equivalent, as determined by a recognized national technical
2529 authority;

- 2530 b) are evaluated against FIPS 140-2 Level 3 or higher, or equivalent, as
2531 determined by a recognized national technical authority, for their physical
2532 security;
2533 c) require password or biometric activation by the subscriber [omitted].

2534 AL4_CM_CRN#080 Binding of key

2535 If the specified service generates the subject's key pair, that the key generation process
2536 securely and uniquely binds that process to the certificate generation and maintains at all
2537 times the secrecy of the private key, until it is accepted by the subject.

2538 AL4_CM_CRN#090 Nature of subject

2539 Record the nature of the subject of the credential [omitted], i.e., private person, a named
2540 person acting on behalf of a corporation or other legal entity, corporation or legal entity,
2541 or corporate machine entity, in a manner that can be unequivocally associated with the
2542 credential and the identity that it asserts.

2543

2544 3.7.2.4.3 Subject Key Pair Generation

2545 An enterprise and its specified service must:

2546 AL4_CM_SKP#010 Key generation by Specified Service

2547 If the specified service generates the subject's keys:

- 2548 a) use a FIPS 140-2 [FIPS140-2] compliant algorithm, or equivalent, as established
2549 by a recognized national technical authority, that is recognized as being fit for the
2550 purposes of the service;
2551 b) only create keys of a key length and for use with a FIPS 140-2 [FIPS140-2]
2552 compliant public key algorithm, or equivalent, as established by a recognized
2553 national technical authority, recognized as being fit for the purposes of the
2554 service;
2555 c) generate and store the keys securely until delivery to and acceptance by the
2556 subject;
2557 d) deliver the subject's private key in a manner that ensures that the privacy of the
2558 key is not compromised and only the subject has access to the private key.

2559 AL4_CM_SKP#020 Key generation by Subject

2560 If the subject generates and presents its own keys, obtain the subject's written
2561 confirmation that it has:

- 2562 a) used a FIPS 140-2 [FIPS140-2] compliant algorithm, or equivalent, as established
2563 by a recognized national technical authority, that is recognized as being fit for the
2564 purposes of the service;
2565 b) created keys of a key length and for use with a FIPS 140-2 [FIPS140-2] compliant
2566 public key algorithm, or equivalent, as established by a recognized national
2567 technical authority, recognized as being fit for the purposes of the service.
2568

2569 **3.7.2.4.4 Credential Delivery**

2570 An enterprise and its specified service must:

2571 AL4_CM_CRD#010 Notify Subject of Credential Issuance

2572 Notify the subject of the credential's issuance and, if necessary, confirm Subject's contact
2573 information by:

- 2574 a) sending notice to the address of record confirmed during identity proofing;
2575 b) **unless the subject presented with a private key, issuing the hardware token**
2576 **to the subject in a manner that confirms the address of record supplied by**
2577 **the applicant during identity proofing;**
2578 c) **issuing the certificate to the subject over a separate channel in a manner that**
2579 **confirms either the address of record or the email address supplied by the**
2580 **applicant during identity proofing.**

2581 AL4_CM_CRD#020 Subject's acknowledgement

2582 Receive acknowledgement of receipt of the **hardware token** before it is activated and **the**
2583 **corresponding certificate and** its directory status record are published (and thereby the
2584 subscription becomes active or re-activated, depending upon the circumstances of issue).

2585 **3.7.3 Part C - Credential Renewal and Re-issuing**

2586 These criteria apply to the renewal and re-issuing of credentials. They address
2587 requirements levied by the use of various technologies to achieve the appropriate AL⁹.
2588 These criteria include by reference all applicable criteria in Section 3.6 and the renewal
2589 and re-issuing processes shall comply in all practical senses with the applicable criteria
2590 set forth in Part B of this section.

2591

2592 **3.7.3.1 Assurance Level 1**

2593 **3.7.3.1.1 Renewal/Re-issuance Procedures**

2594 These criteria address general renewal and re-issuance functions, to be exercised as
2595 specific controls in these circumstances while continuing to observe the general
2596 requirements established for initial credential issuance.

2597 An enterprise and its specified service must:

2598 AL1_CM_RNR#010 Changeable PIN/Password

2599 Permit subjects to change their PINs/passwords.

2600

⁹ Largely driven by the guidance in NIST SP 800-63 [NIST800-63].

2601 **3.7.3.2 Assurance Level 2**

2602 **3.7.3.2.1 Renewal/Re-issuance Procedures**

2603 These criteria address general renewal and re-issuance functions, to be exercised as
2604 specific controls in these circumstances while continuing to observe the general
2605 requirements established for initial credential issuance.

2606 An enterprise and its specified service must:

2607 AL2_CM_RNR#010 Changeable PIN/Password

2608 Permit subjects to change their [omitted] passwords, **but employ reasonable practices**
2609 **with respect to password resets and repeated password failures.**

2610 AL2_CM_RNR#020 Proof-of-possession on Renewal/Re-issuance

2611 **Subjects wishing to change their passwords must demonstrate that they are in**
2612 **possession of the unexpired current token prior to the CSP proceeding to renew or**
2613 **re-issue it.**

2614 AL2_CM_RNR#030 Renewal/Re-issuance limitations

2615 **a. not renew but may re-issue Passwords;**

2616 **b. neither renew nor re-issue expired tokens;**

2617 **c. conduct all renewal / re-issuance interactions with the Subject over a**
2618 **protected channel such as SSL/TLS.**

2619 **Guidance:** Renewal is considered as an extension of usability, whereas re-issuance
2620 requires a change.

2621

2622 **3.7.3.3 Assurance Level 3**

2623 **3.7.3.3.1 Renewal/Re-issuance Procedures**

2624 These criteria address general renewal and re-issuance functions, to be exercised as
2625 specific controls in these circumstances while continuing to observe the general
2626 requirements established for initial credential issuance.

2627 An enterprise and its specified service must:

2628 AL3_CM_RNR#010 Changeable PIN/Password

2629 Permit subjects to change **the passwords used to activate their credentials.**

2630

2631 *Further criteria may be determined after AL3 comparability assessment against Federal*
2632 *CAF and NIST SP 800-63.*

2633

2634 **3.7.3.4 Assurance Level 4**

2635 **3.7.3.4.1 Renewal/Re-issuance Procedures**

2636 These criteria address general renewal and re-issuance functions, to be exercised as
2637 specific controls in these circumstances while continuing to observe the general
2638 requirements established for initial credential issuance.

