

1



2

3

4

Identity Assurance Framework: Service Assessment Criteria

5

6

7

8

9

Version: 2.0

10

Date: 2010-04-08

11

Editor: Richard G. Wilsher

12

Zygma LLC

13

Contributors

14

The full list of contributors can be referenced here:

15

<http://kantarainitiative.org/confluence/display/idassurance/IAF+2.0+Contributors>

16

Abstract

17

The Kantara Initiative Identity Assurance Work Group (IAWG) was formed to foster adoption of identity trust services. The primary deliverable of the IAWG is the Identity Assurance Framework (IAF), which is comprised of many different documents that detail the levels of assurance and the certification program that bring the Framework to the marketplace. The IAF is comprised of a set of documents that includes an Overview publication, the IAF [Glossary](#), a summary [Assurance Levels](#) document, and an [Assurance Assessment Scheme \(AAS\)](#), which encompasses the associated assessment and certification program, as well as several subordinate documents, among them the [Service Assessment Criteria \(SAC\)](#), which establishes baseline criteria for general organizational conformity, identity proofing services, credential strength, and credential management services against which all CSPs will be evaluated. The present document describes the Service Assessment Criteria component of the IAF, including setting out the Assurance 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
57

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. © 2010 Kantara Initiative.

58

59

60 **1 INTRODUCTION4**

61 **2 ASSURANCE LEVELS5**

62 **3 SERVICE ASSESSMENT CRITERIA6**

63 3.1 Context and Scope6

64 3.2 Readership6

65 3.3 Criteria Descriptions7

66 3.4 Terminology8

67 3.5 Common Organizational Service Assessment Criteria9

68 3.5.1 Assurance Level 19

69 3.5.2 Assurance Level 212

70 3.5.3 Assurance Level 322

71 3.5.4 Assurance Level 432

72 3.5.5 Compliance Tables42

73 3.6 Identity Proofing Service Assessment Criteria49

74 3.6.1 Assurance Level 149

75 3.6.2 Assurance Level 251

76 3.6.3 Assurance Level 357

77 3.6.4 Assurance Level 463

78 3.6.5 Compliance Tables68

79 3.7 Credential Management Service Assessment Criteria72

80 3.7.1 Part A - Credential Operating Environment72

81 3.7.2 Part B - Credential Issuing85

82 3.7.3 Part C - Credential Renewal and Re-issuing99

83 3.7.4 Part D - Credential Revocation103

84 3.7.5 Part E - Credential Status Management114

85 3.7.6 Part F - Credential Validation/Authentication118

86 3.7.7 Compliance Tables124

87 **4 REFERENCES132**

88

89

90 1 INTRODUCTION

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

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

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

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

125 **2 ASSURANCE LEVELS**

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

130 **3 SERVICE ASSESSMENT CRITERIA**

131 **3.1 Context and Scope**

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

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

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

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

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

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

154 **3.2 Readership**

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

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

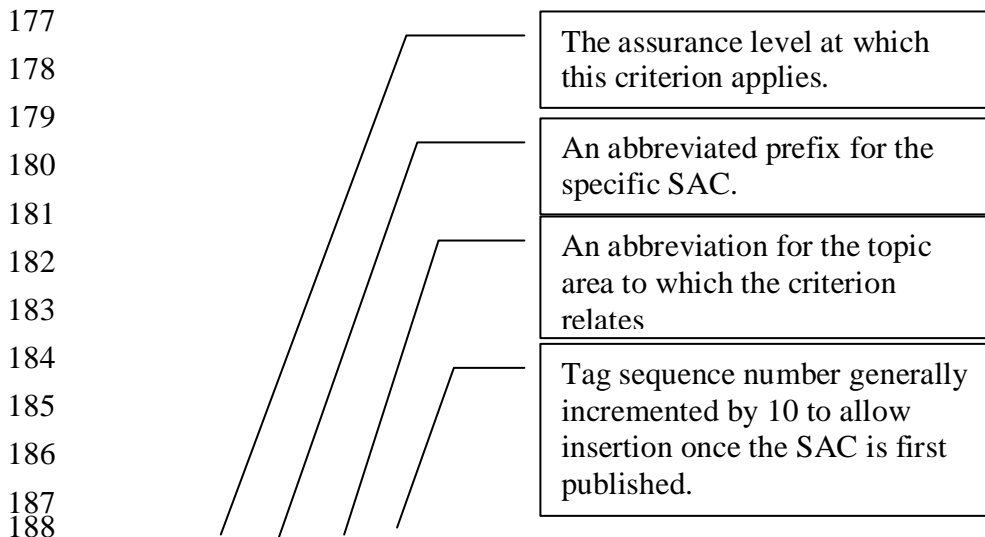
164 This document will also be of interest to those wishing to have a detailed understanding
165 of the operation of the Identity Assurance Framework but who are not actively involved
166 in its operations or in services that may fall within the scope of the Framework.

167 3.3 Criteria Descriptions

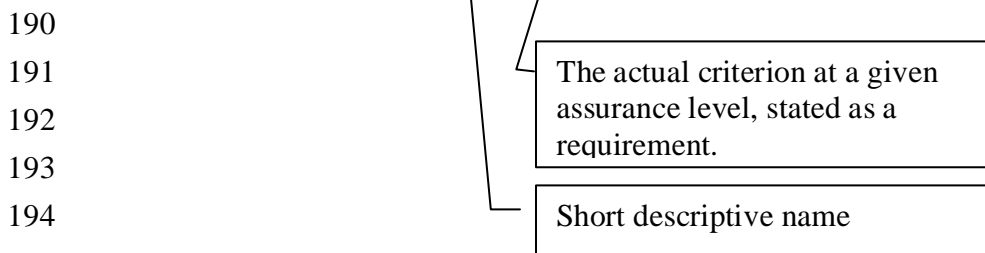
168 The Service Assessment Criteria are organized by AL. Subsections within each level
169 describe the criteria that apply to specific functions. The subsections are parallel.
170 Subsections describing the requirements for the same function at different levels of
171 assurance have the same title.

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

176 The criteria are described as follows:



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



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

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

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

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

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

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

213 **3.4 Terminology**

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

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

218

219 **3.5 Common Organizational Service Assessment Criteria**

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

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

227 **3.5.1 Assurance Level 1**

228 **3.5.1.1 Enterprise and Service Maturity**

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

232 An enterprise and its specified service must:

233 AL1_CO_ESM#010 Established enterprise

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

236 AL1_CO_ESM#020 Established service

237 Be fully operational in all areas described in the assessment package submitted for
238 assessment.

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

245 AL1_CO_ESM#030 Legal & Contractual compliance

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

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

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

253 AL1_CO_ESM#040 No stipulation

254 AL1_CO_ESM#050 No stipulation

255 AL1_CO_ESM#055 Termination provisions

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

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

266 3.5.1.2 Notices and User information

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

269 An enterprise and its specified service must:

270 AL1_CO_NUI#010 General Service Definition

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

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

276 AL1_CO_NUI#020 Service Definition inclusions

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

279 a) a Privacy Policy

280

- 281 AL1_CO_NUI#030 Due notification
- 282 Have in place and follow appropriate policy and procedures to ensure that it notifies
283 Users in a timely and reliable fashion of any changes to the Service Definition and any
284 applicable Terms, Conditions, and Privacy Policy for the specified service.
- 285 AL1_CO_NUI#040 User Acceptance
- 286 Require subscribers and subjects to:
- 287 a) indicate, prior to receiving service, that they have read and accept the terms of
288 service as defined in the Service Definition;
- 289 b) at periodic intervals, determined by significant service provision events (e.g.
290 issuance, re-issuance, renewal), re-affirm their understanding and observance of
291 the terms of service;
- 292 c) always provide full and correct responses to requests for information.
- 293 AL1_CO_NUI#050 Record of User Acceptance
- 294 Obtain a record (hard-copy or electronic) of the subscriber's and subject's acceptance of
295 the terms and conditions of service, prior to initiating the service and thereafter at
296 periodic intervals, determined by significant service provision events (e.g. re-issuance,
297 renewal).
- 298
- 299 **3.5.1.3 Not used**
- 300 **3.5.1.4 Not used**
- 301 **3.5.1.5 Not used**
- 302 **3.5.1.6 Not used**
- 303 **3.5.1.7 Secure Communications**
- 304 AL1_CO_SCO#010 No stipulation
- 305 AL1_CO_SCO#020 Limited access to shared secrets
- 306 Ensure that:
- 307 a) access to shared secrets shall be subject to discretionary controls which permit
308 access to those roles/applications needing such access;
- 309 b) stored shared secrets are not held in their plaintext form unless given adequate
310 physical or logical protection;
- 311 c) any plaintext passwords or secrets are not transmitted across any public or
312 unsecured network.
- 313

314 **3.5.2 Assurance Level 2**

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

318 **3.5.2.1 Enterprise and Service Maturity**

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

321 An enterprise and its specified service must:

322 AL2_CO_ESM#010 Established enterprise

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

325 AL2_CO_ESM#020 Established service

326 Be fully operational in all areas described in the assessment package submitted for
327 assessment.

328 AL2_CO_ESM#030 Legal & Contractual compliance

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

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

339 AL2_CO_ESM#040 Financial Provisions

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

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

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

350 AL2_CO_ESM#050 Data Retention and Protection

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

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

362 AL2_CO_ESM#055 Termination provisions

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

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

373 **3.5.2.2 Notices and User Information/Agreements**

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

377 An enterprise and its specified service must:

378 AL2_CO_NUI#010 General Service Definition

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

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

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

385 AL2_CO_NUI#020 Service Definition inclusions

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

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

404 AL2_CO_NUI#030 Due notification

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

410 AL2_CO_NUI#040 User Acceptance

411 Require subscribers and subjects to:

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

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

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

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

482 AL2_CO_ISM#100 Audit Records

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

489 AL2_CO_ISM#110 Termination provisions

490 This is now AL2_CO_ESM#055.

491

492 **3.5.2.4 Security-relevant Event (Audit) Records**

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

495 An enterprise and its specified service must:

496 AL2_CO_SER#010 Security event logging

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

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

505

506 **3.5.2.5 Operational infrastructure**

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

510 An enterprise and its specified service must:

- 511 AL2_CO_OPN#010 Technical security
- 512 **Demonstrate that the technical controls employed will provide the level of security**
513 **protection required by the risk assessment and the ISMS, or other IT security**
514 **management methods recognized by a government or professional body, and that**
515 **these controls are effectively integrated with the applicable procedural and physical**
516 **security measures.**
- 517 **Guidance:** Appropriate technical controls, suited to this Assurance Level, should be
518 selected from [NIST800-63] or its equivalent, as established by a recognized national
519 technical authority.
- 520 AL2_CO_OPN#020 Defined security roles
- 521 **Define, by means of a job description, the roles and responsibilities for each service-**
522 **related security-relevant task, relating it to specific procedures, (which shall be set**
523 **out in the ISMS, or other IT security management methodology recognized by a**
524 **government or professional body) and other service-related job descriptions. Where**
525 **the role is security-critical or where special privileges or shared duties exist, these**
526 **must be specifically identified as such, including the applicable access privileges**
527 **relating to logical and physical parts of the service's operations.**
- 528 AL2_CO_OPN#030 Personnel recruitment
- 529 **Demonstrate that it has defined practices for the selection, evaluation, and**
530 **contracting of all service-related personnel, both direct employees and those whose**
531 **services are provided by third parties.**
- 532 AL2_CO_OPN#040 Personnel skills
- 533 **Ensure that employees are sufficiently trained, qualified, experienced, and current**
534 **for the roles they fulfill. Such measures must be accomplished either by recruitment**
535 **practices or through a specific training program. Where employees are undergoing**
536 **on-the-job training, they must only do so under the guidance of a mentor possessing**
537 **the defined service experiences for the training being provided.**
- 538 AL2_CO_OPN#050 Adequacy of Personnel resources
- 539 **Have sufficient staff to adequately operate and resource the specified service**
540 **according to its policies and procedures.**
- 541 AL2_CO_OPN#060 Physical access control
- 542 **Apply physical access control mechanisms to ensure that:**
- 543 a) **access to sensitive areas is restricted to authorized personnel;**

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

546 Require a minimum of two person physical access control when accessing any
547 cryptographic modules.

548 AL2_CO_OPN#070 Logical access control

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

551

552 **3.5.2.6 External Services and Components**

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

556 An enterprise and its specified service must:

557 AL2_CO_ESC#010 Contracted policies and procedures

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

563 AL2_CO_ESC#020 Visibility of contracted parties

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

569

570 **3.5.2.7 Secure Communications**

571 An enterprise and its specified service must:

572 AL2_CO_SCO#010 Secure remote communications

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

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

580 AL2_CO_SCO#015 Verification / Authentication confirmation messages

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

587 AL2_CO_SCO#016 Verification of Revoked Credential

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

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

595 AL2_CO_SCO#020 Limited access to shared secrets

596 Ensure that:

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

604
605 **These roles should be defined and documented by the CSP in accordance with**
606 **AL2_CO_OPN#020 above.**

607 AL2_CO_SCO#030 Logical protection of shared secrets

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

- 609 a) **concatenation of the password to a salt and/or username which is then hashed**
 - 610 **with an Approved algorithm such that the computations used to conduct a**
 - 611 **dictionary or exhaustion attack on a stolen password file are not useful to**
 - 612 **attack other similar password files, or;**

 - 613 b) **encryption using an Approved algorithm and modes, and the shared secret**
 - 614 **decrypted only when immediately required for authentication, or;**

 - 615 c) **any secure method allowed to protect shared secrets at Level 3 or 4.**
- 616
- 617

618 **3.5.3 Assurance Level 3**

619 Achieving AL3 requires meeting more stringent criteria in addition to all criteria required
620 to achieve AL2.

621 **3.5.3.1 Enterprise and Service Maturity**

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

624 An enterprise and its specified service must:

625 AL3_CO_ESM#010 Established enterprise

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

628 AL3_CO_ESM#020 Established service

629 Be fully operational in all areas described in the assessment package submitted for
630 assessment.

631 AL3_CO_ESM#030 Legal & Contractual compliance

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

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

642 AL3_CO_ESM#040 Financial Provisions

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

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

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

653 AL3_CO_ESM#050 Data Retention and Protection

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

660 AL3_CO_ESM#055 Termination provisions

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

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

671 AL3_CO_ESM#060 Ownership

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

675 AL3_CO_ESM#070 Independent management and operations

676 **Demonstrate that, for the purposes of providing the specified service, its**
677 **management and operational structures are distinct, autonomous, have discrete**
678 **legal accountability, and operate according to separate policies, procedures, and**
679 **controls.**

680

681 **3.5.3.2 Notices and User Information**

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

685 An enterprise and its specified service must:

686 AL3_CO_NUI#010 General Service Definition

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

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

693 AL3_CO_NUI#020 Service Definition inclusions

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

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

712 AL3_CO_NUI#030 Due notification

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

718 AL3_CO_NUI#040 User Acceptance

719 Require subscribers and subjects to:

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

726 AL3_CO_NUI#050 Record of User Acceptance

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

731 AL3_CO_NUI#060 Withdrawn

732 Withdrawn.

733 AL3_CO_NUI#070 Change of Subscriber Information

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

738 AL3_CO_NUI#080 Withdrawn

739 Withdrawn.

740

741 **3.5.3.3 Information Security Management**

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

747 An enterprise and its specified service must:

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

779 AL3_CO_ISM#070 System Installation and Operation Controls

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

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

792 AL3_CO_ISM#080 Internal Service Audit

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

797 AL3_CO_ISM#090 Independent Audit

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

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

806 AL3_CO_ISM#100 Audit Records

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

813 AL3_CO_ISM#110 Termination provisions

814 This is now AL3_CO_ESM#055.

815 AL3_CO_ISM#120 Best Practice Security Management

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

822

823 **3.5.3.4 Security-Relevant Event (Audit) Records**

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

826 An enterprise and its specified service must:

827 AL3_CO_SER#010 Security Event Logging

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

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

836

837 **3.5.3.5 Operational Infrastructure**

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

841 An enterprise and its specified service must:

842 AL3_CO_OPN#010 Technical security

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

846 controls are effectively integrated with the applicable procedural and physical security
847 measures.