2639 An enterprise and its specified service must:

2640 AL4_CM_RNR#010 Changeable PIN/Password

2641 Permit subjects to change the passwords used to activate their credentials.

2642

2643 *Further criteria may be determined after AL4 comparability assessment against Federal*
2644 *CAF and NIST SP 800-63.*

2645

2646 **3.7.4 Part D - Credential Revocation**

2647 These criteria deal with credential revocation and the determination of the legitimacy of a
2648 revocation request.

2649 **3.7.4.1 Assurance Level 1**

2650 An enterprise and its specified service must:

2651 **3.7.4.1.1 Not used**

2652 **3.7.4.1.2 Not used**

2653 **3.7.4.1.3 Secure Revocation Request**

2654 This criterion applies when revocation requests between remote components of a service
2655 are made over a secured communication.

2656 An enterprise and its specified service must:

2657 AL1_CM_SRR#010 Submit Request

2658 Submit a request for revocation to the Credential Issuer service (function), using a
2659 secured network communication, if necessary.

2660

2661 **3.7.4.2 Assurance Level 2**

2662 **3.7.4.2.1 Revocation Procedures**

2663 These criteria address general revocation functions, such as the processes involved and
2664 the basic requirements for publication.

2665 An enterprise and its specified service must:

2666 AL2_CM_RVP#010 Revocation procedures

2667 a) **State the conditions under which revocation of an issued credential may**
2668 **occur;**

2669 b) **State the processes by which a revocation request may be submitted;**

2670 c) **State the persons and organizations from which a revocation request will be**
2671 **accepted;**

2672 d) **State the validation steps that will be applied to ensure the validity (identity)**
2673 **of the Revocant, and;**

2674 e) **State the response time between a revocation request being accepted and the**
2675 **publication of revised certificate status.**

2676 AL2_CM_RVP#020 Secure status notification

2677 **Ensure that published credential status notification information can be relied upon**
2678 **in terms of the enterprise of its origin (i.e., its authenticity) and its correctness (i.e.,**
2679 **its integrity).**

2680 AL2_CM_RVP#030 Revocation publication

2681 **Unless the credential will expire automatically within 72 hours:**

2682 **Ensure that published credential status notification is revised within 72 hours of the**
2683 **receipt of a valid revocation request, such that any subsequent attempts to use that**
2684 **credential in an authentication shall be unsuccessful.**

2685 AL2_CM_RVP#040 Verify revocation identity

2686 **Establish that the identity for which a revocation request is received is one that was**
2687 **issued by the specified service.**

2688 AL2_CM_RVP#050 Revocation Records

2689 **Retain a record of any revocation of a credential that is related to a specific identity**
2690 **previously verified, solely in connection to the stated credential. At a minimum,**
2691 **records of revocation must include:**

- 2692 a) **the Revocant's full name;**
2693 b) **the Revocant's authority to revoke (e.g., subscriber themselves, someone**
2694 **acting with the subscriber's power of attorney, the credential issuer, law**
2695 **enforcement, or other legal due process);**
2696 c) **the Credential Issuer's identity (if not directly responsible for the identity**
2697 **proofing service);**
2698 d) **the identity associated with the credential (whether the subscriber's name or**
2699 **a pseudonym);**
2700 e) **the reason for revocation.**

2701 AL2_CM_RVP#060 Record Retention

2702 **Retain, securely, the record of the revocation process for the duration of the**
2703 **subscriber's account plus 7.5 years.**

2704

2705 **3.7.4.2.2 Verify Revocant's Identity**

2706 Revocation of a credential requires that the requestor and the nature of the request be
2707 verified as rigorously as the original identity proofing. The enterprise should not act on a
2708 request for revocation without first establishing the validity of the request (if it does not,
2709 itself, determine the need for revocation).

2710 In order to do so, the enterprise and its specified service must:

2711 AL2_CM_RVR#010 Verify revocation identity

2712 **Establish that the credential for which a revocation request is received was one that**
2713 **was issued by the specified service, applying the same process and criteria as would**
2714 **be applied to an original identity proofing.**

2715 AL2_CM_RVR#020 Revocation reason

2716 **Establish the reason for the revocation request as being sound and well founded, in**
2717 **combination with verification of the Revocant, according to AL2_ID_RVR#030,**
2718 **AL2_ID_RVR#040, or AL2_ID_RVR#050.**

2719 AL2_CM_RVR#030 Verify Subscriber as Revocant

2720 **When the subscriber seeks revocation of the subscriber's own credential, the**
2721 **enterprise must:**

- 2722 a) **if in person, require presentation of a primary Government Picture ID**
2723 **document that shall be electronically verified by a record check against the**
2724 **provided identity with the specified issuing authority's records;**
2725 b) **if remote:**
2726 i. **electronically verify a signature against records (if available),**
2727 **confirmed with a call to a telephone number of record, or;**
2728 ii. **authenticate an electronic request as being from the same subscriber,**
2729 **supported by a credential at Assurance Level 2 or higher.**

2730 AL2_CM_RVR#040 CSP as Revocant

2731 **Where a CSP seeks revocation of a subscriber's credential, the enterprise must**
2732 **establish that the request is either:**

- 2733 a) **from the specified service itself, with authorization as determined by**
2734 **established procedures, or;**
2735 b) **from the client Credential Issuer, by authentication of a formalized request**
2736 **over the established secure communications network.**

2737 AL2_CM_RVR#050 Verify Legal Representative as Revocant

2738 **Where the request for revocation is made by a law enforcement officer or**
2739 **presentation of a legal document, the enterprise must:**

- 2740 a) **if in-person, verify the identity of the person presenting the request;**
2741 b) **if remote:**
2742 i. **in paper/facsimile form, verify the origin of the legal document by a**
2743 **database check or by telephone with the issuing authority, or;**
2744 ii. **as an electronic request, authenticate it as being from a recognized**
2745 **legal office, supported by a credential at Assurance Level 2 or higher.**
2746

2747 **3.7.4.2.3 Secure Revocation Request**

2748 This criterion applies when revocation requests must be communicated between remote
2749 components of the service organization.