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

851 AL3_CO_OPN#020 Defined security roles

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

859 AL3_CO_OPN#030 Personnel recruitment

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

865 AL3_CO_OPN#040 Personnel skills

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

871 AL3_CO_OPN#050 Adequacy of Personnel resources

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

874 AL3_CO_OPN#060 Physical access control

875 Apply physical access control mechanisms to ensure that:

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

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

880 AL3_CO_OPN#070 Logical access control

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

883

884 3.5.3.6 External Services and Components

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

888 An enterprise and its specified service must:

889 AL3_CO_ESC#010 Contracted policies and procedures

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

895 AL3_CO_ESC#020 Visibility of contracted parties

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

901

902 3.5.3.7 Secure Communications

903 An enterprise and its specified service must:

904 AL3_CO_SCO#010 Secure remote communications

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

911 **cryptographic module**, or equivalent, as established by a recognized national technical
912 authority.

913 AL3_CO_SCO#020 Limited access to shared secrets

914 Ensure that:

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

932
933 **These roles should be defined and documented by the CSP in accordance with**
934 **AL3_CO_OPN#020 above.**

935
936

937 **3.5.4 Assurance Level 4**

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

940 **3.5.4.1 Enterprise and Service Maturity**

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

943 An enterprise and its specified service must:

944 AL4_CO_ESM#010 Established enterprise

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

947 AL4_CO_ESM#020 Established service

948 Be fully operational in all areas described in the assessment package submitted for
949 assessment.

950 AL4_CO_ESM#030 Legal & Contractual compliance

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

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

961 AL4_CO_ESM#040 Financial Provisions

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

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

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

972 AL4_CO_ESM#050 Data Retention and Protection

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

979 Termination provisions

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

985 **Guidance:** Termination covers the cessation of the business activities, the service
986 provider itself ceasing business operations altogether, change of ownership of the service-
987 providing business, and other similar events which change the status and/or operations of
988 the service provider in any way which interrupts the continued provision of the specific
989 service.

990 AL4_CO_ESM#060 Ownership

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

994 AL4_CO_ESM#070 Independent Management and Operations

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

998

999 **3.5.4.2 Notices and Subscriber Information/Agreements**

1000 Criteria in this section address the publication of information describing the service and
1001 the manner of and any limitations upon its provision, and how users are required to accept
1002 those terms.

- 1003 An enterprise and its specified service must:
- 1004 AL4_CO_NUI#010 General Service Definition
- 1005 Make available to the intended user community a Service Definition that includes all
1006 applicable Terms, Conditions, and Fees, including any limitations of its usage, and
1007 definitions of any terms having specific intention or interpretation. Specific provisions
1008 are stated in further criteria in this section.
- 1009 **Guidance:** The intended user community encompasses potential and actual subscribers,
1010 subjects, and relying parties.
- 1011 AL4_CO_NUI#020 Service Definition inclusions
- 1012 Make available a Service Definition for the specified service containing clauses that
1013 provide the following information:
- 1014 a) Privacy, Identity Proofing & Verification, and Revocation and Termination
1015 Policies;
- 1016 b) the country in or legal jurisdiction under which the service is operated;
- 1017 c) if different to the above, the legal jurisdiction under which subscriber and any
1018 relying party agreements are entered into;
- 1019 d) applicable legislation with which the service complies;
- 1020 e) obligations incumbent upon the CSP;
- 1021 f) obligations incumbent upon the subscriber;
- 1022 g) notifications and guidance for relying parties, especially in respect of actions they
1023 are expected to take should they choose to rely upon the service's product;
- 1024 h) statement of warranties;
- 1025 i) statement of liabilities toward both Subjects and Relying Parties;
- 1026 j) procedures for notification of changes to terms and conditions;
- 1027 k) steps the CSP will take in the event that it chooses or is obliged to terminate the
1028 service;
- 1029 l) availability of the specified service per se and of its help desk facility.
- 1030 AL4_CO_NUI#030 Due Notification
- 1031 Have in place and follow appropriate policy and procedures to ensure that it notifies
1032 subscribers and subjects in a timely and reliable fashion of any changes to the Service
1033 Definition and any applicable Terms, Conditions, Fees, and Privacy Policy for the
1034 specified service, and provide a clear means by which subscribers and subjects must
1035 indicate that they wish to accept the new terms or terminate their subscription.
- 1036 AL4_CO_NUI#040 User Acceptance
- 1037 Require subscribers and subjects to:

- 1038 a) indicate, prior to receiving service, that they have read and accept the terms of
1039 service as defined in the Service Definition, thereby indicating their properly-
1040 informed opt-in;
1041 b) at periodic intervals, determined by significant service provision events (e.g.
1042 issuance, re-issuance, renewal) and otherwise at least once every five years, re-
1043 affirm their understanding and observance of the terms of service;
1044 c) always provide full and correct responses to requests for information.

1045 AL4_CO_NUI#050 Record of User Acceptance

1046 Obtain a record (hard-copy or electronic) of the subscriber's and subject's acceptance of
1047 the terms and conditions of service, prior to initiating the service and thereafter reaffirm
1048 the agreement at periodic intervals, determined by significant service provision events
1049 (e.g. issuance, re-issuance, renewal) and otherwise at least once every five years.

1050 AL4_CO_NUI#060 Withdrawn

1051 Withdrawn.

1052 AL4_CO_NUI#070 Change of Subscriber Information

1053 Require and provide the mechanisms for subscribers and subjects to provide in a timely
1054 manner full and correct amendments should any of their recorded information change, as
1055 required under the terms of their use of the service, and only after the subscriber's and/or
1056 subject's identity has been authenticated.

1057 AL4_CO_NUI#080 Withdrawn

1058 Withdrawn.

1059

1060 **3.5.4.3 Information Security Management**

1061 These criteria address the way in which the enterprise manages the security of its
1062 business, the specified service, and information it holds relating to its user community.

1063 This section focuses on the key components that comprise a well-established and
1064 effective Information Security Management System (ISMS), or other IT security
1065 management methodology recognized by a government or professional body.

1066 An enterprise and its specified service must:

1067 AL4_CO_ISM#010 Documented policies and procedures

1068 Have documented all security-relevant administrative, management, and technical
1069 policies and procedures. The enterprise must ensure that these are based upon recognized

- 1070 standards, published references, or organizational guidelines, are adequate for the
1071 specified service, and are implemented in the manner intended.
- 1072 AL4_CO_ISM#020 Policy Management and Responsibility
- 1073 Have a clearly defined managerial role, at a senior level, where full responsibility for the
1074 business' security policies is vested and from which review, approval, and promulgation
1075 of policy and related procedures is applied and managed. The latest approved versions of
1076 these policies must be applied at all times.
- 1077 AL4_CO_ISM#030 Risk Management
- 1078 Demonstrate a risk management methodology that adequately identifies and mitigates
1079 risks related to the specified service and its user community and must show that on-going
1080 risk assessment review is conducted as a part of the business' procedures, such as
1081 adherence to SAS 70 or [\[IS27001\]](#) methods.
- 1082 AL4_CO_ISM#040 Continuity of Operations Plan
- 1083 Have and keep updated a continuity of operations plan that covers disaster recovery and
1084 the resilience of the specified service and must show that **on-going review of this plan is**
1085 **conducted as a part of the business' procedures.**
- 1086 AL4_CO_ISM#050 Configuration Management
- 1087 Demonstrate that there is in place a configuration management system that at least
1088 includes:
- 1089 a) version control for software system components;
1090 b) timely identification and installation of all organizationally-approved patches for
1091 any software used in the provisioning of the specified service;
1092 c) version control and managed distribution for all documentation associated with
1093 the specification, management, and operation of the system, covering both
1094 internal and publicly available materials.
- 1095 AL4_CO_ISM#060 Quality Management
- 1096 Demonstrate that there is in place a quality management system that is appropriate for the
1097 specified service.
- 1098 AL4_CO_ISM#070 System Installation and Operation Controls
- 1099 Apply controls during system development, procurement, installation, and operation that
1100 protect the security and integrity of the system environment, hardware, software, and
1101 communications having particular regard to:

- 1102 a) the software and hardware development environments, for customized
1103 components;
- 1104 b) the procurement process for commercial off-the-shelf (COTS) components;
1105 c) contracted consultancy/support services;
1106 d) shipment of system components;
1107 e) storage of system components;
1108 f) installation environment security;
1109 g) system configuration;
1110 h) transfer to operational status.
- 1111 AL4_CO_ISM#080 Internal Service Audit
- 1112 Be audited at least once every 12 months for effective provision of the specified service
1113 by independent internal audit functions of the enterprise responsible for the specified
1114 service, unless it can show that by reason of its organizational size or due to other
1115 justifiable operational restrictions it is unreasonable to be so audited.
- 1116 AL4_CO_ISM#090 Independent Audit
- 1117 Be audited by an independent auditor at least every 24 months to ensure the
1118 organization's security-related practices are consistent with the policies and procedures
1119 for the specified service.
- 1120 **Guidance:** The appointed auditor should have appropriate accreditation or other
1121 acceptable experience and qualification, comparable to that required of Kantara-
1122 Accredited Assessors. It is expected that it will be cost-effective for the organization to
1123 use the same Kantara-Accredited Assessor for the purposes of fulfilling this criterion as
1124 they do for the maintenance of their grant of Kantara Recognition.
- 1125 AL4_CO_ISM#100 Audit Records
- 1126 Retain records of all audits, both internal and independent, for a period which, as a
1127 minimum, fulfills its legal obligations and otherwise for greater periods either as it may
1128 have committed to in its Service Definition or required by any other obligations it has
1129 with/to a subscriber, and which in any event is not less than 36 months. Such records
1130 must be held securely and be protected against unauthorized access loss, alteration, public
1131 disclosure, or unapproved destruction.
- 1132 AL4_CO_ISM#110 Termination provisions
- 1133 This is now AL4_CO_ESM#055.

1134 AL4_CO_ISM#120 Best Practice Security Management

1135 Have in place a certified Information Security Management System (ISMS), or other IT
1136 security management methodology recognized by a government or professional body,
1137 that **has been assessed and found to be in compliance with the requirements of**
1138 **ISO/IEC 27001 [IS27001] and which applies and is appropriate to the CSP in**
1139 **question.** All requirements expressed in preceding criteria in this section must *inter alia*
1140 fall wholly within the scope of this ISMS, or the selected recognized alternative.

1141

1142 3.5.4.4 Security-Related (Audit) Records

1143 The criteria in this section are concerned with the need to provide an auditable log of all
1144 events that are pertinent to the correct and secure operation of the service.

1145 An enterprise and its specified service must:

1146 AL4_CO_SER#010 Security Event Logging

1147 Maintain a log of all relevant security events concerning the operation of the service,
1148 together with a **precise** record of the time at which the event occurred (time-stamp)
1149 **provided by a trusted time-source** and retain such records with appropriate protection
1150 and controls to ensure successful retrieval, accounting for service definition, risk
1151 management requirements, applicable legislation, and organizational policy.

1152 **Guidance:** The trusted time source could be an external trusted service or a network time
1153 server or other hardware timing device. The time source must be not only precise but
1154 authenticatable as well.

1155

1156 3.5.4.5 Operational Infrastructure

1157 The criteria in this section address the infrastructure within which the delivery of the
1158 specified service takes place. It puts particular emphasis upon the personnel involved,
1159 and their selection, training, and duties.

1160 An enterprise and its specified service must:

1161 AL4_CO_OPN#010 Technical Security

1162 Demonstrate that the technical controls employed will provide the level of security
1163 protection required by the risk assessment and the ISMS, or other IT security
1164 management methods recognized by a government or professional body, and that these
1165 controls are effectively integrated with the applicable procedural and physical security
1166 measures.

- 1167 **Guidance:** Appropriate technical controls, suited to this Assurance Level, should be
1168 selected from [\[NIST800-63\]](#) or its equivalent, as established by a recognized national
1169 technical authority.
- 1170 AL4_CO_OPN#020 Defined Security Roles
- 1171 Define, by means of a job description, the roles and responsibilities for each service-
1172 related security-relevant task, relating it to specific procedures (which shall be set out in
1173 the ISMS, or other IT security management methodology recognized by a government or
1174 professional body) and other service-related job descriptions. Where the role is security-
1175 critical or where special privileges or shared duties exist, these must be specifically
1176 identified as such, including the applicable access privileges relating to logical and
1177 physical parts of the service's operations.
- 1178 AL4_CO_OPN#030 Personnel Recruitment
- 1179 Demonstrate that it has defined practices for the selection, vetting, and contracting of all
1180 service-related personnel, both direct employees and those whose services are provided
1181 by third parties. Full records of all searches and supporting evidence of qualifications and
1182 past employment must be kept for the duration of the individual's employment plus the
1183 longest lifespan of any credential issued under the Service Policy.
- 1184 AL4_CO_OPN#040 Personnel skills
- 1185 Ensure that employees are sufficiently trained, qualified, experienced, and current for the
1186 roles they fulfill. Such measures must be accomplished either by recruitment practices or
1187 through a specific training program. Where employees are undergoing on-the-job
1188 training, they must only do so under the guidance of a mentor possessing the defined
1189 service experiences for the training being provided.
- 1190 AL4_CO_OPN#050 Adequacy of Personnel resources
- 1191 Have sufficient staff to adequately operate and resource the specified service according to
1192 its policies and procedures.
- 1193 AL4_CO_OPN#060 Physical access control
- 1194 Apply physical access control mechanisms to ensure that:
- 1195 a) access to sensitive areas is restricted to authorized personnel;
- 1196 b) all removable media and paper documents containing sensitive information as
1197 plain-text are stored in secure containers;
- 1198 c) there is 24/7 monitoring for unauthorized intrusions.
1199

1200 AL4_CO_OPN#070 Logical access control

1201 Employ logical access control mechanisms that ensure access to sensitive system
1202 functions and controls is restricted to authorized personnel.

1203

1204 **3.5.4.6 External Services and Components**

1205 This section addresses the relationships and obligations upon contracted parties both to
1206 apply the policies and procedures of the enterprise and also to be available for assessment
1207 as critical parts of the overall service provision.

1208 An enterprise and its specified service must:

1209 AL4_CO_ESC#010 Contracted Policies and Procedures

1210 Where the enterprise uses external suppliers for specific packaged components of the
1211 service or for resources which are integrated with its own operations and under its
1212 control, ensure that those parties are engaged through reliable and appropriate contractual
1213 arrangements which stipulate which critical policies, procedures, and practices sub-
1214 contractors are required to fulfill.

1215 AL4_CO_ESC#020 Visibility of Contracted Parties

1216 Where the enterprise uses external suppliers for specific packaged components of the
1217 service or for resources which are integrated with its own operations and under its
1218 control, ensure that the suppliers' compliance with contractually-stipulated policies and
1219 procedures, and thus with the IAF Service Assessment Criteria, can be independently
1220 verified, and subsequently monitored if necessary.

1221

1222 **3.5.4.7 Secure Communications**

1223 An enterprise and its specified service must:

1224 AL4_CO_SCO#010 Secure remote communications

1225 If the specific service components are located remotely from and communicate over a
1226 public or unsecured network with other service components or other CSPs it services, the
1227 communications must be cryptographically authenticated, including long-term and
1228 session tokens, by an authentication protocol that meets the requirements of AL4 and
1229 encrypted using either a FIPS 140-2 [FIPS140-2] Level 2 (or higher) validated hardware
1230 cryptographic module or any FIPS 140-2 Level 3 or 4 validated cryptographic module, or
1231 equivalent, as established by a recognized national technical authority.

- 1232 AL4_CO_SCO#020 Limited access to shared secrets
- 1233 Ensure that:
- 1234 a) access to shared secrets shall be subject to discretionary controls which permit
 - 1235 access to those roles/applications which need such access;
 - 1236 b) stored shared secrets are encrypted such that:
 - 1237 i the encryption key for the shared secret file is encrypted under a key held
 - 1238 in a FIPS 140-2 [FIPS140-2] Level 2 (or higher) validated hardware
 - 1239 cryptographic module, or equivalent, as established by a recognized
 - 1240 national technical authority, or any FIPS 140-2 Level 3 or 4 validated
 - 1241 cryptographic module, or equivalent, as established by a recognized
 - 1242 national technical authority, and decrypted only as immediately required
 - 1243 for an authentication operation;
 - 1244 ii they are protected as a key within the boundary of a FIPS 140-2 Level 2
 - 1245 (or higher) validated hardware cryptographic module, or equivalent, as
 - 1246 established by a recognized national technical authority, or any
 - 1247 FIPS 140-2 Level 3 or 4 cryptographic module, or equivalent, as
 - 1248 established by a recognized national technical authority, and are not
 - 1249 exported in plaintext from the module;
 - 1250 iii they are split by an "*n from m*" cryptographic secret-sharing method;
 - 1251 c) any long-term (i.e., not session) shared secrets are revealed only to the subscriber
 - 1252 and the CSP's direct agents (bearing in mind (a) above).
 - 1253
 - 1254

1255 **3.5.5 Compliance Tables**

1256 Use the following tables to correlate criteria for a particular Assurance Level (AL) and
1257 the evidence offered to support compliance.

1258 Service providers preparing for an assessment can use the table appropriate to the AL at
1259 which they are seeking approval to correlate evidence with criteria or to justify non-
1260 applicability (e.g., "specific service types not offered").

1261 Assessors can use the tables to record the steps in their assessment and their
1262 determination of compliance or failure.

1263 **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	

1264

1265

1266

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	

1267

1268

1269

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	

1270

1271

1272

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	

1273

1274

1275 **3.6 Identity Proofing Service Assessment Criteria**

1276 The Service Assessment Criteria in this section establish the requirements for the
1277 technical conformity of identity proofing services at all ALs defined in Section 2 and in
1278 the [Identity Assurance Framework: Levels of Assurance](#) document. These criteria apply
1279 to a particular kind of electronic trust service (ETS) recognized by the IAWG and to the
1280 related credential service provider (CSP)—an identity proofing service for both
1281 individual identity and institutional identity credentials¹. (For definitions of terms used in
1282 this section, see the [Identity Assurance Framework: Glossary](#) document). These criteria
1283 are generally referred to elsewhere within IAWG documentation as ID-SAC [ID-SAC].

1284 These criteria do not address the delivery of a credential to the applicant/subscriber,
1285 which is dealt with by the Credential Management SAC (CM-SAC), described in Section
1286 3.7.

1287 These criteria may only be used in an assessment in one of the following circumstances:

- 1288 • In conjunction with the Common Organizational SAC (CO-SAC), described in
1289 Section 3.5, for a standalone identity proofing service.
- 1290 • In combination with one or more other SACs that must include the CO-SAC and
1291 where the identity proofing functions that these criteria address form part of a
1292 larger service offering.

1293 **3.6.1 Assurance Level 1**

1294 **3.6.1.1 Policy**

1295 An enterprise or specified service must:

1296 AL1_ID_POL#010 Unique service identity

1297 Ensure that a unique identity is attributed to the specific service, such that credentials
1298 issued by it can be distinguishable from those issued by other services, including services
1299 operated by the same enterprise.

1300 AL1_ID_POL#020 Unique subject identity

1301 Ensure that each applicant's identity is unique within the service's community of subjects
1302 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.

1303

1304 **3.6.1.2 Identity Verification**

1305 **3.6.1.2.1 In-Person Public Verification**

1306 An enterprise or specified service must:

1307 AL1_ID_IPV#010 Required evidence

1308 Accept a self-assertion of identity.

1309 AL1_ID_IPV#020 Evidence checks

1310 Accept self-attestation of evidence.

1311

1312 **3.6.1.2.2 Remote Public Verification**

1313 If the specific service offers remote identity proofing to applicants with whom it has no
1314 previous relationship, then it must comply with the criteria in this section.

1315 An enterprise or specified service must:

1316 AL1_ID_RPV#010 Required evidence

1317 Require the applicant to provide a contact telephone number or email address.

1318 AL1_ID_RPV#020 Evidence checks

1319 Verify the provided information by either:

1320 a) confirming the request by calling the number;

1321 b) successfully sending a confirmatory email and receiving a positive
1322 acknowledgement.

1323

1324 **3.6.1.2.3 Secondary Verification**

1325 In each of the above cases, an enterprise or specified service must:

1326 AL1_ID_SCV#010 Secondary checks

1327 Have in place additional measures (e.g., require additional documentary evidence, delay
1328 completion while out-of-band checks are undertaken) to deal with any anomalous
1329 circumstances that can be reasonably anticipated (e.g., a legitimate and recent change of
1330 address that has yet to be established as the address of record).

1331

1332

1333 **3.6.2 Assurance Level 2**

1334 **3.6.2.1 Policy**

1335 The specific service must show that it applies identity proofing policies and procedures
1336 and that it retains appropriate records of identity proofing activities and evidence.

1337 The enterprise or specified service must:

1338 AL2_ID_POL#010 Unique service identity

1339 Ensure that a unique identity is attributed to the specific service, such that credentials
1340 issued by it can be distinguishable from those issued by other services, including services
1341 operated by the same enterprise.

1342 AL2_ID_POL#020 Unique subject identity

1343 Ensure that each applicant's identity is unique within the service's community of subjects
1344 and uniquely associable with tokens and/or credentials issued to that identity.

1345 AL2_ID_POL#030 Published Proofing Policy

1346 **For each service it offers, make available the Identity Proofing Policy under which it**
1347 **verifies the identity of applicants² in form, language, and media accessible to the**
1348 **declared community of Users.**

1349 AL2_ID_POL#040 Adherence to Proofing Policy

1350 **Perform all identity proofing strictly in accordance with its published Identity**
1351 **Proofing Policy.**

1352

1353 **3.6.2.2 Identity Verification**

1354 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.

- 1355 AL2_ID_IDV#000 Identity Proofing classes
- 1356 a) **include in its Service Definition at least one of the following classes of identity**
1357 **proofing service, and;**
- 1358 b) **may offer any additional classes of identity proofing service it chooses,**
1359 **subject to the nature and the entitlement of the CSP concerned;**
- 1360 c) **Fulfill the applicable assessment criteria according to its choice of identity**
1361 **proofing service, i.e. conform to at least one of the criteria sets defined in:**
- 1362 i) §3.6.2.2.1, “[In-Person Public Verification](#)”;
- 1363 ii) §3.6.2.2.2, “[Remote Public Verification](#)”;
- 1364 iii) §3.6.2.2.3, “[Current Relationship Verification](#)”;
- 1365 iv) §3.6.2.2.4, “[Affiliation Verification](#)”.

1366 **3.6.2.2.1 In-Person Public Verification**

1367 If the specific service offers in-person identity proofing to applicants with whom it has no
1368 previous relationship, then it must comply with the criteria in this section.

1369 The enterprise or specified service must:

- 1370 AL2_ID_IPV#010 Required evidence

1371 **Ensure that the applicant is in possession of a primary Government Picture ID**
1372 **document that bears a photographic image of the holder.**

- 1373 AL2_ID_IPV#020 Evidence checks

1374 **Have in place and apply processes which ensure that the presented document:**

- 1375 a) **appears to be a genuine document properly issued by the claimed issuing**
1376 **authority and valid at the time of application;**
- 1377 b) **bears a photographic image of the holder that matches that of the applicant;**
- 1378 c) **provides all reasonable certainty that the identity exists and that it uniquely**
1379 **identifies the applicant.**
- 1380

1381 **3.6.2.2.2 Remote Public Verification**

1382 If the specific service offers remote identity proofing to applicants with whom it has no
1383 previous relationship, then it must comply with the criteria in this section.

1384 An enterprise or specified service must:

- 1385 AL2_ID_RPV#010 Required evidence
- 1386 **Ensure that the applicant submits the references of and attests to current possession**
1387 **of a primary Government Picture ID document, and one of:**
- 1388 a) **a second Government ID;**
 - 1389 b) **an employee or student ID number;**
 - 1390 c) **a financial account number (e.g., checking account, savings account, loan or**
1391 **credit card) or;**
 - 1392 d) **a utility service account number (e.g., electricity, gas, or water) for an address**
1393 **matching that in the primary document.**
- 1394 **Ensure that the applicant provides additional verifiable personal information that at**
1395 **a minimum must include:**
- 1396 a) **a name that matches the referenced photo-ID;**
 - 1397 b) **date of birth and;**
 - 1398 c) **current address or personal telephone number.**
- 1399 **Additional information may be requested so as to ensure a unique identity, and**
1400 **alternative information may be sought where the enterprise can show that it leads to**
1401 **at least the same degree of certitude when verified.**
- 1402 AL2_ID_RPV#020 Evidence checks
- 1403 **Inspection and analysis of records against the provided identity references with the**
1404 **specified issuing authorities/institutions or through similar databases:**
- 1405 a) **the existence of such records with matching name and reference numbers;**
 - 1406 b) **corroboration of date of birth, current address of record, and other personal**
1407 **information sufficient to ensure a unique identity.**
- 1408
- 1409
- 1410 **Confirm address of record by at least one of the following means:**
- 1411 a) **RA sends notice to an address of record confirmed in the records check and**
1412 **receives a mailed or telephonic reply from applicant;**
 - 1413 b) **RA issues credentials in a manner that confirms the address of record**
1414 **supplied by the applicant, for example by requiring applicant to enter on-line**
1415 **some information from a notice sent to the applicant;**
 - 1416 c) **RA issues credentials in a manner that confirms ability of the applicant to**
1417 **receive telephone communications at telephone number or email at email**
1418 **address associated with the applicant in records. Any secret sent over an**
1419 **unprotected channel shall be reset upon first use.**
- 1420
- 1421 **Additional checks should be performed so as to establish the uniqueness of the**
1422 **claimed identity.**

1423 **Alternative checks may be performed where the enterprise can show that they lead**
1424 **to at least the same degree of certitude.**

1425

1426 **3.6.2.2.3 Current Relationship Verification**

1427 If the specific service offers identity proofing to applicants with whom it has a current
1428 relationship, then it must comply with the criteria in this section.

1429 The enterprise or specified service must:

1430 AL2_ID_CRV#010 Required evidence

1431 **Ensure that it has previously exchanged with the applicant a shared secret (e.g., a**
1432 **PIN or password) that meets AL2 (or higher) entropy requirements³.**

1433 AL2_ID_CRV#020 Evidence checks

1434 **Ensure that it has:**

- 1435 a) **only issued the shared secret after originally establishing the applicant’s**
1436 **identity with a degree of rigor equivalent to that required under either the**
1437 **AL2 (or higher) requirements for in-person or remote public verification;**
1438 b) **an ongoing business relationship sufficient to satisfy the enterprise of the**
1439 **applicant’s continued personal possession of the shared secret.**

1440

1441 **3.6.2.2.4 Affiliation Verification**

1442 If the specific service offers identity proofing to applicants on the basis of some form of
1443 affiliation, then it must comply with the criteria in this section for the purposes of
1444 establishing that affiliation, in addition to the previously stated requirements for the
1445 verification of the individual’s identity.

1446 The enterprise or specified service must:

1447 AL2_ID_AFV#000 Meet preceding criteria

1448 **Meet all the criteria set out above, under §3.6.2.2.3, “[Current Relationship](#)**
1449 **[Verification](#)”.**

1450 AL2_ID_AFV#010 Required evidence

1451 **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.

- 1452 a) **identification from the organization with which it is claiming affiliation;**
1453 b) **agreement from the organization that the applicant may be issued a**
1454 **credential indicating that an affiliation exists.**

1455 AL2_ID_AFV#020 Evidence checks

1456 **Have in place and apply processes which ensure that the presented documents:**

- 1457 a) **each appear to be a genuine document properly issued by the claimed issuing**
1458 **authorities and valid at the time of application;**
1459 b) **refer to an existing organization with a contact address;**
1460 c) **indicate that the applicant has some form of recognizable affiliation with the**
1461 **organization;**
1462 d) **appear to grant the applicant an entitlement to obtain a credential indicating**
1463 **its affiliation with the organization.**
1464

1465 **3.6.2.2.5 Secondary Verification**

1466 In each of the above cases, the enterprise or specified service must:

1467 AL2_ID_SCV#010 Secondary checks

1468 Have in place additional measures (e.g., require additional documentary evidence, delay
1469 completion while out-of-band checks are undertaken) to deal with any anomalous
1470 circumstances that can be reasonably anticipated (e.g., a legitimate and recent change of
1471 address that has yet to be established as the address of record).

1472

1473 **3.6.2.3 Verification Records**

1474 The specific service must retain records of the identity proofing (verification) that it
1475 undertakes and provide them to qualifying parties when so required.

1476 An enterprise or specified service must:

1477 AL2_ID_VRC#010 Verification Records for Personal Applicants

1478 **Log, taking account of all applicable legislative and policy obligations, a record of**
1479 **the facts of the verification process, including a reference relating to the verification**
1480 **processes and the date and time of verification.**

1481 **Guidance:** The facts of the verification process should include the specific record
1482 information (source, unique reference, value/content) used in establishing the applicant's
1483 identity, and will be determined by the specific processes used and documents accepted
1484 by the CSP. The CSP need not retain these records itself if it uses a third-party service
1485 which retains such records securely and to which the CSP has access when required, in

1486 which case it must retain a record of the identity of the third-party service providing the
1487 verification service or the location at which the (in-house) verification was performed.