2750 An enterprise and its specified service must:

2751 AL2_CM_SRR#010 Submit Request

2752 Submit a request for the revocation to the Credential Issuer service (function), using a
2753 secured network communication.

2754 **3.7.4.3 Assurance Level 3**

2755 **3.7.4.3.1 Revocation Procedures**

2756 These criteria address general revocation functions, such as the processes involved and
2757 the basic requirements for publication.

2758 An enterprise and its specified service must:

2759 AL3_CM_RVP#010 Revocation procedures

2760 a) State the conditions under which revocation of an issued credential may occur;

2761 b) State the processes by which a revocation request may be submitted;

2762 c) State the persons and organizations from which a revocation request will be
2763 accepted;

2764 d) State the validation steps that will be applied to ensure the validity (identity) of
2765 the Revocant, and;

2766 e) State the response time between a revocation request being accepted and the
2767 publication of revised certificate status.

2768 AL3_CM_RVP#020 Secure status notification

2769 Ensure that published credential status notification information can be relied upon in
2770 terms of the enterprise being its origin (i.e., its authenticity) and its correctness (i.e., its
2771 integrity).

2772 AL3_CM_RVP#030 Revocation publication

2773 **[Omitted]** Ensure that published credential status notification is revised within **24** hours
2774 of the receipt of a valid revocation request, such that any subsequent attempts to use that
2775 credential in an authentication shall be unsuccessful. **The nature of the revocation**
2776 **mechanism shall be in accord with the technologies supported by the service.**

2777 AL3_CM_RVP_#040 Verify Revocation Identity

2778 Establish that the identity for which a revocation request is received is one that was
2779 issued by the specified service.

2780 AL3_CM_RVP#050 Revocation Records

2781 Retain a record of any revocation of a credential that is related to a specific identity
2782 previously verified, solely in connection to the stated credential. At a minimum, records
2783 of revocation must include:

- 2784 a) the Revocant's full name;
2785 b) the Revocant's authority to revoke (e.g., subscriber themselves, someone acting
2786 with the subscriber's power of attorney, the credential issuer, law enforcement, or
2787 other legal due process);
2788 c) the Credential Issuer's identity (if not directly responsible for the identity
2789 proofing service);
2790 d) the identity associated with the credential (whether the subscriber's name or a
2791 pseudonym);
2792 e) the reason for revocation.

2793 AL3_CM_RVP#060 Record Retention

2794 Retain, securely, the record of the revocation process for a period which is in compliance
2795 with:

- 2796 a) the records retention policy required by AL2_CM_CPP#010, and;
2797 b) applicable legislation;

2798 and which, in addition, must be not less than the duration of the subscriber's account plus
2799 7.5 years.

2800

2801 **3.7.4.3.2 Verify Revocant's Identity**

2802 Revocation of a credential requires that the requestor and the nature of the request be
2803 verified as rigorously as the original identity proofing. The enterprise should not act on a
2804 request for revocation without first establishing the validity of the request (if it does not,
2805 itself, determine the need for revocation).

2806 In order to do so, the enterprise and its specified service must:

2807 AL3_CM_RVR#010 Verify revocation identity

2808 Establish that the credential for which a revocation request is received is one that was
2809 initially issued by the specified service, applying the same process and criteria as would
2810 be applied to an original identity proofing.

2811 AL3_CM_RVR#020 Revocation reason

2812 Establish the reason for the revocation request as being sound and well founded, in
2813 combination with verification of the Revocant, according to AL3_ID_RVR#030,
2814 AL3_ID_RVR#040, or AL3_ID_RVR#050.

2815 AL3_CM_RVR#030 Verify Subscriber as Revocant

2816 When the subscriber seeks revocation of the subscriber's own credential:

- 2817 a) if in-person, require presentation of a primary Government Picture ID document
2818 that shall be electronically verified by a record check against the provided identity
2819 with the specified issuing authority's records;
2820 b) if remote:
2821 i. electronically verify a signature against records (if available), confirmed
2822 with a call to a telephone number of record, or;
2823 ii. as an electronic request, authenticate it as being from the same subscriber,
2824 supported by a credential at Assurance Level 3 or higher.

2825 AL3_CM_RVR#040 Verify CSP as Revocant

2826 Where a CSP seeks revocation of a subscriber's credential, establish that the request is
2827 either:

- 2828 a) from the specified service itself, with authorization as determined by established
2829 procedures, or;
2830 b) from the client Credential Issuer, by authentication of a formalized request over
2831 the established secure communications network.

2832 AL3_CM_RVR#050 Verify Legal Representative as Revocant

2833 Where the request for revocation is made by a law enforcement officer or presentation of
2834 a legal document:

- 2835 a) if in person, verify the identity of the person presenting the request, or;
2836 b) if remote:
2837 i. in paper/facsimile form, verify the origin of the legal document by a
2838 database check or by telephone with the issuing authority, or;
2839 ii. as an electronic request, authenticate it as being from a recognized legal
2840 office, supported by a credential at Assurance Level 3 or higher.
2841

2842 **3.7.4.3.3 Secure Revocation Request**

2843 This criterion applies when revocation requests must be communicated between remote
2844 components of the service organization.

2845 An enterprise and its specified service must:

2846 AL3_CM_SRR#010 Submit Request

2847 Submit a request for the revocation to the Credential Issuer service (function), using a
2848 secured network communication.

2849 **3.7.4.4 Assurance Level 4**

2850 **3.7.4.4.1 Revocation Procedures**

2851 These criteria address general revocation functions, such as the processes involved and
2852 the basic requirements for publication.

2853 An enterprise and its specified service must:

2854 AL4_CM_RVP#010 Revocation procedures

2855 a) State the conditions under which revocation of an issued certificate may occur;

2856 b) State the processes by which a revocation request may be submitted;

2857 c) State the persons and organizations from which a revocation request will be
2858 accepted;

2859 d) State the validation steps that will be applied to ensure the validity (identity) of
2860 the Revocant, and;

2861 e) State the response time between a revocation request being accepted and the
2862 publication of revised certificate status.

2863 AL4_CM_RVP#020 Secure status notification

2864 Ensure that published credential status notification information can be relied upon in
2865 terms of the enterprise of its origin (i.e., its authenticity) and its correctness (i.e., its
2866 integrity).