1488 AL2_ID_VRC#020 Verification Records for Affiliated Applicants

1489 **In addition to the foregoing, log, taking account of all applicable legislative and**
1490 **policy obligations, a record of the additional facts of the verification process must be**
1491 **performed. At a minimum, records of identity information must include:**

- 1492 a) **the subscriber's full name;**
- 1493 b) **the subscriber's current address of record;**
- 1494 c) **the subscriber's current telephone or email address of record;**
- 1495 d) **the subscriber's acknowledgement for issuing the subject with a credential;**
- 1496 e) **type, issuing authority, and reference number(s) of all documents checked in**
1497 **the identity proofing process.**

1498 AL2_ID_VRC#030 Record Retention

1499 **Either retain, securely, the record of the verification process for the duration of the**
1500 **subscriber account plus 7.5 years, or submit same record to a client CSP that has**
1501 **undertaken to retain the record for the requisite period or longer.**

1502

1503

1504 **3.6.3 Assurance Level 3**

1505 **3.6.3.1 Policy**

1506 The specific service must show that it applies identity proofing policies and procedures
1507 and that it retains appropriate records of identity proofing activities and evidence.

1508 The enterprise or specified service must:

1509 AL3_ID_POL#010 Unique service identity

1510 Ensure that a unique identity is attributed to the specific service, such that credentials
1511 issued by it can be distinguishable from those issued by other services, including services
1512 operated by the same enterprise.

1513 AL3_ID_POL#020 Unique subject identity

1514 Ensure that each applicant's identity is unique within the service's community of subjects
1515 and uniquely associable with tokens and/or credentials issued to that identity.

1516 AL3_ID_POL#030 Published Proofing Policy

1517 Make available the Identity Proofing Policy under which it verifies the identity of
1518 applicants⁴ in form, language, and media accessible to the declared community of Users.

1519 AL3_ID_POL#040 Adherence to Proofing Policy

1520 Perform all identity proofing strictly in accordance with its published Identity Proofing
1521 Policy, through application of the procedures and processes set out in its Identity Proofing
1522 Practice Statement.

1523

1524 **3.6.3.2 Identity Verification**

1525 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.

- 1526 AL3_ID_IDV#000 Identity Proofing classes
- 1527 a) include in its Service Definition at least one of the following classes of identity
1528 proofing services, and;
- 1529 b) may offer any additional classes of identity proofing service it chooses, subject to
1530 the nature and the entitlement of the CSP concerned;
- 1531 c) Fulfill the applicable assessment criteria according to its choice of identity
1532 proofing service, i.e. conform to at least one of the criteria sets defined in:
- 1533 i) §3.6.3.2.1, “[In-Person Public Verification](#)”;
- 1534 ii) §3.6.3.2.2, “[Remote Public Verification](#)”;
- 1535 iii) §3.6.3.2.4, “[Affiliation Verification](#)”.
- 1536

1537 **3.6.3.2.1 In-Person Public Verification**

1538 A specific service that offers identity proofing to applicants with whom it has no previous
1539 relationship must comply with the criteria in this section.

1540 The enterprise or specified service must:

- 1541 AL3_ID_IPV#010 Required evidence
- 1542 Ensure that the applicant is in possession of a primary Government Picture ID document
1543 that bears a photographic image of the holder.

- 1544 AL3_ID_IPV#020 Evidence checks
- 1545 **Have in place and apply processes which ensure** that the presented document:
- 1546 a) appears to be a genuine document properly issued by the claimed issuing
1547 authority and valid at the time of application;
- 1548 b) bears a photographic image of the holder that matches that of the applicant;
- 1549 c) **is electronically verified by a record check with the specified issuing
1550 authority or through similar databases that:**
- 1551 i) **establishes the existence of such records with matching name and
1552 reference numbers;**
- 1553 ii) **corroborates date of birth, current address of record, and other
1554 personal information sufficient to ensure a unique identity;**
- 1555 d) provides all reasonable certainty that the identity exists and that it uniquely
1556 identifies the applicant.
- 1557

1558 **3.6.3.2.2 Remote Public Verification**

1559 A specific service that offers remote identity proofing to applicants with whom it has no
1560 previous relationship must comply with the criteria in this section.

1561 The enterprise or specified service must:

1562 AL3_ID_RPV#010 Required evidence

1563 Ensure that the applicant submits the references of and attests to current possession of a
1564 primary Government Picture ID document, and one of:

- 1565 a) a second Government ID;
- 1566 b) an employee or student ID number;
- 1567 c) a financial account number (e.g., checking account, savings account, loan, or
1568 credit card), or;
- 1569 d) a utility service account number (e.g., electricity, gas, or water) for an address
1570 matching that in the primary document.

1571 Ensure that the applicant provides additional verifiable personal information that at a
1572 minimum must include:

- 1573 e) a name that matches the referenced photo-ID;
- 1574 f) date of birth;
- 1575 g) current address or personal telephone number.

1576 Additional information may be requested so as to ensure a unique identity, and alternative
1577 information may be sought where the enterprise can show that it leads to at least the same
1578 degree of certitude when verified.

1579

1580 AL3_ID_RPV#020 Evidence checks

1581 **Electronically verify by a record check against the provided identity references with**
1582 **the specified issuing authorities/institutions or through similar databases:**

- 1583 a) the existence of such records with matching name and reference numbers;
- 1584 b) corroboration of date of birth, current address of record, **or personal telephone**
1585 **number**, and other personal information sufficient to ensure a unique identity;
- 1586 c) **dynamic verification of personal information previously provided by or**
1587 **likely to be known only by the applicant.**

1588

1589

1590 Confirm address of record by at least one of the following means:

- 1591 a) RA sends notice to an address of record confirmed in the records check and
1592 receives a mailed or telephonic reply from applicant;

- 1593 b) RA issues credentials in a manner that confirms the address of record supplied by
1594 the applicant, for example by requiring applicant to enter on-line some
1595 information from a notice sent to the applicant;
1596 c) RA issues credentials in a manner that confirms ability of the applicant to receive
1597 telephone communications at telephone number or email at email address
1598 associated with the applicant in records. Any secret sent over an unprotected
1599 channel shall be reset upon first use.
1600

1601 Additional checks may be performed so as to establish the uniqueness of the claimed
1602 identity, and alternative checks may be performed where the enterprise can show that they
1603 lead to at least the same degree of certitude.

1604 **3.6.3.2.3 Current Relationship Verification**

1605 No stipulation.
1606

1607 **3.6.3.2.4 Affiliation Verification**

1608 A specific service that offers identity proofing to applicants on the basis of some form of
1609 affiliation must comply with the criteria in this section to establish that affiliation and
1610 with the previously stated requirements to verify the individual's identity.

1611 The enterprise or specified service must:

1612 AL3_ID_AFV#000 Meet preceding criteria

1613 Meet all the criteria set out above, under §3.6.3.2.2, "[Remote Public Verification](#)".

1614 AL3_ID_AFV#010 Required evidence

1615 Ensure that the applicant possesses:

- 1616 a) identification from the organization with which it is claiming affiliation;
1617 b) agreement from the organization that the applicant may be issued a credential
1618 indicating that an affiliation exists.

1619 AL3_ID_AFV#020 Evidence checks

1620 Have in place and apply processes which ensure that the presented documents:

- 1621 a) each appear to be a genuine document properly issued by the claimed issuing
1622 authorities and valid at the time of application;
1623 b) refer to an existing organization with a contact address;
1624 c) indicate that the applicant has some form of recognizable affiliation with the
1625 organization;

1626 d) appear to grant the applicant an entitlement to obtain a credential indicating an
1627 affiliation with the organization.
1628

1629 **3.6.3.2.5 Secondary Verification**

1630 In each of the above cases, the enterprise or specified service must also meet the
1631 following criteria:

1632 AL3_ID_SCV#010 Secondary checks

1633 Have in place additional measures (e.g., require additional documentary evidence, delay
1634 completion while out-of-band checks are undertaken) to deal with any anomalous
1635 circumstance that can reasonably be anticipated (e.g., a legitimate and recent change of
1636 address that has yet to be established as the address of record).

1637 **3.6.3.3 Verification Records**

1638 The specific service must retain records of the identity proofing (verification) that it
1639 undertakes and provide them to qualifying parties when so required.

1640 The enterprise or specified service must:

1641 AL3_ID_VRC#010 Verification Records for Personal Applicants

1642 Log, taking account of all applicable legislative and policy obligations, a record of the
1643 facts of the verification process **and the identity of the registrar**, including a reference
1644 relating to the verification processes and the date and time of verification.

1645 **Guidance:** The facts of the verification process should include the specific record
1646 information (source, unique reference, value/content) used in establishing the applicant's
1647 identity, and will be determined by the specific processes used and documents accepted
1648 by the CSP. The CSP need not retain these records itself if it uses a third-party service
1649 which retains such records securely and to which the CSP has access when required, in
1650 which case it must retain a record of the identity of the third-party service providing the
1651 verification service or the location at which the (in-house) verification was performed.

1652 AL3_ID_VRC#020 Verification Records for Affiliated Applicants

1653 In addition to the foregoing, log, taking account of all applicable legislative and policy
1654 obligations, a record of the additional facts of the verification process must be performed.
1655 At a minimum, records of identity information must include:

- 1656 a) the 'full name;
- 1657 b) the subscriber's current address of record;
- 1658 c) the subscriber's current telephone or email address of record;
- 1659 d) the subscriber's acknowledgement of issuing the subject with a credential;

- 1660 e) type, issuing authority, and reference number(s) of all documents checked in the
1661 identity proofing process;
1662 f) **where required, a telephone or email address for related contact and/or**
1663 **delivery of credentials/notifications.**

1664 AL3_ID_VRC#030 Record Retention

1665 Either retain, securely, the record of the verification/revocation process for the duration of
1666 the subscriber account plus 7.5 years, or submit the same record to a client CSP that has
1667 undertaken to retain the record for the requisite period or longer.

1668

1669

1670 **3.6.4 Assurance Level 4**

1671 Identity proofing at Assurance Level 4 requires the physical presence of the applicant in
1672 front of the registration officer with photo ID or other readily verifiable biometric identity
1673 information, as well as the requirements set out by the following criteria.

1674 **3.6.4.1 Policy**

1675 The specific service must show that it applies identity proofing policies and procedures
1676 and that it retains appropriate records of identity proofing activities and evidence.

1677 The enterprise or specified service must:

1678 AL4_ID_POL#010 Unique service identity

1679 Ensure that a unique identity is attributed to the specific service, such that credentials
1680 issued by it can be distinguishable from those issued by other services, including services
1681 operated by the same enterprise.

1682 AL4_ID_POL#020 Unique subject identity

1683 Ensure that each applicant's identity is unique within the service's community of subjects
1684 and uniquely associable with tokens and/or credentials issued to that identity.

1685 AL4_ID_POL#030 Published Proofing Policy

1686 Make available the Identity Proofing Policy under which it verifies the identity of
1687 applicants⁵ in form, language, and media accessible to the declared community of users.

1688 AL4_ID_POL#040 Adherence to Proofing Policy

1689 Perform all identity proofing strictly in accordance with its published Identity Proofing
1690 Policy, through application of the procedures and processes set out in its Identity Proofing
1691 Practice Statement.

1692

1693 **3.6.4.2 Identity Verification**

1694 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.

- 1695 AL4_ID_IDV#000 Identity Proofing classes
- 1696 **[Omitted] offer only face-to-face identity proofing service. Remote verification is not**
1697 **allowed at this assurance level;**
- 1698
- 1699 The enterprise or specified service must:
- 1700 **3.6.4.2.1 In-Person Public Verification**
- 1701 AL4_ID_IPV#010 Required evidence
- 1702 Ensure that the applicant is in possession of:
- 1703 a) a primary Government Picture ID document that bears a photographic image of
1704 the **holder and either:**
- 1705 i) **secondary Government Picture ID or an account number issued by a**
1706 **regulated financial institution or;**
- 1707 ii) **two items confirming name, and address or telephone number, such**
1708 **as: utility bill, professional license or membership, or other evidence**
1709 **of equivalent standing.**
- 1710 AL4_ID_IPV#020 No stipulation
- 1711 AL4_ID_IPV#030 Evidence checks – primary ID
- 1712 **Ensure that the presented document:**
- 1713 a) **appears to be a genuine document properly issued by the claimed issuing**
1714 **authority and valid at the time of application;**
- 1715 b) **bears a photographic image of the holder which matches that of the**
1716 **applicant;**
- 1717 c) **is electronically verified by a record check with the specified issuing**
1718 **authority or through similar databases that:**
- 1719 i) **establishes the existence of such records with matching name and**
1720 **reference numbers;**
- 1721 ii) **corroborates date of birth, current address of record, and other**
1722 **personal information sufficient to ensure a unique identity;**
- 1723 d) **provides all reasonable certainty, at AL4, that the identity exists and that it**
1724 **uniquely identifies the applicant.**
- 1725 AL4_ID_IPV#040 Evidence checks – secondary ID
- 1726 **Ensure that the presented document meets the following conditions:**
- 1727 a) **If it is secondary Government Picture ID:**

- 1728 i) appears to be a genuine document properly issued by the claimed
1729 issuing authority and valid at the time of application;
1730 ii) bears a photographic image of the holder which matches that of the
1731 applicant;
1732 iii) states an address at which the applicant can be contacted.
1733 b) If it is a financial institution account number, is verified by a record check
1734 with the specified issuing authority or through similar databases that:
1735 i) establishes the existence of such records with matching name and
1736 reference numbers;
1737 ii) corroborates date of birth, current address of record, and other
1738 personal information sufficient to ensure a unique identity.
1739 c) If it is two utility bills or equivalent documents:
1740 i) each appears to be a genuine document properly issued by the
1741 claimed issuing authority;
1742 ii) corroborates current address of record or telephone number
1743 sufficient to ensure a unique identity.

1744 AL4_ID_IPV#050 Applicant knowledge checks

1745 Where the applicant is unable to satisfy any of the above requirements, that the
1746 applicant can provide a unique identifier, such as a Social Security Number (SSN),
1747 that matches the claimed identity.

1748

1749 **3.6.4.2.2 Remote Public Verification**

1750 Not permitted

1751 **3.6.4.2.3 Affiliation Verification**

1752 A specific service that offers identity proofing to applicants on the basis of some form of
1753 affiliation must comply with the criteria in this section to establish that affiliation, in
1754 addition to complying with the previously stated requirements for verifying the
1755 individual's identity.

1756 The enterprise or specified service must:

1757 AL4_ID_AJV#000 Meet preceding criteria

1758 Meet all the criteria set out above, under §3.6.4.2.1, “[In-Person Public Verification](#)”.

1759 AL4_ID_AJV#010 Required evidence

1760 Ensure that the applicant possesses:

- 1761 a) identification from the organization with which it is claiming affiliation;

1762 b) agreement from the organization that the applicant may be issued a credential
1763 indicating that an affiliation exists.

1764 AL4_ID_AFV#020 Evidence checks

1765 Have in place and apply processes which ensure that the presented documents:

- 1766 a) each appear to be a genuine document properly issued by the claimed issuing
1767 authorities and valid at the time of application;
1768 b) refer to an existing organization with a contact address;
1769 c) indicate that the applicant has some form of recognizable affiliation with the
1770 organization;
1771 d) appear to grant the applicant an entitlement to obtain a credential indicating an
1772 affiliation with the organization.
1773

1774 **3.6.4.2.4 Secondary Verification**

1775 In each of the above cases, the enterprise or specified service must also meet the
1776 following criteria:

1777 AL4_ID_SCV#010 Secondary checks

1778 Have in place additional measures (e.g., require additional documentary evidence, delay
1779 completion while out-of-band checks are undertaken) to deal with any anomalous
1780 circumstances that can reasonably be anticipated (e.g., a legitimate and recent change of
1781 address that has yet to be established as the address of record).

1782

1783 **3.6.4.3 Verification Records**

1784 The specific service must retain records of the identity proofing (verification) that it
1785 undertakes and provide them to qualifying parties when so required.

1786 The enterprise or specified service must:

1787 AL4_ID_VRC#010 Verification Records for Personal Applicants

1788 Log, taking account of all applicable legislative and policy obligations, a record of the
1789 facts of the verification process and the identity of the registrar, including a reference
1790 relating to the verification processes and the date and time of verification **issued by a**
1791 **trusted time-source**.

1792 **Guidance:** The facts of the verification process should include the specific record
1793 information (source, unique reference, value/content) used in establishing the applicant's
1794 identity, and will be determined by the specific processes used and documents accepted
1795 by the CSP. The CSP need not retain these records itself if it uses a third-party service

1796 which retains such records securely and to which the CSP has access when required, in
1797 which case it must retain a record of the identity of the third-party service providing the
1798 verification service or the location at which the (in-house) verification was performed.

1799 AL4_ID_VRC#020 Verification Records for Affiliated Applicants

1800 In addition to the foregoing, log, taking account of all applicable legislative and policy
1801 obligations, a record of the additional facts of the verification process must be performed.
1802 At a minimum, records of identity information must include:

- 1803 a) the subscriber's full name;
- 1804 b) the subscriber's current address of record;
- 1805 c) the subscriber's current telephone or email address of record;
- 1806 d) the subscriber's authorization for issuing the subject a credential;
- 1807 e) type, issuing authority, and reference number(s) of all documents checked in the
1808 identity proofing process;
- 1809 **f) a biometric record of each required representative of the affiliating**
1810 **organization (e.g., a photograph, fingerprint, voice recording), as determined**
1811 **by that organization's governance rules/charter.**

1812 AL4_ID_VRC#030 Record Retention

1813 Either retain, securely, the record of the verification/revocation process for the duration of
1814 the subscriber account plus **10.5** years, or submit the record to a client CSP that has
1815 undertaken to retain the record for the requisite period or longer.

1816

1817

1818 **3.6.5 Compliance Tables**

1819 Use the following tables to correlate criteria for a particular Assurance Level (AL) and
1820 the evidence offered to support compliance.

1821 Service providers preparing for an assessment can use the table appropriate to the AL at
1822 which they are seeking approval to correlate evidence with criteria or to justify non-
1823 applicability (e.g., "specific service types not offered").

1824 Assessors can use the tables to record the steps in their assessment and their
1825 determination of compliance or failure.

1826 **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	

1827

1828

1829

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	

1830

1831

1832

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	

1833

1834

1835

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	

1836

1837

1838 **3.7 Credential Management Service Assessment Criteria**

- 1839 The Service Assessment Criteria in this section establish requirements for the functional
1840 conformity of credential management services and their providers at all ALs defined in
1841 Section 2 and in the [Identity Assurance Framework: Levels of Assurance](#) document.
1842 These criteria are generally referred to elsewhere within IAF documentation as CM-SAC.
- 1843 The criteria are divided into five parts. Each part deals with a specific functional aspect
1844 of the overall credential management process.
- 1845 This SAC must be used in conjunction with the Common Organizational SAC
1846 (CO-SAC), described in Section 3.5, and, in addition, must either:
- 1847 • explicitly include the criteria of the Identity Proofing SAC ([ID-SAC]) described
1848 in Section 3.6, or
 - 1849 • rely upon the criteria of the ID-SAC [ID-SAC] being fulfilled by the use of a
1850 Kantara-approved ID-proofing service.

1851 **3.7.1 Part A - Credential Operating Environment**

1852 The criteria in this part deal with the overall operational environment in which the
1853 credential life-cycle management is conducted. The credential management service
1854 assessment criteria must be used in conjunction with the Common Organizational criteria
1855 described in Section 3.5. In addition, they must either explicitly include the identity
1856 proofing service assessment criteria described in Section 3.6 or rely upon those criteria
1857 being fulfilled by the use of a Kantara-approved identity proofing service.

1858 These criteria describe requirements for the overall operational environment in which
1859 credential lifecycle management is conducted. The common organizational criteria
1860 describe broad requirements. The criteria in this section describe implementation
1861 specifics. Implementation depends on the AL. The procedures and processes required to
1862 create a secure environment for management of credentials and the particular
1863 technologies that are considered strong enough to meet the assurance requirements differ
1864 considerably from level to level.

1865 **3.7.1.1 Assurance Level 1**

1866 These criteria apply to PINs and passwords, as well as SAML assertions.

1867 **3.7.1.1.1 Not used**

1868 No stipulation.

1869

1870 **3.7.1.1.2 Security Controls**

1871 An enterprise and its specified service must:

- 1872 AL1_CM_CTR#010 No stipulation
- 1873 AL1_CM_CTR#020 Protocol threat risk assessment and controls
- 1874 Account for at least the following protocol threats and apply appropriate controls:
- 1875 a) password guessing, such that the resistance to an on-line guessing attack against a
1876 selected user/password is at least 1 in 2^{10} (1,024);
- 1877 b) message replay.
- 1878 AL1_CM_CTR#025 No stipulation
- 1879 AL1_CM_CTR#030 System threat risk assessment and controls
- 1880 Account for the following system threats and apply appropriate controls:
- 1881 a) the introduction of malicious code;
- 1882 b) compromised authentication arising from insider action;
- 1883 c) out-of-band attacks by other users and system operators (e.g., the ubiquitous
1884 shoulder-surfing);
- 1885 d) spoofing of system elements/applications;
- 1886 e) malfeasance on the part of subscribers and subjects.
- 1887
- 1888 **3.7.1.1.3 Storage of Long-term Secrets**
- 1889 AL1_CM_STS#010 Withdrawn
- 1890 Withdrawn (AL1_CO_SCO#020 (a) & (b) enforce this requirement)
- 1891
- 1892 **3.7.1.1.4 Not used**
- 1893 **3.7.1.1.5 Subject Options**
- 1894 AL1_CM_OPN#010 Withdrawn
- 1895 Withdrawn – see AL1_CM_RNR#010.
- 1896

1897 **3.7.1.2 Assurance Level 2**

1898 These criteria apply to passwords, as well as acceptable SAML assertions.

1899 **3.7.1.2.1 Credential Policy and Practices**

1900 These criteria apply to the policy and practices under which credentials are managed.

1901 An enterprise and its specified service must:

1902 AL2_CM_CPP#010 Credential Policy and Practice Statement

1903 **Include in its Service Definition a description of the policy against which it issues**
1904 **credentials and the corresponding practices it applies in their management. At a**
1905 **minimum, the Credential Policy and Practice Statement must specify:**

- 1906 a) **if applicable, any OIDs related to the Practice and Policy Statement;**
1907 b) **how users may subscribe to the service/apply for credentials and how users'**
1908 **credentials will be delivered to them;**
1909 c) **how subscribers acknowledge receipt of tokens and credentials and what**
1910 **obligations they accept in so doing (including whether they consent to**
1911 **publication of their details in credential status directories);**
1912 d) **how credentials may be renewed, modified, revoked, and suspended,**
1913 **including how requestors are authenticated or their identity re-proven;**
1914 e) **what actions a subscriber must take to terminate a subscription;**
1915 f) **how records are retained and archived.**

1916 AL2_CM_CPP#020 No stipulation

1917 AL2_CM_CPP#030 Management Authority

1918 **Have a nominated management body with authority and responsibility for**
1919 **approving the Credential Policy and Practice Statement and for its implementation.**

1920

1921 **3.7.1.2.2 Security Controls**

1922 An enterprise and its specified service must:

1923 AL2_CM_CTR#010 Secret revelation

1924 **Withdrawn.**

1925 AL2_CM_CTR#020 Protocol threat risk assessment and controls

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

- 1928 a) password guessing, such that the resistance to an on-line guessing attack against a
1929 selected user/password is at least 1 in 2^{14} (**16,384**);
- 1930 b) message replay, **showing that it is impractical**;
- 1931 c) **eavesdropping, showing that it is impractical.**
- 1932 AL2_CM_CTR#025 Permitted authentication protocols
- 1933 **Permit only the following authentication protocols:**
- 1934 a) **tunneled password**;
- 1935 b) **zero knowledge-base password**;
- 1936 c) **SAML assertions.**
- 1937 AL2_CM_CTR#028 One-time passwords
- 1938 **Use only one-time passwords which:**
- 1939 a) **are generated using an approved block-cipher or hash function to combine a**
1940 **symmetric key, stored on the device, with a nonce**;
- 1941 b) **derive the nonce from a date and time, or a counter generated on the device**;
- 1942 c) **have a limited lifetime, in the order of minutes.**
- 1943
- 1944 AL2_CM_CTR#030 System threat risk assessment and controls
- 1945 Account for the following system threats **in its risk assessment** and apply **[omitted]**
1946 controls **that reduce them to acceptable risk levels:**
- 1947 a) the introduction of malicious code;
- 1948 b) compromised authentication arising from insider action;
- 1949 c) out-of-band attacks by both users and system operators (e.g., the ubiquitous
1950 shoulder-surfing);
- 1951 d) spoofing of system elements/applications;
- 1952 e) malfeasance on the part of subscribers and subjects;
- 1953 f) **intrusions leading to information theft.**
- 1954 AL2_CM_CTR#040 Specified Service's Key Management
- 1955 **Specify and observe procedures and processes for the generation, storage, and**
1956 **destruction of its own cryptographic keys used for securing the specific service's**
1957 **assertions and other publicized information. At a minimum, these should address:**
- 1958 a) **the physical security of the environment**;
- 1959 b) **access control procedures limiting access to the minimum number of**
1960 **authorized personnel**;
- 1961 c) **public-key publication mechanisms**;
- 1962 d) **application of controls deemed necessary as a result of the service's risk**
1963 **assessment**;

- 1964 e) **destruction of expired or compromised private keys in a manner that**
1965 **prohibits their retrieval, or their archival in a manner that prohibits their**
1966 **reuse;**
1967 f) **applicable cryptographic module security requirements, quoting FIPS 140-2**
1968 **[FIPS140-2] or equivalent, as established by a recognized national technical**
1969 **authority.**
1970

1971 **3.7.1.2.3 Storage of Long-term Secrets**

1972 AL2_CM_STS#010 Withdrawn

1973 Withdrawn (AL2_CO_SCO#020 (a) & (b) enforce this requirement).

1974

1975 **3.7.1.2.4 Security-Relevant Event (Audit) Records**

1976 **3.7.1.2.5 No stipulation**

1977 AL2_CM_OPN#010 Withdrawn

1978 Withdrawn – see AL2_CM_RNR#010.

1979

1980

1981 **3.7.1.3 Assurance Level 3**

1982 These criteria apply to one-time password devices and soft crypto applications protected
1983 by passwords or biometric controls, as well as cryptographically-signed SAML
1984 assertions.

1985 **3.7.1.3.1 Credential Policy and Practices**

1986 These criteria apply to the policy and practices under which credentials are managed.

1987 An enterprise and its specified service must:

1988 AL3_CM_CPP#010 Credential Policy and Practice Statement

1989 Include in its Service Definition a full description of the policy against which it issues
1990 credentials and the corresponding practices it applies in their issuance. At a minimum,
1991 the Credential Policy and Practice Statement must specify:

- 1992 a) if applicable, any OIDs related to the Credential Policy and Practice Statement;
1993 b) how users may subscribe to the service/apply for credentials and how the users'
1994 credentials will be delivered to them;
1995 c) how subscribers acknowledge receipt of tokens and credentials and what
1996 obligations they accept in so doing (including whether they consent to publication
1997 of their details in credential status directories);
1998 d) how credentials may be renewed, modified, revoked, and suspended, including
1999 how requestors are authenticated or their identity proven;
2000 e) what actions a subscriber must take to terminate a subscription;
2001 f) how records are retained and archived.

2002 AL3_CM_CPP#020 No stipulation

2003 AL3_CM_CPP#030 Management Authority

2004 Have a nominated or appointed high-level management body with authority and
2005 responsibility for approving the Certificate Policy and Certification Practice Statement,
2006 including ultimate responsibility for their proper implementation.

2007

2008 **3.7.1.3.2 Security Controls**

2009 AL3_CM_CTR#010 No stipulation

2010 AL3_CM_CTR#020 Protocol threat risk assessment and controls

2011 Account for at least the following protocol threats in its risk assessment and apply
2012 controls that reduce them to acceptable risk levels:

- 2013 a) password guessing, such that the resistance to an on-line guessing attack against a
2014 selected user/password is at least 1 in 2^{14} (**16,384**);
2015 b) message replay, showing that it is impractical;
2016 c) eavesdropping, showing that it is impractical;
2017 **d) relying party (verifier) impersonation, showing that it is impractical;**
2018 **e) man-in-the-middle attack, showing that it is impractical.**

2019 **The above list shall not be considered to be a complete list of threats to be addressed**
2020 **by the risk assessment.**

2021 AL3_CM_CTR#025 Permitted authentication protocols

2022 For non-PKI credentials, permit only the following authentication protocols:

- 2023 a) tunneled password;
2024 b) zero knowledge-base password;
2025 c) SAML assertions.

2026 AL3_CM_CTR#030 System threat risk assessment and controls

2027 Account for the following system threats in its risk assessment and apply controls that
2028 reduce them to acceptable risk levels:

- 2029 a) the introduction of malicious code;
2030 b) compromised authentication arising from insider action;
2031 c) out-of-band attacks by both users and system operators (e.g., shoulder-surfing);
2032 d) spoofing of system elements/applications;
2033 e) malfeasance on the part of subscribers and subjects;
2034 f) intrusions leading to information theft.

2035 The above list shall not be considered to be a complete list of threats to be addressed by
2036 the risk assessment.

2037 AL3_CM_CTR#040 Specified Service's Key Management

2038 Specify and observe procedures and processes for the generation, storage, and destruction
2039 of its own cryptographic keys used for securing the specific service's assertions and other
2040 publicized information. At a minimum, these should address:

- 2041 a) the physical security of the environment;
2042 b) access control procedures limiting access to the minimum number of authorized
2043 personnel;
2044 c) public-key publication mechanisms;
2045 d) application of controls deemed necessary as a result of the service's risk
2046 assessment;
2047 e) destruction of expired or compromised private keys in a manner that prohibits
2048 their retrieval or their archival in a manner that prohibits their reuse;

2049 f) applicable cryptographic module security requirements, quoting FIPS 140-2
2050 [FIPS140-2] or equivalent, as established by a recognized national technical
2051 authority.
2052

2053 **3.7.1.3.3 Storage of Long-term Secrets**

2054 An enterprise and its specified service must:

2055 AL3_CM_STS#010 Withdrawn

2056 Withdrawn (AL3_CO_SCO#020 (a) & (b) enforce this requirement).

2057 AL3_CM_STS#020 Stored Secret Encryption

2058 Encrypt such shared secret files so that:

- 2059 a) the encryption key for the shared secret file is encrypted under a key held in a
2060 FIPS 140-2 [FIPS140-2] Level 2 or higher validated hardware or software
2061 cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module, or
2062 equivalent, as established by a recognized national technical authority;
- 2063 b) the shared secret file is decrypted only as immediately required for an
2064 authentication operation;
- 2065 c) shared secrets are protected as a key within the boundary of a FIPS 140-2 Level 2
2066 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or
2067 4 cryptographic module and are not exported from the module in plain text, or
2068 equivalent, as established by a recognized national technical authority;
- 2069 d) shared secrets are split by an "*n from m*" cryptographic secret sharing method.
2070

2071 **3.7.1.3.4 Security-relevant Event (Audit) Records**

2072 These criteria describe the need to provide an auditable log of all events that are pertinent
2073 to the correct and secure operation of the service. The common organizational criteria
2074 applying to provision of an auditable log of all security-related events pertinent to the
2075 correct and secure operation of the service must also be considered carefully. These
2076 criteria carry implications for credential management operations.