2867 AL4_CM_RVP#030 Revocation publication

2868 Ensure that published credential status notification is revised within **18** hours of the
2869 receipt of a valid revocation request, such that any subsequent attempts to use that
2870 credential in an authentication shall be unsuccessful. The nature of the revocation
2871 mechanism shall be in accordance with the technologies supported by the service.

2872 AL4_CM_RVP#040 No stipulation

2873 AL4_CM_RVP#050 Revocation Records

2874 Retain a record of any revocation of a credential that is related to a specific identity
2875 previously verified, solely in connection to the stated credential. At a minimum, records
2876 of revocation must include:

2877 a) the Revocant's full name;

- 2878 b) the Revocant's authority to revoke (e.g., subscriber themselves, someone acting
2879 with the subscriber's power of attorney, the credential issuer, law enforcement, or
2880 other legal due process);
2881 c) the Credential Issuer's identity (if not directly responsible for the identity
2882 proofing service);
2883 d) the identity associated with the credential (whether the subscriber's name or a
2884 pseudonym);
2885 e) the reason for revocation.

2886 AL4_CM_RVP#060 Record Retention

2887 Retain, securely, the record of the revocation process for a period which is in compliance
2888 with:

2889 c) the records retention policy required by AL2_CM_CPP#010, and;

2890 d) applicable legislation;

2891 and which, in addition, must be not less than the duration of the subscriber's account plus
2892 7.5 years.

2893

2894 **3.7.4.4.2 Verify Revocant's Identity**

2895 Revocation of a credential requires that the requestor and the nature of the request be
2896 verified as rigorously as the original identity proofing. The enterprise should not act on a
2897 request for revocation without first establishing the validity of the request (if it does not,
2898 itself, determine the need for revocation).

2899 In order to do so, the enterprise and its specified service must:

2900 AL4_CM_RVR#010 Verify revocation identity

2901 Establish that the credential for which a revocation request is received is one that was
2902 initially issued by the specified service, applying the same process and criteria as would
2903 apply to an original identity proofing.

2904 AL4_CM_RVR#020 Revocation reason

2905 Establish the reason for the revocation request as being sound and well founded, in
2906 combination with verification of the Revocant, according to AL4_CM_RVR#030,
2907 AL4_CM_RVR#040, or AL4_CM_RVR#050.

2908 AL4_CM_RVR#030 Verify Subscriber as Revocant

2909 Where the subscriber seeks revocation of the subscriber's own credential:

- 2910 a) if in person, require presentation of a primary Government Picture ID document
2911 that shall be **[Omitted]** verified by a record check against the provided identity
2912 with the specified issuing authority's records;
2913 b) if remote:
2914 i. verify a signature against records (if available), confirmed with a call to a
2915 telephone number of record, or;
2916 ii. as an electronic request, authenticate it as being from the same subscriber,
2917 supported by a **different** credential at **Assurance Level 4**.

2918 AL4_CM_RVR#040 Verify CSP as Revocant

2919 Where a CSP seeks revocation of a subscriber's credential, establish that the request is
2920 either:

- 2921 a) from the specified service itself, with authorization as determined by established
2922 procedures, or;
2923 b) from the client Credential Issuer, by authentication of a formalized request over
2924 the established secure communications network.

2925 AL4_CM_RVR#050 Verify Legal Representative as Revocant

2926 Where the request for revocation is made by a law enforcement officer or presentation of
2927 a legal document:

- 2928 a) if in-person, verify the identity of the person presenting the request, or;
2929 b) if remote:
2930 i. in paper/facsimile form, verify the origin of the legal document by a
2931 database check or by telephone with the issuing authority;
2932 ii. as an electronic request, authenticate it as being from a recognized legal
2933 office, supported by a different credential at **Assurance Level 4**.

2934 **3.7.4.4.3 Re-keying a credential**

2935 Re-keying of a credential requires that the requestor be verified as the subject with as
2936 much rigor as was applied to the original identity proofing. The enterprise should not act
2937 on a request for re-key without first establishing that the requestor is identical to the
2938 subject.

2939 In order to do so, the enterprise and its specified service must:

2940 AL4_CM_RKY#010 Verify Requestor as Subscriber

2941 **Where the subscriber seeks a re-key for the subscriber's own credential:**

- 2942 a) **if in-person, require presentation of a primary Government Picture ID**
2943 **document that shall be verified by a record check against the provided**
2944 **identity with the specified issuing authority's records;**
2945 b) **if remote:**

2960 **3.7.5 Part E - Credential Status Management**

2961 These criteria deal with credential status management, such as the receipt of requests for
2962 new status information arising from a new credential being issued or a revocation or other
2963 change to the credential that requires notification. They also deal with the provision of
2964 status information to requesting parties (Verifiers, Relying Parties, courts and others
2965 having regulatory authority, etc.) having the right to access such information.

2966 **3.7.5.1 Assurance Level 1**

2967 **3.7.5.1.1 Status Maintenance**

2968 An enterprise and its specified service must:

2969 AL1_CM_CSM#010 Maintain Status Record

2970 Maintain a record of the status of all credentials issued.

2971 AL1_CM_CSM#020 No stipulation

2972 AL1_CM_CSM#030 No stipulation

2973 AL1_CM_CSM#040 Status Information Availability

2974 Provide, with 95% availability, a secure automated mechanism to allow relying parties to
2975 determine credential status and authenticate the subject's identity.

2976

2977 **3.7.5.2 Assurance Level 2**

2978 **3.7.5.2.1 Status Maintenance**

2979 An enterprise and its specified service must:

2980 AL2_CM_CSM#010 Maintain Status Record

2981 Maintain a record of the status of all credentials issued.

2982 AL2_CM_CSM#020 Validation of Status Change Requests

2983 **Authenticate all requestors seeking to have a change of status recorded and**
2984 **published and validate the requested change before considering processing the**
2985 **request. Such validation should include:**

2986 a) **the requesting source as one from which the specified service expects to**
2987 **receive such requests;**

2988 b) **if the request is not for a new status, the credential or identity as being one**
2989 **for which a status is already held.**

2990 AL2_CM_CSM#030 Revision to Published Status

2991 **Process authenticated requests for revised status information and have the revised**
2992 **information available for access within a period of 72 hours.**

2993 AL2_CM_CSM#040 Status Information Availability

2994 Provide, with 95% availability, a secure automated mechanism to allow relying parties to
2995 determine credential status and authenticate the subject's identity.