2077 In the specific context of a certificate management service, an enterprise and its specified
2078 service must:

2079 AL3_CM_SER#010 Security event logs

2080 Ensure that such audit records include:

- 2081 a) the identity of the point of registration (irrespective of whether internal or
2082 outsourced);

- 2083 b) generation of the subscriber's keys or the evidence that the subscriber was in
2084 possession of both parts of their own key-pair;
2085 c) generation of the subscriber's certificate;
2086 d) dissemination of the subscriber's certificate;
2087 e) any revocation or suspension associated with the subscriber's certificate.
2088

2089 **3.7.1.3.5 Subject options**

2090 AL3_CM_OPN#010 Changeable PIN/Password

2091 Withdrawn – see AL3_CM_RNR#010.

2092

2093 **3.7.1.4 Assurance Level 4**

2094 These criteria apply exclusively to cryptographic technology deployed through a Public
2095 Key Infrastructure. This technology requires hardware tokens protected by password or
2096 biometric controls. No other forms of credential are permitted at AL4.

2097 **3.7.1.4.1 Certification Policy and Practices**

2098 These criteria apply to the policy and practices under which certificates are managed.

2099 An enterprise and its specified service must:

2100 AL4_CM_CPP#010 No stipulation

2101 AL4_CM_CPP#020 Certificate Policy/Certification Practice Statement

2102 **Include in its Service Definition its full Certificate Policy and the corresponding**
2103 **Certification and Practice Statement. The Certificate Policy and Certification**
2104 **Practice Statement must conform to IETF RFC 3647 (2003-11) [RFC 3647] in their**
2105 **content and scope or be demonstrably consistent with the content or scope of that**
2106 **RFC. At a minimum, the Certificate Policy must specify:**

- 2107 a) **applicable OIDs for each certificate type issued;**
2108 b) **how users may subscribe to the service/apply for certificates, and how**
2109 **certificates will be issued to them;**
2110 c) **if users present their own keys, how they will be required to demonstrate**
2111 **possession of the private key;**
2112 d) **if users' keys are generated for them, how the private keys will be delivered**
2113 **to them;**
2114 e) **how subscribers acknowledge receipt of tokens and credentials and what**
2115 **obligations they accept in so doing (including whether they consent to**
2116 **publication of their details in certificate status directories);**
2117 f) **how certificates may be renewed, re-keyed, modified, revoked, and**
2118 **suspended, including how requestors are authenticated or their identity**
2119 **proven;**
2120 g) **what actions a subscriber must take to terminate their subscription.**

2121 AL4_CM_CPP#030 Management Authority

2122 Have a nominated or appointed high-level management body with authority and
2123 responsibility for approving the Certificate Policy and Certification Practice Statement,
2124 including ultimate responsibility for their proper implementation.

2125

2126 **3.7.1.4.2 Security Controls**

2127 An enterprise and its specified service must:

- 2128 AL4_CM_CTR#010 No stipulation
- 2129 AL4_CM_CTR#020 Protocol threat risk assessment and controls
- 2130 Account for at least the following protocol threats in its risk assessment and apply
2131 controls that reduce them to acceptable risk levels:
- 2132 a) password guessing, showing that there is sufficient entropy;
2133 b) message replay, showing that it is impractical;
2134 c) eavesdropping, showing that it is impractical;
2135 d) relying party (verifier) impersonation, showing that it is impractical;
2136 e) man-in-the-middle attack, showing that it is impractical;
2137 **f) session hijacking, showing that it is impractical.**
- 2138 The above list shall not be considered to be a complete list of threats to be addressed by
2139 the risk assessment.
- 2140 AL4_CM_CTR#025 No stipulation
- 2141 AL4_CM_CTR#030 System threat risk assessment and controls
- 2142 Account for the following system threats in its risk assessment and apply controls that
2143 reduce them to acceptable risk levels:
- 2144 a) the introduction of malicious code;
2145 b) compromised authentication arising from insider action;
2146 c) out-of-band attacks by both users and system operators (e.g., shoulder-surfing);
2147 d) spoofing of system elements/applications;
2148 e) malfeasance on the part of subscribers and subjects;
2149 f) intrusions leading to information theft.
- 2150 The above list shall not be considered to be a complete list of threats to be addressed by
2151 the risk assessment.
- 2152 AL4_CM_CTR#040 Specified Service's Key Management
- 2153 Specify and observe procedures and processes for the generation, storage, and destruction
2154 of its own cryptographic keys used for securing the specific service's assertions and other
2155 publicized information. At a minimum, these should address:
- 2156 a) the physical security of the environment;
2157 b) access control procedures limiting access to the minimum number of authorized
2158 personnel;
2159 c) public-key publication mechanisms;
2160 d) application of controls deemed necessary as a result of the service's risk
2161 assessment;

- 2162 e) destruction of expired or compromised private keys in a manner that prohibits
2163 their retrieval, or their archival in a manner which prohibits their reuse;
2164 f) applicable cryptographic module security requirements, quoting FIPS 140-2
2165 [FIPS140-2] or equivalent, as established by a recognized national technical
2166 authority.
2167

2168 **3.7.1.4.3 Storage of Long-term Secrets**

2169 The enterprise and its specified service must meet the following criteria:

2170 AL4_CM_STS#010 Stored Secrets

- 2171 a) Withdrawn (AL4_CO_SCO#020 (a) & (b) enforce this requirement)
2172 b) **apply discretionary access controls that limit access to trusted administrators**
2173 **and to those applications that require access.**

2174 AL4_CM_STS#020 Stored Secret Encryption

2175 Encrypt such [omitted] secret files so that:

- 2176 a) the encryption key for the [omitted] secret file is encrypted under a key held in a
2177 FIPS 140-2 [FIPS140-2] Level 2 or higher validated hardware cryptographic
2178 module or any FIPS 140-2 Level 3 or 4 cryptographic module, or equivalent, as
2179 established by a recognized national technical authority;
2180 b) the [omitted] secret file is decrypted only as immediately required for a key
2181 recovery operation;
2182 c) [omitted] secrets are protected as a key within the boundary of a FIPS 140-2
2183 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2
2184 Level 3 or 4 cryptographic module and are not exported from the module in
2185 plaintext, or equivalent, as established by a recognized national technical
2186 authority;
2187 d) escrowed secrets are split by an "n from m" cryptographic secret **storing** method.
2188

2189 **3.7.1.4.4 Security-relevant Event (Audit) Records**

2190 These criteria describe the need to provide an auditable log of all events that are pertinent
2191 to the correct and secure operation of the service. The common organizational criteria
2192 relating to the recording of all security-related events must also be considered carefully.
2193 These criteria carry implications for credential management operations.

2194 In the specific context of a certificate management service, an enterprise and its specified
2195 service must:

- 2196 AL4_CM_SER#010 Security event logs
- 2197 Ensure that such audit records include:
- 2198 a) the identity of the point of registration (irrespective of whether internal or
2199 outsourced);
- 2200 b) generation of the subscriber's keys or evidence that the subscriber was in
2201 possession of both parts of the key-pair;
- 2202 c) generation of the subscriber's certificate;
- 2203 d) dissemination of the subscriber's certificate;
- 2204 e) any revocation or suspension associated with the subscriber's credential.
2205

2206 **3.7.1.4.5 Subject Options**

- 2207 AL4_CM_OPN#010 Changeable PIN/Password
- 2208 Withdrawn – see AL4_CM_RNR#010.
- 2209

2210 **3.7.2 Part B - Credential Issuing**

2211 These criteria apply to the verification of the identity of the subject of a credential and
2212 with token strength and credential delivery mechanisms. They address requirements
2213 levied by the use of various technologies to achieve the appropriate AL⁶. These criteria
2214 include by reference all applicable criteria in Section 3.6.

2215 **3.7.2.1 Assurance Level 1**

2216 **3.7.2.1.1 Identity Proofing**

2217 These criteria determine how the enterprise shows compliance with the criteria for
2218 fulfilling identity proofing functions.

2219 The enterprise and its specified service must:

2220 AL1_CM_IDP#010 Self-managed Identity Proofing

2221 If the enterprise assumes direct responsibility for identity proofing functions, show, by
2222 direct inclusion, compliance with all applicable identity proofing service assessment
2223 criteria⁷ ([ID-SAC]) for AL1 or higher.

2224 AL1_CM_IDP#020 Kantara-Recognized outsourced service

2225 If the enterprise outsources responsibility for identity proofing functions and uses a
2226 service already Kantara-Recognized, show that the service in question has been approved
2227 at AL1 or higher.

2228 AL1_CM_IDP#030 Non-recognized outsourced service

2229 If the enterprise outsources responsibility for identity proofing functions, ensure that each
2230 provider of such a service demonstrates compliance with all applicable identity proofing
2231 service assessment criteria for AL1 or higher, and that the enterprise, itself, has in place
2232 controls to ensure the continued fulfillment of those criteria by the provider to which the
2233 functions have been outsourced.

2234 AL1_CM_IDP#040 Revision to subscriber information

2235 Provide a means for subscribers to amend their stored information after registration.

2236

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.

- 2237 **3.7.2.1.2 Credential Creation**
- 2238 These criteria address the requirements for creation of credentials that can only be used at
2239 AL1. Any credentials/tokens that comply with the criteria stipulated for AL2 and higher
2240 are acceptable at AL1.
- 2241 An enterprise and its specified service must:
- 2242 AL1_CM_CRN#010 Authenticated Request
- 2243 Only accept a request to generate a credential and bind it to an identity if the source of the
2244 request can be authenticated as being authorized to perform identity proofing at AL1 or
2245 higher.
- 2246 AL1_CM_CRN#020 No stipulation
- 2247 AL1_CM_CRN#030 Credential uniqueness
- 2248 Allow the subscriber to select a credential (e.g., UserID) that is verified to be unique
2249 within the specified service’s community and assigned uniquely to a single identity
2250 subject.
- 2251 **3.7.2.1.3 Not used**
- 2252 **3.7.2.1.4 Not used**
- 2253
- 2254

2255 **3.7.2.2 Assurance Level 2**

2256 **3.7.2.2.1 Identity Proofing**

2257 These criteria determine how the enterprise shows compliance with the criteria for
2258 fulfilling identity proofing functions.

2259 The enterprise and its specified service must:

2260 AL2_CM_IDP#010 Self-managed Identity Proofing

2261 If the enterprise assumes direct responsibility for identity proofing functions, show, by
2262 direct inclusion, compliance with all applicable identity proofing service assessment
2263 criteria ([ID-SAC]) for AL2 or higher.

2264 AL2_CM_IDP#020 Kantara-Recognized outsourced service

2265 If the enterprise outsources responsibility for identity proofing functions and uses a
2266 service already Kantara-Recognized, show that the service in question has been approved
2267 at AL2 or higher **and that its approval has at least six months of remaining validity.**

2268 AL2_CM_IDP#030 Non- Kantara-Recognized outsourced service

2269 If the enterprise outsources responsibility for identity proofing functions, ensure that each
2270 provider of such a service demonstrates compliance with all applicable identity proofing
2271 service assessment criteria for AL2 or higher, and that the enterprise, itself, has in place
2272 controls to ensure the continued fulfillment of those criteria by the provider to which the
2273 functions have been outsourced.

2274 AL2_CM_IDP#040 Revision to subscriber information

2275 Provide a means for subscribers to **securely** amend their stored information after
2276 registration, **either by re-proving their identity, as in the initial registration process,**
2277 **or by using their credentials to authenticate their revision.**

2278

2279 **3.7.2.2.2 Credential Creation**

2280 These criteria define the requirements for creation of credentials whose highest use is at
2281 AL2. Credentials/tokens that comply with the criteria stipulated at AL3 and higher are
2282 also acceptable at AL2 and below.

2283 Note, however, that a token and credential required by a higher AL but created according
2284 to these criteria may not necessarily provide that higher level of assurance for the claimed
2285 identity of the subscriber. Authentication can only be provided at the assurance level at
2286 which the identity is proven.

- 2287 An enterprise and its specified service must:
- 2288 AL2_CM_CRN#010 Authenticated Request
- 2289 Only accept a request to generate a credential and bind it to an identity if the source of the
2290 request can be authenticated, **i.e., Registration Authority, as being authorized to**
2291 **perform identity proofing at AL2 or higher.**
- 2292 AL2_CM_CRN#020 Unique identity
- 2293 **Ensure that the identity which relates to a specific applicant is unique within the**
2294 **specified service, including identities previously used and that are now cancelled,**
2295 **other than its re-assignment to the same applicant.**
- 2296 Guidance: This requirement is intended to prevent identities that may exist in a Relying
2297 Party’s access control list from possibly representing a different physical person.
- 2298 AL2_CM_CRN#030 Credential uniqueness
- 2299 Allow the subscriber to select a credential (e.g., UserID) that is verified to be unique
2300 within the specified service’s community and assigned uniquely to a single identity
2301 subject.
- 2302 AL2_CM_CRN#035 Convey credential
- 2303 **Be capable of conveying the unique identity information associated with a credential**
2304 **to Verifiers and Relying Parties.**
- 2305 AL2_CM_CRN#040 Password strength
- 2306 **Only allow passwords that, over the life of the password, have resistance to an on-**
2307 **line guessing attack against a selected user/password of at least 1 in 2^{14} (16,384),**
2308 **accounting for state-of-the-art attack strategies, and at least 10 bits of min-entropy⁸.**
- 2309 AL2_CM_CRN#050 One-time password strength
- 2310 **Only allow password tokens that have a resistance to online guessing attack against**
2311 **a selected user/password of at least 1 in 2^{14} (16,384), accounting for state-of-the-art**
2312 **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.

- 2313 AL2_CM_CRN#060 Software cryptographic token strength
- 2314 **Ensure that software cryptographic keys stored on general-purpose devices:**
- 2315 a) **are protected by a key and cryptographic protocol that are evaluated against**
- 2316 **FIPS 140-2 [[FIPS140-2](#)] Level 2, or equivalent, as established by a recognized**
- 2317 **national technical authority;**
- 2318 b) **require password or biometric activation by the subscriber or employ a**
- 2319 **password protocol when being used for authentication.**
- 2320 AL2_CM_CRN#070 Hardware token strength
- 2321 **Ensure that hardware tokens used to store cryptographic keys:**
- 2322 a) **employ a cryptographic module that is evaluated against FIPS 140-2**
- 2323 **[[FIPS140-2](#)] Level 1 or higher, or equivalent, as established by a recognized**
- 2324 **national technical authority;**
- 2325 b) **require password or biometric activation by the subscriber or also employ a**
- 2326 **password when being used for authentication.**
- 2327 AL2_CM_CRN#080 No stipulation
- 2328 AL2_CM_CRN#090 Nature of subject
- 2329 **Record the nature of the subject of the credential (which must correspond to the**
- 2330 **manner of identity proofing performed), i.e., physical person, a named person acting**
- 2331 **on behalf of a corporation or other legal entity, corporation or legal entity, or**
- 2332 **corporate machine entity, in a manner that can be unequivocally associated with the**
- 2333 **credential and the identity that it asserts. If the credential is based upon a**
- 2334 **pseudonym this must be indicated in the credential.**
- 2335 **3.7.2.2.3 Subject Key Pair Generation**
- 2336 No stipulation.
- 2337 **3.7.2.2.4 Credential Delivery**
- 2338 An enterprise and its specified service must:
- 2339 AL2_CM_CRD#010 Notify Subject of Credential Issuance
- 2340 **Notify the subject of the credential's issuance and, if necessary, confirm the**
- 2341 **Subject's contact information by:**
- 2342 a) **sending notice to the address of record confirmed during identity proofing**
- 2343 **or;**
- 2344 b) **issuing the credential(s) in a manner that confirms the address of record**
- 2345 **supplied by the applicant during identity proofing or;**

2346 c) **issuing the credential(s) in a manner that confirms the ability of the applicant**
2347 **to receive telephone communications at a fixed-line telephone number or**
2348 **postal address supplied by the applicant during identity proofing.**

2349 AL2_CM_CRD#015 Confirm Applicant's identity (in person)

2350 **Prior to delivering the credential, require the Applicant to identify themselves in**
2351 **person in any new electronic transaction (beyond the first transaction or encounter)**
2352 **by either:**

2353 (a) **using a secret which was established during a prior transaction or**
2354 **encounter, or sent to the Applicant's phone number, email address, or**
2355 **physical address of record, or;**

2356 (b) **through the use of a biometric that was recorded during a prior**
2357 **encounter.**

2358 AL2_CM_CRD#016 Confirm Applicant's identity (remotely)

2359 **Prior to delivering the credential, require the Applicant to identify themselves in any**
2360 **new electronic transaction (beyond the first transaction or encounter) by presenting**
2361 **a temporary secret which was established during a prior transaction or encounter,**
2362 **or sent to the Applicant's phone number, email address, or physical address of**
2363 **record.**

2364
2365

2366 **3.7.2.3 Assurance Level 3**

2367 **3.7.2.3.1 Identity Proofing**

2368 These criteria in this section determine how the enterprise shows compliance with the
2369 criteria for fulfilling identity proofing functions.

2370 The enterprise and its specified service must:

2371 AL3_CM_IDP#010 Self-managed Identity Proofing

2372 If the enterprise assumes direct responsibility for identity proofing functions, show, by
2373 direct inclusion, compliance with all applicable identity proofing service assessment
2374 criteria for **AL3 or AL4**.

2375 AL3_CM_IDP#020 Kantara-Recognized outsourced service

2376 If the enterprise outsources responsibility for identity proofing functions and uses a
2377 service already Kantara-Recognized, show that the service in question has been certified
2378 at **AL3 or AL4** and that its approval has at least six months of remaining validity.

2379 AL3_CM_IDP#030 Non- Kantara-Recognized outsourced service

2380 **Not use any non- Kantara-Recognized services for identity proofing unless they can**
2381 **be demonstrated to have satisfied equivalently rigorous requirements established by**
2382 **another scheme recognized by IAWG.**

2383 AL3_CM_IDP#040 Revision to subscriber information

2384 Provide a means for subscribers to securely amend their stored information after
2385 registration, either by re-proving their identity as in the initial registration process or by
2386 using their credentials to authenticate their revision. **Successful revision must, where**
2387 **necessary, instigate the re-issuance of the credential.**

2388

2389 **3.7.2.3.2 Credential Creation**

2390 These criteria define the requirements for creation of credentials whose highest use is
2391 AL3. Any credentials/tokens that comply with the criteria stipulated at AL4 are also
2392 acceptable at AL3 and below.

2393 Note, however, that a token and credential type required by a higher AL but created
2394 according to these criteria may not necessarily provide that higher level of assurance for
2395 the claimed identity of the subscriber. Authentication can only be provided at the
2396 assurance level at which the identity is proven.

2397 An enterprise and its specified service must:

- 2398 AL3_CM_CRN#010 Authenticated Request
- 2399 Only accept a request to generate a credential and bind it to an identity if the source of the
2400 request, i.e., Registration Authority, can be authenticated as being authorized to perform
2401 identity proofing at AL3 or higher.
- 2402 AL3_CM_CRN#020 Unique identity
- 2403 Ensure that the identity which relates to a specific applicant is unique within the specified
2404 service, including identities previously used and that are now cancelled other than its re-
2405 assignment to the same applicant.
- 2406 **Guidance:** This requirement is intended to prevent identities that may exist in a Relying
2407 Party's access control lists from possibly representing a different physical person.
- 2408
- 2409 AL3_CM_CRN#030 Credential uniqueness
- 2410 Allow the subscriber to select a credential (e.g., UserID) that is verified to be unique
2411 within the specified service's community and assigned uniquely to a single identity
2412 subject.
- 2413 AL3_CM_CRN#035 Convey credential
- 2414 Be capable of conveying the unique identity information associated with a credential to
2415 Verifiers and Relying Parties.
- 2416 AL3_CM_CRN#040 PIN/Password strength
- 2417 **Not use PIN/password tokens.**
- 2418 AL3_CM_CRN#050 One-time password strength
- 2419 Only allow one-time password tokens that:
- 2420 a) **depend on a symmetric key stored on a personal hardware device evaluated**
2421 **against FIPS 140-2 [FIPS140-2] Level 1 or higher, or equivalent, as**
2422 **established by a recognized national technical authority;**
- 2423 b) **permit at least 10⁶ possible password values;**
- 2424 c) **require password or biometric activation by the subscriber.**
- 2425 AL3_CM_CRN#060 Software cryptographic token strength
- 2426 Ensure that software cryptographic keys stored on general-purpose devices:

- 2427 a) are protected by a key and cryptographic protocol that are evaluated against
2428 FIPS 14-2 [FIPS140-2] Level 2, or equivalent, as established by a recognized
2429 national technical authority;
2430 b) require password or biometric activation by the subscriber or employ a password
2431 protocol when being used for authentication.

2432 AL3_CM_CRN#070 Hardware token strength

2433 Ensure that hardware tokens used to store cryptographic keys:

- 2434 a) employ a cryptographic module that is evaluated against FIPS 140-2 [FIPS140-2]
2435 Level 1 or higher, or equivalent, as established by a recognized national technical
2436 authority;
2437 b) require password or biometric activation by the subscriber or also employ a
2438 password when being used for authentication.

2439 AL3_CM_CRN#080 Binding of key

2440 **If the specified service generates the subject's key pair, that the key generation**
2441 **process securely and uniquely binds that process to the certificate generation and**
2442 **maintains at all times the secrecy of the private key, until it is accepted by the**
2443 **subject.**

2444 AL3_CM_CRN#090 Nature of subject

2445 Record the nature of the subject of the credential (which must correspond to the manner
2446 of identity proofing performed), i.e., private person, a named person acting on behalf of a
2447 corporation or other legal entity, corporation or legal entity, or corporate machine entity,
2448 in a manner that can be unequivocally associated with the credential and the identity that
2449 it asserts. [Omitted]

2450

2451 **3.7.2.3.3 Subject Key Pair Generation**

2452 An enterprise and its specified service must:

2453 AL3_CM_SKP#010 Key generation by Specified Service

2454 **If the specified service generates the subject's keys:**

- 2455 a) use a FIPS 140-2 [FIPS140-2] compliant algorithm, or equivalent, as
2456 established by a recognized national technical authority, that is recognized as
2457 being fit for the purposes of the service;
2458 b) only create keys of a key length and for use with a FIPS 140-2 [FIPS140-2]
2459 compliant public key algorithm, or equivalent, as established by a recognized

- 2460 **national technical authority, recognized as being fit for the purposes of the**
2461 **service;**
2462 c) **generate and store the keys securely until delivery to and acceptance by the**
2463 **subject;**
2464 d) **deliver the subject’s private key in a manner that ensures that the privacy of**
2465 **the key is not compromised and only the subject has access to the private**
2466 **key.**

2467 AL3_CM_SKP#020 Key generation by Subject

2468 **If the subject generates and presents its own keys, obtain the subject’s written**
2469 **confirmation that it has:**

- 2470 a) **used a FIPS 140-2 [FIPS140-2] compliant algorithm, or equivalent, as**
2471 **established by a recognized national technical authority, that is recognized as**
2472 **being fit for the purposes of the service;**
2473 b) **created keys of a key length and for use with a FIPS 140-2 [FIPS140-2]**
2474 **compliant public key algorithm, or equivalent, as established by a recognized**
2475 **national technical authority, recognized as being fit for the purposes of the**
2476 **service.**
2477

2478 **3.7.2.3.4 Credential Delivery**

2479 An enterprise and its specified service must:

2480 AL3_CM_CRD#010, Notify Subject of Credential Issuance

2481 Notify the subject of the credential’s issuance and, if necessary, confirm Subject’s contact
2482 information by:

- 2483 a) **sending notice to the address of record confirmed during identity proofing, and**
2484 **either:**
2485 i) **issuing the credential(s) in a manner that confirms the address of**
2486 **record supplied by the applicant during identity proofing, or;**
2487 ii) **issuing the credential(s) in a manner that confirms the ability of the**
2488 **applicant to receive telephone communications at a phone number**
2489 **supplied by the applicant during identity proofing, while recording**
2490 **the applicant’s voice.**

2491 AL3_CM_CRD#020 Subject’s acknowledgement

2492 **Receive acknowledgement of receipt of the credential before it is activated and its**
2493 **directory status record is published (and thereby the subscription becomes active or**
2494 **re-activated, depending upon the circumstances of issue).**

2495

2496

2497 **3.7.2.4 Assurance Level 4**

2498 **3.7.2.4.1 Identity Proofing**

2499 These criteria determine how the enterprise shows compliance with the criteria for
2500 fulfilling identity proofing functions.

2501 An enterprise and its specified service must:

2502 AL4_CM_IDP#010 Self-managed Identity Proofing

2503 If the enterprise assumes direct responsibility for identity proofing functions, show, by
2504 direct inclusion, compliance with all applicable identity proofing service assessment
2505 criteria for [omitted] AL4.

2506 AL4_CM_IDP#020 Kantara-Recognized outsourced service

2507 If the enterprise outsources responsibility for identity proofing functions and uses a
2508 service already Kantara-Recognized, show that the service in question has been certified
2509 at [omitted] AL4 and that its approval has at least **12** months of remaining validity.

2510 AL4_CM_IDP#030 Non- Kantara-Recognized outsourced service

2511 Not use any non- Kantara-Recognized outsourced services for identity proofing unless
2512 they can be demonstrated to have satisfied equivalently rigorous requirements established
2513 by another scheme recognized by IAWG.

2514 AL4_CM_IDP#040 Revision to subscriber information

2515 Provide a means for subscribers to securely amend their stored information after
2516 registration, either by re-proving their identity as in the initial registration process or by
2517 using their credentials to authenticate their revision. Successful revision must, where
2518 necessary, instigate the re-issuance of the credential.

2519

2520 **3.7.2.4.2 Credential Creation**

2521 These criteria define the requirements for creation of credentials whose highest use is
2522 AL4.

2523 Note, however, that a token and credential created according to these criteria may not
2524 necessarily provide that level of assurance for the claimed identity of the subscriber.
2525 Authentication can only be provided at the assurance level at which the identity is proven.

2526 An enterprise and its specified service must:

- 2527 AL4_CM_CRN#010 Authenticated Request
- 2528 Only accept a request to generate a credential and bind it to an identity if the source of the
2529 request, i.e., Registration Authority, can be authenticated as being authorized to perform
2530 identity proofing at AL4.
- 2531 AL4_CM_CRN#020 Unique identity
- 2532 Ensure that the identity which relates to a specific applicant is unique within the specified
2533 service, including identities previously used and that are now cancelled, other than its re-
2534 assignment to the same applicant.
- 2535 **Guidance:** This requirement is intended to prevent identities that may exist in a Relying
2536 Party's access control lists from possibly representing a different physical person.
- 2537 AL4_CM_CRN#030 Credential uniqueness
- 2538 Allow the subscriber to select a credential (e.g., UserID) that is verified to be unique
2539 within the specified service's community and assigned uniquely to a single identity
2540 subject.
- 2541 AL4_CM_CRN#035 Convey credential
- 2542 Be capable of conveying the unique identity information associated with a credential to
2543 Verifiers and Relying Parties.
- 2544 AL4_CM_CRN#040 PIN/Password strength
- 2545 *Not* use PIN/password tokens.
- 2546 AL4_CM_CRN#050 One-time password strength
- 2547 **Not use one-time password tokens.**
- 2548 AL4_CM_CRN#060 Software cryptographic token strength
- 2549 **Not use software cryptographic tokens.**
- 2550 AL4_CM_CRN#070 Hardware token strength
- 2551 Ensure that hardware tokens used to store cryptographic keys:
- 2552 a) employ a cryptographic module that is validated against FIPS 140-2 [[FIPS140-2](#)]
2553 Level 2 or higher, or equivalent, as determined by a recognized national technical
2554 authority;

- 2555 b) are evaluated against FIPS 140-2 Level 3 or higher, or equivalent, as
2556 determined by a recognized national technical authority, for their physical
2557 security;
2558 c) require password or biometric activation by the subscriber [omitted].

2559 AL4_CM_CRN#080 Binding of key

2560 If the specified service generates the subject's key pair, that the key generation process
2561 securely and uniquely binds that process to the certificate generation and maintains at all
2562 times the secrecy of the private key, until it is accepted by the subject.

2563 AL4_CM_CRN#090 Nature of subject

2564 Record the nature of the subject of the credential [omitted], i.e., private person, a named
2565 person acting on behalf of a corporation or other legal entity, corporation or legal entity,
2566 or corporate machine entity, in a manner that can be unequivocally associated with the
2567 credential and the identity that it asserts.

2568

2569 3.7.2.4.3 Subject Key Pair Generation

2570 An enterprise and its specified service must:

2571 AL4_CM_SKP#010 Key generation by Specified Service

2572 If the specified service generates the subject's keys:

- 2573 a) use a FIPS 140-2 [FIPS140-2] compliant algorithm, or equivalent, as established
2574 by a recognized national technical authority, that is recognized as being fit for the
2575 purposes of the service;
2576 b) only create keys of a key length and for use with a FIPS 140-2 [FIPS140-2]
2577 compliant public key algorithm, or equivalent, as established by a recognized
2578 national technical authority, recognized as being fit for the purposes of the
2579 service;
2580 c) generate and store the keys securely until delivery to and acceptance by the
2581 subject;
2582 d) deliver the subject's private key in a manner that ensures that the privacy of the
2583 key is not compromised and only the subject has access to the private key.