2996 AL2_CM_CSM#050 Inactive Credentials

2997 **Disable any credential that has not been successfully used for authentication during**
2998 **a period of 18 months.**

2999

3000 **3.7.5.3 Assurance Level 3**

3001 **3.7.5.3.1 Status Maintenance**

3002 An enterprise and its specified service must:

3003 AL3_CM_CSM#010 Maintain Status Record

3004 Maintain a record of the status of all credentials issued.

3005 AL3_CM_CSM#020 Validation of Status Change Requests

3006 Authenticate all requestors seeking to have a change of status recorded and published and
3007 validate the requested change before considering processing the request. Such validation
3008 should include:

- 3009 a) the requesting source as one from which the specified service expects to receive
3010 such requests;
3011 b) if the request is not for a new status, the credential or identity as being one for
3012 which a status is already held.

3013 AL3_CM_CSM#030 Revision to Published Status

3014 Process authenticated requests for revised status information and have the revised
3015 information available for access within a period of 72 hours.

3016 AL3_CM_CSM#040 Status Information Availability

3017 Provide, with **99%** availability, a secure automated mechanism to allow relying parties to
3018 determine credential status and authenticate the subject's identity.

3019 AL3_CM_CSM#050 Inactive Credentials

3020 Disable any credential that has not been successfully used for authentication during a
3021 period of 18 months.

3022

3023 **3.7.5.4 Assurance Level 4**

3024 **3.7.5.4.1 Status Maintenance**

3025 An enterprise and its specified service must:

3026 AL4_CM_CSM#010 Maintain Status Record

3027 Maintain a record of the status of all credentials issued.

3028 AL4_CM_CSM#020 Validation of Status Change Requests

3029 Authenticate all requestors seeking to have a change of status recorded and published and
3030 validate the requested change before considering processing the request. Such validation
3031 should include:

- 3032 a) the requesting source as one from which the specified service expects to receive
3033 such requests;
3034 b) if the request is not for a new status, the credential or identity as being one for
3035 which a status is already held.

3036 AL4_CM_CSM#030 Revision to Published Status

3037 Process authenticated requests for revised status information and have the revised
3038 information available for access within a period of 72 hours.

3039 AL4_CM_CSM#040 Status Information Availability

3040 Provide, with 99% availability, a secure automated mechanism to allow relying parties to
3041 determine credential status and authenticate the subject's identity.

3042 AL4_CM_CSM#050 Inactive Credentials

3043 Disable any credential that has not been successfully used for authentication during a
3044 period of 18 months.

3045 **3.7.6 Part F - Credential Validation/Authentication**

3046 These criteria apply to credential validation and identity authentication.

3047 **3.7.6.1 Assurance Level 1**

3048 **3.7.6.1.1 Assertion Security**

3049 An enterprise and its specified service must:

3050 AL1_CM_ASS#010 Validation and Assertion Security

3051 Provide validation of credentials to a Relying Party using a protocol that:

- 3052 a) requires authentication of the specified service or of the validation source;
- 3053 b) ensures the integrity of the authentication assertion;
- 3054 c) protects assertions against manufacture, modification and substitution, and
- 3055 secondary authenticators from manufacture;

3056 and which, specifically:

- 3057 d) creates assertions which are specific to a single transaction;
- 3058 e) where assertion references are used, generates a new reference whenever a new
- 3059 assertion is created;
- 3060 f) when an assertion is provided indirectly, either signs the assertion or sends it via a
- 3061 protected channel, using a strong binding mechanism between the secondary
- 3062 authenticator and the referenced assertion;
- 3063 g) requires the secondary authenticator to:
 - 3064 i) be signed when provided directly to Relying Party, or;
 - 3065 ii) have a minimum of 64 bits of entropy when provision is indirect (i.e.
 - 3066 through the credential user).

3067 AL1_CM_ASS#015 No stipulation

3068 AL1_CM_ASS#020 No Post Authentication

3069 *Not* authenticate credentials that have been revoked.

3070 AL1_CM_ASS#030 Proof of Possession

3071 Use an authentication protocol that requires the claimant to prove possession and control
3072 of the authentication token.

3073 AL1_CM_ASS#040 Assertion Lifetime

3074 Generate assertions so as to indicate and effect their expiration within:

- 3075 a) 12 hours after their creation, where the service shares a common internet domain
3076 with the Relying Party;
- 3077 b) five minutes after their creation, where the service does not share a common
3078 internet domain with the Relying Party.
- 3079

3080 **3.7.6.2 Assurance Level 2**

3081 **3.7.6.2.1 Assertion Security**

3082 An enterprise and its specified service must:

3083 AL2_CM_ASS#010 Validation and Assertion Security

3084 Provide validation of credentials to a Relying Party using a protocol that:

- 3085 a) requires authentication of the specified service, itself, or of the validation source;
- 3086 b) ensures the integrity of the authentication assertion;
- 3087 c) protects assertions against manufacture, modification, **substitution and**
- 3088 **disclosure**, and secondary authenticators from manufacture, **capture and replay**;
- 3089 **d) uses approved cryptography techniques;**

3090 and which, specifically:

- 3091 e) creates assertions which are specific to a single transaction;
- 3092 f) where assertion references are used, generates a new reference whenever a new
- 3093 assertion is created;
- 3094 g) when an assertion is provided indirectly, either signs the assertion or sends it via a
- 3095 protected channel, using a strong binding mechanism between the secondary
- 3096 authenticator and the referenced assertion;
- 3097 **h) send assertions either via a channel mutually-authenticated with the Relying**
- 3098 **Party, or signed and encrypted for the Relying Party;**
- 3099 i) requires the secondary authenticator to:
 - 3100 i) be signed when provided directly to Relying Party, or;
 - 3101 ii) have a minimum of 64 bits of entropy when provision is indirect (i.e.
 - 3102 through the credential user);
 - 3103 **iii) be transmitted to the Subject through a protected channel which is**
 - 3104 **linked to the primary authentication process in such a way that**
 - 3105 **session hijacking attacks are resisted;**
 - 3106 **iv) not be subsequently transmitted over an unprotected channel or to an**
 - 3107 **unauthenticated party while it remains valid.**

3108 AL2_CM_ASS#015 No False Authentication

3109 **Employ techniques which ensure that system failures do not result in ‘false positive**

3110 **authentication’ errors.**

3111 AL2_CM_ASS#020 No Post Authentication

3112 *Not* authenticate credentials that have been revoked **unless the time of the transaction**

3113 **for which verification is sought precedes the time of revocation of the credential.**

- 3114 AL2_CM_ASS#030 Proof of Possession
- 3115 Use an authentication protocol that requires the claimant to prove possession and control
3116 of the authentication token.
- 3117 AL2_CM_ASS#040 Assertion Lifetime
- 3118 Generate assertions so as to indicate and effect their expiration:
- 3119 a) 12 hours after their creation, where the service shares a common internet domain
3120 with the Relying Party;
- 3121 b) five minutes after their creation, where the service does not share a common
3122 internet domain with the Relying Party.
- 3123

3124 **3.7.6.3 Assurance Level 3**

3125 **3.7.6.3.1 Assertion Security**

3126 An enterprise and its specified service must:

3127 AL3_CM_ASS#010 Validation and Assertion Security

3128 Provide validation of credentials to a Relying Party using a protocol that:

- 3129 a) requires authentication of the specified service, itself, or of the validation source;
3130 b) ensures the integrity of the authentication assertion.

3131 AL3_CM_ASS#015 No False Authentication

3132 Employ techniques which ensure that system failures do not result in ‘false positive
3133 authentication’ errors.

3134 AL3_CM_ASS#020 Post Authentication

3135 *Not* authenticate credentials that have been revoked unless the time of the transaction for
3136 which verification is sought precedes the time of revocation of the credential.

3137 AL3_CM_ASS#030 Proof of Possession

3138 Use an authentication protocol that requires the claimant to prove possession and control
3139 of the authentication token.

3140 AL3_CM_ASS#040 Assertion Lifetime

3141 **For non-cryptographic credentials**, generate assertions so as to indicate and effect their
3142 expiration 12 hours after their creation; **otherwise, notify the relying party of how often**
3143 **the revocation status sources are updated.**

3144

3145 **3.7.6.4 Assurance Level 4**

3146 **3.7.6.4.1 Assertion Security**

3147 An enterprise and its specified service must:

3148 AL4_CM_ASS#010 Validation and Assertion Security

3149 Provide validation of credentials to a Relying Party using a protocol that:

- 3150 a) requires authentication of the specified service, itself, or of the validation source;
3151 b) ensures the integrity of the authentication assertion.

3152 AL4_CM_ASS#015 No False Authentication

3153 Employ techniques which ensure that system failures do not result in ‘false positive
3154 authentication’ errors.

3155 AL4_CM_ASS#020 Post Authentication

3156 *Not* authenticate credentials that have been revoked unless the time of the transaction for
3157 which verification is sought precedes the time of revocation of the credential.

3158 AL4_CM_ASS#030 Proof of Possession

3159 Use an authentication protocol that requires the claimant to prove possession and control
3160 of the authentication token.

3161 AL4_CM_ASS#040 Assertion Lifetime

3162 **[Omitted]** Notify the relying party of how often the revocation status sources are
3163 updated.

3164

3165 **3.7.7 Compliance Tables**

3166 Use the following tables to correlate criteria for a particular Assurance Level (AL) and
3167 the evidence offered to support compliance.

3168 Service providers preparing for an assessment can use the table appropriate to the AL at
3169 which they are seeking approval to correlate evidence with criteria or to justify non-
3170 applicability (e.g., “specific service types not offered”).

3171 Assessors can use the tables to record the steps in their assessment and their
3172 determination of compliance or failure.

3173 **Table 3-9 CM-SAC - AL1 Compliance**

Clause	Description	Compliance
Part A – Credential Operating Environment		
AL1_CM_CTR#010	No stipulation	No conformity requirement
AL1_CM_CTR#020	Protocol threat risk assessment and controls	
AL1_CM_CTR#025	No stipulation	No conformity requirement
AL1_CM_CTR#030	System threat risk assessment and controls	
AL1_CM_STS#010	Withdrawn	No conformity requirement
AL1_CM_OPN#010	Changeable PIN/Password	
Part B – Credential Issuing		
AL1_CM_IDP#010	Self-managed Identity Proofing	
AL1_CM_IDP#020	Kantara-Recognized outsourced service	
AL1_CM_IDP#030	Non-recognized outsourced service	
AL1_CM_IDP#040	Revision to subscriber information	
AL1_CM_CRN#010	Authenticated Request	
AL1_CM_CRN#020	No stipulation	No conformity requirement
AL1_CM_CRN#030	Credential uniqueness	
Part C – Credential Renewal and Re-issuing		
AL1_CM_RNR#010	Changeable PIN/Password	
Part D – Credential Revocation		
AL1_CM_SRR#010	Submit Request	
Part E – Credential Status Management		
AL1_CM_CSM#010	Maintain Status Record	
AL1_CM_CSM#020	No stipulation	No conformity requirement
AL1_CM_CSM#030	No stipulation	No conformity requirement

AL1_CM_CSM#040	Status Information Availability	
Part F – Credential Validation / Authentication		
AL1_CM_ASS#010	Validation and Assertion Security	
AL1_CM_ASS#015	No stipulation	No conformity requirement
AL1_CM_ASS#020	No Post Authentication	
AL1_CM_ASS#030	Proof of Possession	
AL1_CM_ASS#040	Assertion Lifetime	

3174

3175

Table 3-10 CM-SAC - AL2 Compliance

Clause	Description	Compliance
Part A - Credential Operating Environment		
AL2_CM_CPP#010	Credential Policy and Practice Statement	
AL2_CM_CPP#020	No stipulation	No conformity requirement
AL2_CM_CPP#030	Management Authority	
AL2_CM_CTR#010	Withdrawn	No conformity requirement
AL2_CM_CTR#020	Protocol threat risk assessment and controls	
AL2_CM_CTR#025	Permitted authentication protocols	
AL2_CM_CTR#028	One-time passwords	
AL2_CM_CTR#030	System threat risk assessment and controls	
AL2_CM_CTR#040	Specified Service's Key Management	
AL2_CM_STS#010	Withdrawn	No conformity requirement
AL2_CM_OPN#010	Withdrawn	No conformity requirement
Part B – Credential Issuing		
AL2_CM_IDP#010	Self-managed identity proofing	
AL2_CM_IDP#020	Kantara-Recognized outsourced service	
AL2_CM_IDP#030	Non- Kantara-Recognized outsourced service	
AL2_CM_IDP#040	Revision to subscriber information	
AL2_CM_CRN#010	Authenticated Request	
AL2_CM_CRN#020	Unique identity	
AL2_CM_CRN#030	Credential uniqueness	
AL2_CM_CRN#035	Convey credential	
AL2_CM_CRN#040	Password strength	
AL2_CM_CRN#050	One-time password strength	
AL2_CM_CRN#060	Software cryptographic token strength	
AL2_CM_CRN#070	Hardware token strength	
AL2_CM_CRN#080	No stipulation	No conformity requirement
AL2_CM_CRN#090	Nature of subject	
AL2_CM_CRD#010	Notify Subject of Credential Issuance	
AL2_CM_CRD#015	Confirm Applicant's identity (in person)	
AL2_CM_CRD#016	Confirm Applicant's identity (remotely)	
Part C – Credential Renewal and Re-issuing		

AL2_CM_RNR#010	Changeable PIN/Password	
AL2_CM_RNR#020	Proof-of-possession on Renewal/Re-issuance	
AL2_CM_RNR#030	Renewal/Re-issuance limitations	
Part D – Credential Revocation		
AL2_CM_RVP#010	Revocation procedures	
AL2_CM_RVP#020	Secure status notification	
AL2_CM_RVP#030	Revocation publication	
AL2_CM_RVP#040	Verify revocation identity	
AL2_CM_RVP#050	Revocation Records	
AL2_CM_RVP#060	Record Retention	
AL2_CM_RVR#010	Verify revocation identity	
AL2_CM_RVR#020	Revocation reason	
AL2_CM_RVR#030	Verify Subscriber as Revocant	
AL2_CM_RVR#040	CSP as Revocant	
AL2_CM_RVR#050	Verify Legal Representative as Revocant	
AL2_CM_SRR#010	Submit Request	
Part E – Credential Status Management		
AL2_CM_CSM#010	Maintain Status Record	
AL2_CM_CSM#020	Validation of Status Change Requests	
AL2_CM_CSM#030	Revision to Published Status	
AL2_CM_CSM#040	Status Information Availability	
AL2_CM_CSM#050	Inactive Credentials	
Part F – Credential Validation / Authentication		
AL2_CM_ASS#010	Validation and Assertion Security	
AL2_CM_ASS#015	No False Authentication	
AL2_CM_ASS#020	No Post Authentication	
AL2_CM_ASS#030	Proof of Possession	
AL2_CM_ASS#040	Assertion Lifetime	

3176

3177

Table 3-11 CM-SAC - AL3 Compliance

Clause	Description	Compliance
Part A – Credential Operating Environment		
AL3_CM_CPP#010	Credential Policy and Practice Statement	
AL3_CM_CPP#020	No stipulation	No conformity requirement
AL3_CM_CPP#030	Management Authority	
AL3_CM_CTR#010	No stipulation	No conformity requirement
AL3_CM_CTR#020	Protocol threat risk assessment and controls	
AL3_CM_CTR#025	Permitted authentication protocols	
AL3_CM_CTR#030	System threat risk assessment and controls	
AL3_CM_CTR#040	Specified Service's Key Management	
AL3_CM_STS#010	Withdrawn	No conformity requirement
AL3_CM_STS#020	Stored Secret Encryption	
AL3_CM_SER#010	Security event logs	
AL3_CM_OPN#010	Changeable PIN/Password	
Part B – Credential Issuing		
AL3_CM_IDP#010	Self-managed Identity Proofing	
AL3_CM_IDP#020	Kantara-Recognized outsourced service	
AL3_CM_IDP#030	Non- Kantara-Recognized outsourced service	
AL3_CM_IDP#040	Revision to subscriber information	
AL3_CM_CRN#010	Authenticated Request	
AL3_CM_CRN#020	Unique identity	
AL3_CM_CRN#030	Credential uniqueness	
AL3_CM_CRN#035	Convey credential	
AL3_CM_CRN#040	PIN/Password strength	
AL3_CM_CRN#050	One-time password strength	
AL3_CM_CRN#060	Software cryptographic token strength	
AL3_CM_CRN#070	Hardware token strength	
AL3_CM_CRN#080	Binding of key	
AL3_CM_CRN#090	Nature of subject	
AL3_CM_SKP#010	Key generation by Specified Service	
AL3_CM_SKP#020	Key generation by Subject	
AL3_CM_CRD#010	Notify Subject of Credential Issuance	

AL3_CM_CRD#020	Subject's acknowledgement	
Part C – Credential Renewal and Re-issuing		
AL3_CM_RNR#010	Changeable PIN/Password	
Part D – Credential Revocation		
AL3_CM_RVP#010	Revocation procedures	
AL3_CM_RVP#020	Secure status notification	
AL3_CM_RVP#030	Revocation publication	
AL3_CM_RVP#040	Verify Revocation Identity	
AL3_CM_RVP#050	Revocation Records	
AL3_CM_RVP#060	Record Retention	
AL3_CM_RVR#010	Verify revocation identity	
AL3_CM_RVR#020	Revocation reason	
AL3_CM_RVR#030	Verify Subscriber as Revocant	
AL3_CM_RVR#040	Verify CSP as Revocant	
AL3_CM_RVR#050	Verify Legal Representative as Revocant	
AL3_CM_SRR#010	Submit Request	
Part E – Credential Status Management		
AL3_CM_CSM#010	Maintain Status Record	
AL3_CM_CSM#020	Validation of Status Change Requests	
AL3_CM_CSM#030	Revision to Published Status	
AL3_CM_CSM#040	Status Information Availability	
AL3_CM_CSM#050	Inactive Credentials	
Part F – Credential Validation / Authentication		
AL3_CM_ASS#010	Validation and Assertion Security	
AL3_CM_ASS#015	No False Authentication	
AL3_CM_ASS#020	Post Authentication	
AL3_CM_ASS#030	Proof of Possession	
AL3_CM_ASS#040	Assertion Lifetime	

3178

3179

Table 3-12 CM-SAC - AL4 Compliance

Clause	Description	Compliance
Part A - Credential Operating Environment		
AL4_CM_CPP#010	No stipulation	No conformity requirement
AL4_CM_CPP#020	Certificate Policy/Certification Practice Statement	
AL4_CM_CPP#030	Management Authority	
AL4_CM_CTR#010	No stipulation	No conformity requirement
AL4_CM_CTR#020	Protocol threat risk assessment and controls	
AL4_CM_CTR#025	No stipulation	No conformity requirement
AL4_CM_CTR#030	System threat risk assessment and controls	
AL4_CM_CTR#040	Specified Service's Key Management	
AL4_CM_STS#010	Stored Secrets	
AL4_CM_STS#020	Stored Secret Encryption	
AL4_CM_SER#010	Security event logs	
AL4_CM_OPN#010	Withdrawn	No conformity requirement
Part B – Credential Issuing		
AL4_CM_IDP#010	Self-managed Identity Proofing	
AL4_CM_IDP#020	Kantara-Recognized outsourced service	
AL4_CM_IDP#030	Non- Kantara-Recognized outsourced service	
AL4_CM_IDP#040	Revision to subscriber information	
AL4_CM_CRN#010	Authenticated Request	
AL4_CM_CRN#020	Unique identity	
AL4_CM_CRN#030	Credential uniqueness	
AL4_CM_CRN#035	Convey credential	
AL4_CM_CRN#040	PIN/Password strength	
AL4_CM_CRN#050	One-time password strength	
AL4_CM_CRN#060	Software cryptographic token strength	
AL4_CM_CRN#070	Hardware token strength	
AL4_CM_CRN#080	Binding of key	
AL4_CM_CRN#090	Nature of subject	
AL4_CM_SKP#010	Key generation by Specified Service	
AL4_CM_SKP#020	Key generation by Subject	
AL4_CM_CRD#010	Notify Subject of Credential Issuance	

AL4_CM_CRD#020	Subject's acknowledgement	
Part C – Credential Renewal and Re-issuing		
AL4_CM_RNR#010	Changeable PIN/Password	
Part D – Credential Revocation		
AL4_CM_RVP#010	Revocation procedures	
AL4_CM_RVP#020	Secure status notification	
AL4_CM_RVP#030	Revocation publication	
AL4_CM_RVP#040	No stipulation	No conformity requirement
AL4_CM_RVP#050	Revocation Records	
AL4_CM_RVP#060	Record Retention	
AL4_CM_RVR#010	Verify revocation identity	
AL4_CM_RVR#020	Revocation reason	
AL4_CM_RVR#030	Verify Subscriber as Revocant	
AL4_CM_RVR#040	Verify CSP as Revocant	
AL4_CM_RVR#050	Verify Legal Representative as Revocant	
AL4_CM_RKY#010	Verify Requestor as Subscriber	
AL4_CM_RKY#020	Re-key requests other than subscriber	
AL4_CM_SRR#010	Submit Request	
Part E – Credential Status Management		
AL4_CM_CSM#010	Maintain Status Record	
AL4_CM_CSM#020	Validation of Status Change Requests	
AL4_CM_CSM#030	Revision to Published Status	
AL4_CM_CSM#040	Status Information Availability	
AL4_CM_CSM#050	Inactive Credentials	
Part F – Credential Validation / Authentication		
AL4_CM_ASS#010	Validation and Assertion Security	
AL4_CM_ASS#015	No False Authentication	
AL4_CM_ASS#020	Post Authentication	
AL4_CM_ASS#030	Proof of Possession	
AL4_CM_ASS#040	Assertion Lifetime	

3180

3181 4 REFERENCES

3182

3183 [CAF] Louden, Chris, Spencer, Judy, Burr, Bill, Hawkins, Kevin, Temoshok, David,
3184 Cornell, John, Wilsher, Richard G., Timchak, Steve, Sill, Stephen, Silver, Dave, Harrison,
3185 Von, eds., "E-Authentication Credential Assessment Framework (CAF)," E-
3186 Authentication Initiative, Version 2.0.0 (March 16, 2005).
3187 <http://www.cio.gov/eauthentication/documents/CAF.pdf>

3188

3189 [EAP CSAC 04011] "EAP working paper: Identity Proofing Service Assessment Criteria
3190 (ID-SAC)," Electronic Authentication Partnership, Draft 0.1.3 (July 20, 2004)
3191 http://eap.projectliberty.org/docs/Jul2004/EAP_CSAC_04011_0-1-3_ID-SAC.doc

3192

3193 [EAPTrustFramework] "Electronic Authentication Partnership Trust Framework"
3194 Electronic Authentication Partnership, Version 1.0. (January 6, 2005)
3195 http://eap.projectliberty.org/docs/Trust_Framework_010605_final.pdf

3196

3197 [FIPS140-2] "Security Requirements for Cryptographic Modules" Federal Information
3198 Processing Standards. (May 25, 2001) <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>

3200

3201 [IS27001] ISO/IEC 27001:2005 "Information technology - Security techniques -
3202 Requirements for information security management systems" International Organization
3203 for Standardization.
3204 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

3205

3206 [M-04-04] Bolton, Joshua B., eds., "E-Authentication Guidance for Federal Agencies,"
3207 Office of Management and Budget, (December 16, 2003).
3208 <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>

3209

3210 [NIST800-63] Burr, William E., Dodson, Donna F., Polk, W. Timothy, eds., "Electronic
3211 Authentication Guideline: : Recommendations of the National Institute of Standards and
3212 Technology," Version 1.0.2, National Institute of Standards and Technology, (April,
3213 2006). http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

3214

- 3215 [RFC 3647] Chokhani, S., Ford, W., Sabett, R., Merrill, C., Wu, S., eds., "Internet X.509
3216 Public Key Infrastructure Certificate Policy and Certification Practices Framework," The
3217 Internet Engineering Task Force (November, 2003). <http://www.ietf.org/rfc/rfc3647.txt>
3218
3219