2584 AL4_CM_SKP#020 Key generation by Subject

2585 If the subject generates and presents its own keys, obtain the subject's written
2586 confirmation that it has:

- 2587 a) used a FIPS 140-2 [FIPS140-2] compliant algorithm, or equivalent, as established
2588 by a recognized national technical authority, that is recognized as being fit for the
2589 purposes of the service;
2590 b) created keys of a key length and for use with a FIPS 140-2 [FIPS140-2] compliant
2591 public key algorithm, or equivalent, as established by a recognized national
2592 technical authority, recognized as being fit for the purposes of the service.
2593

2594 **3.7.2.4.4 Credential Delivery**

2595 An enterprise and its specified service must:

2596 AL4_CM_CRD#010 Notify Subject of Credential Issuance

2597 Notify the subject of the credential's issuance and, if necessary, confirm Subject's contact
2598 information by:

- 2599 a) sending notice to the address of record confirmed during identity proofing;
2600 b) **unless the subject presented with a private key, issuing the hardware token**
2601 **to the subject in a manner that confirms the address of record supplied by**
2602 **the applicant during identity proofing;**
2603 c) **issuing the certificate to the subject over a separate channel in a manner that**
2604 **confirms either the address of record or the email address supplied by the**
2605 **applicant during identity proofing.**

2606 AL4_CM_CRD#020 Subject's acknowledgement

2607 Receive acknowledgement of receipt of the **hardware token** before it is activated and **the**
2608 **corresponding certificate and** its directory status record are published (and thereby the
2609 subscription becomes active or re-activated, depending upon the circumstances of issue).

2610

2611 **3.7.3 Part C - Credential Renewal and Re-issuing**

2612 These criteria apply to the renewal and re-issuing of credentials. They address
2613 requirements levied by the use of various technologies to achieve the appropriate AL⁹.
2614 These criteria include by reference all applicable criteria in Section 3.6 and the renewal
2615 and re-issuing processes shall comply in all practical senses with the applicable criteria
2616 set forth in Part B of this section.

2617

2618 **3.7.3.1 Assurance Level 1**

2619 **3.7.3.1.1 Renewal/Re-issuance Procedures**

2620 These criteria address general renewal and re-issuance functions, to be exercised as
2621 specific controls in these circumstances while continuing to observe the general
2622 requirements established for initial credential issuance.

2623 An enterprise and its specified service must:

2624 AL1_CM_RNR#010 Changeable PIN/Password

2625 Permit subjects to change their PINs/passwords.

2626

2627

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

2628 **3.7.3.2 Assurance Level 2**

2629 **3.7.3.2.1 Renewal/Re-issuance Procedures**

2630 These criteria address general renewal and re-issuance functions, to be exercised as
2631 specific controls in these circumstances while continuing to observe the general
2632 requirements established for initial credential issuance.

2633 An enterprise and its specified service must:

2634 AL2_CM_RNR#010 Changeable PIN/Password

2635 Permit subjects to change their [omitted] passwords, **but employ reasonable practices**
2636 **with respect to password resets and repeated password failures.**

2637 AL2_CM_RNR#020 Proof-of-possession on Renewal/Re-issuance

2638 **Subjects wishing to change their passwords must demonstrate that they are in**
2639 **possession of the unexpired current token prior to the CSP proceeding to renew or**
2640 **re-issue it.**

2641 AL2_CM_RNR#030 Renewal/Re-issuance limitations

2642 **a. not renew but may re-issue Passwords;**

2643 **b. neither renew nor re-issue expired tokens;**

2644 **c. conduct all renewal / re-issuance interactions with the Subject over a**
2645 **protected channel such as SSL/TLS.**

2646 **Guidance:** Renewal is considered as an extension of usability, whereas re-issuance
2647 requires a change.

2648

2649

2650 **3.7.3.3 Assurance Level 3**

2651 **3.7.3.3.1 Renewal/Re-issuance Procedures**

2652 These criteria address general renewal and re-issuance functions, to be exercised as
2653 specific controls in these circumstances while continuing to observe the general
2654 requirements established for initial credential issuance.

2655 An enterprise and its specified service must:

2656 AL3_CM_RNR#010 Changeable PIN/Password

2657 Permit subjects to change **the passwords used to activate their credentials.**

2658

2659 *Further criteria may be determined after AL3 comparability assessment against Federal*
2660 *CAF and NIST SP 800-63.*

2661

2662

2663 **3.7.3.4 Assurance Level 4**

2664 **3.7.3.4.1 Renewal/Re-issuance Procedures**

2665 These criteria address general renewal and re-issuance functions, to be exercised as
2666 specific controls in these circumstances while continuing to observe the general
2667 requirements established for initial credential issuance.

2668 An enterprise and its specified service must:

2669 AL4_CM_RNR#010 Changeable PIN/Password

2670 Permit subjects to change the passwords used to activate their credentials.

2671

2672 *Further criteria may be determined after AL4 comparability assessment against Federal*
2673 *CAF and NIST SP 800-63.*

2674

2675

2676 **3.7.4 Part D - Credential Revocation**

2677 These criteria deal with credential revocation and the determination of the legitimacy of a
2678 revocation request.

2679 **3.7.4.1 Assurance Level 1**

2680 An enterprise and its specified service must:

2681 **3.7.4.1.1 Not used**

2682 **3.7.4.1.2 Not used**

2683 **3.7.4.1.3 Secure Revocation Request**

2684 This criterion applies when revocation requests between remote components of a service
2685 are made over a secured communication.

2686 An enterprise and its specified service must:

2687 AL1_CM_SRR#010 Submit Request

2688 Submit a request for revocation to the Credential Issuer service (function), using a
2689 secured network communication, if necessary.

2690

2691

2692 **3.7.4.2 Assurance Level 2**

2693 **3.7.4.2.1 Revocation Procedures**

2694 These criteria address general revocation functions, such as the processes involved and
2695 the basic requirements for publication.

2696 An enterprise and its specified service must:

2697 AL2_CM_RVP#010 Revocation procedures

2698 a) **State the conditions under which revocation of an issued credential may**
2699 **occur;**

2700 b) **State the processes by which a revocation request may be submitted;**

2701 c) **State the persons and organizations from which a revocation request will be**
2702 **accepted;**

2703 d) **State the validation steps that will be applied to ensure the validity (identity)**
2704 **of the Revocant, and;**

2705 e) **State the response time between a revocation request being accepted and the**
2706 **publication of revised certificate status.**

2707 AL2_CM_RVP#020 Secure status notification

2708 **Ensure that published credential status notification information can be relied upon**
2709 **in terms of the enterprise of its origin (i.e., its authenticity) and its correctness (i.e.,**
2710 **its integrity).**

2711 AL2_CM_RVP#030 Revocation publication

2712 **Unless the credential will expire automatically within 72 hours:**

2713 **Ensure that published credential status notification is revised within 72 hours of the**
2714 **receipt of a valid revocation request, such that any subsequent attempts to use that**
2715 **credential in an authentication shall be unsuccessful.**

2716 AL2_CM_RVP#040 Verify revocation identity

2717 **Establish that the identity for which a revocation request is received is one that was**
2718 **issued by the specified service.**

2719 AL2_CM_RVP#050 Revocation Records

2720 **Retain a record of any revocation of a credential that is related to a specific identity**
2721 **previously verified, solely in connection to the stated credential. At a minimum,**
2722 **records of revocation must include:**

- 2723 a) **the Revocant's full name;**
2724 b) **the Revocant's authority to revoke (e.g., subscriber themselves, someone**
2725 **acting with the subscriber's power of attorney, the credential issuer, law**
2726 **enforcement, or other legal due process);**
2727 c) **the Credential Issuer's identity (if not directly responsible for the identity**
2728 **proofing service);**
2729 d) **the identity associated with the credential (whether the subscriber's name or**
2730 **a pseudonym);**
2731 e) **the reason for revocation.**

2732 AL2_CM_RVP#060 Record Retention

2733 **Retain, securely, the record of the revocation process for the duration of the**
2734 **subscriber's account plus 7.5 years.**

2735

2736 **3.7.4.2.2 Verify Revocant's Identity**

2737 Revocation of a credential requires that the requestor and the nature of the request be
2738 verified as rigorously as the original identity proofing. The enterprise should not act on a
2739 request for revocation without first establishing the validity of the request (if it does not,
2740 itself, determine the need for revocation).

2741 In order to do so, the enterprise and its specified service must:

2742 AL2_CM_RVR#010 Verify revocation identity

2743 **Establish that the credential for which a revocation request is received was one that**
2744 **was issued by the specified service, applying the same process and criteria as would**
2745 **be applied to an original identity proofing.**

2746 AL2_CM_RVR#020 Revocation reason

2747 **Establish the reason for the revocation request as being sound and well founded, in**
2748 **combination with verification of the Revocant, according to AL2_ID_RVR#030,**
2749 **AL2_ID_RVR#040, or AL2_ID_RVR#050.**

2750 AL2_CM_RVR#030 Verify Subscriber as Revocant

2751 **When the subscriber seeks revocation of the subscriber's own credential, the**
2752 **enterprise must:**

- 2753 a) **if in person, require presentation of a primary Government Picture ID**
2754 **document that shall be electronically verified by a record check against the**
2755 **provided identity with the specified issuing authority's records;**
2756 b) **if remote:**
2757 i. **electronically verify a signature against records (if available),**
2758 **confirmed with a call to a telephone number of record, or;**
2759 ii. **authenticate an electronic request as being from the same subscriber,**
2760 **supported by a credential at Assurance Level 2 or higher.**

2761 AL2_CM_RVR#040 CSP as Revocant

2762 **Where a CSP seeks revocation of a subscriber's credential, the enterprise must**
2763 **establish that the request is either:**

- 2764 a) **from the specified service itself, with authorization as determined by**
2765 **established procedures, or;**
2766 b) **from the client Credential Issuer, by authentication of a formalized request**
2767 **over the established secure communications network.**

2768 AL2_CM_RVR#050 Verify Legal Representative as Revocant

2769 **Where the request for revocation is made by a law enforcement officer or**
2770 **presentation of a legal document, the enterprise must:**

- 2771 a) **if in-person, verify the identity of the person presenting the request;**
2772 b) **if remote:**
2773 i. **in paper/facsimile form, verify the origin of the legal document by a**
2774 **database check or by telephone with the issuing authority, or;**
2775 ii. **as an electronic request, authenticate it as being from a recognized**
2776 **legal office, supported by a credential at Assurance Level 2 or higher.**
2777

2778 **3.7.4.2.3 Secure Revocation Request**

2779 This criterion applies when revocation requests must be communicated between remote
2780 components of the service organization.

2781 An enterprise and its specified service must:

2782 AL2_CM_SRR#010 Submit Request

2783 Submit a request for the revocation to the Credential Issuer service (function), using a
2784 secured network communication.

2785

2786 **3.7.4.3 Assurance Level 3**

2787 **3.7.4.3.1 Revocation Procedures**

2788 These criteria address general revocation functions, such as the processes involved and
2789 the basic requirements for publication.

2790 An enterprise and its specified service must:

2791 AL3_CM_RVP#010 Revocation procedures

2792 a) State the conditions under which revocation of an issued credential may occur;

2793 b) State the processes by which a revocation request may be submitted;

2794 c) State the persons and organizations from which a revocation request will be
2795 accepted;

2796 d) State the validation steps that will be applied to ensure the validity (identity) of
2797 the Revocant, and;

2798 e) State the response time between a revocation request being accepted and the
2799 publication of revised certificate status.

2800 AL3_CM_RVP#020 Secure status notification

2801 Ensure that published credential status notification information can be relied upon in
2802 terms of the enterprise being its origin (i.e., its authenticity) and its correctness (i.e., its
2803 integrity).

2804 AL3_CM_RVP#030 Revocation publication

2805 **[Omitted]** Ensure that published credential status notification is revised within **24** hours
2806 of the receipt of a valid revocation request, such that any subsequent attempts to use that
2807 credential in an authentication shall be unsuccessful. **The nature of the revocation**
2808 **mechanism shall be in accord with the technologies supported by the service.**

2809 AL3_CM_RVP_#040 Verify Revocation Identity

2810 Establish that the identity for which a revocation request is received is one that was
2811 issued by the specified service.

2812 AL3_CM_RVP#050 Revocation Records

2813 Retain a record of any revocation of a credential that is related to a specific identity
2814 previously verified, solely in connection to the stated credential. At a minimum, records
2815 of revocation must include:

- 2816 a) the Revocant's full name;
2817 b) the Revocant's authority to revoke (e.g., subscriber themselves, someone acting
2818 with the subscriber's power of attorney, the credential issuer, law enforcement, or
2819 other legal due process);
2820 c) the Credential Issuer's identity (if not directly responsible for the identity
2821 proofing service);
2822 d) the identity associated with the credential (whether the subscriber's name or a
2823 pseudonym);
2824 e) the reason for revocation.

2825 AL3_CM_RVP#060 Record Retention

2826 Retain, securely, the record of the revocation process for a period which is in compliance
2827 with:

- 2828 a) the records retention policy required by AL2_CM_CPP#010, and;
2829 b) applicable legislation;

2830 and which, in addition, must be not less than the duration of the subscriber's account plus
2831 7.5 years.

2832

2833 **3.7.4.3.2 Verify Revocant's Identity**

2834 Revocation of a credential requires that the requestor and the nature of the request be
2835 verified as rigorously as the original identity proofing. The enterprise should not act on a
2836 request for revocation without first establishing the validity of the request (if it does not,
2837 itself, determine the need for revocation).

2838 In order to do so, the enterprise and its specified service must:

2839 AL3_CM_RVR#010 Verify revocation identity

2840 Establish that the credential for which a revocation request is received is one that was
2841 initially issued by the specified service, applying the same process and criteria as would
2842 be applied to an original identity proofing.

2843 AL3_CM_RVR#020 Revocation reason

2844 Establish the reason for the revocation request as being sound and well founded, in
2845 combination with verification of the Revocant, according to AL3_ID_RVR#030,
2846 AL3_ID_RVR#040, or AL3_ID_RVR#050.

2847 AL3_CM_RVR#030 Verify Subscriber as Revocant

2848 When the subscriber seeks revocation of the subscriber's own credential:

- 2849 a) if in-person, require presentation of a primary Government Picture ID document
2850 that shall be electronically verified by a record check against the provided identity
2851 with the specified issuing authority's records;
2852 b) if remote:
2853 i. electronically verify a signature against records (if available), confirmed
2854 with a call to a telephone number of record, or;
2855 ii. as an electronic request, authenticate it as being from the same subscriber,
2856 supported by a credential at Assurance Level **3** or higher.

2857 AL3_CM_RVR#040 Verify CSP as Revocant

2858 Where a CSP seeks revocation of a subscriber's credential, establish that the request is
2859 either:

- 2860 a) from the specified service itself, with authorization as determined by established
2861 procedures, or;
2862 b) from the client Credential Issuer, by authentication of a formalized request over
2863 the established secure communications network.

2864 AL3_CM_RVR#050 Verify Legal Representative as Revocant

2865 Where the request for revocation is made by a law enforcement officer or presentation of
2866 a legal document:

- 2867 a) if in person, verify the identity of the person presenting the request, or;
2868 b) if remote:
2869 i. in paper/facsimile form, verify the origin of the legal document by a
2870 database check or by telephone with the issuing authority, or;
2871 ii. as an electronic request, authenticate it as being from a recognized legal
2872 office, supported by a credential at Assurance Level **3** or higher.
2873

2874 **3.7.4.3.3 Secure Revocation Request**

2875 This criterion applies when revocation requests must be communicated between remote
2876 components of the service organization.

2877 An enterprise and its specified service must:

2878 AL3_CM_SRR#010 Submit Request

2879 Submit a request for the revocation to the Credential Issuer service (function), using a
2880 secured network communication.

2881

2882 **3.7.4.4 Assurance Level 4**

2883 **3.7.4.4.1 Revocation Procedures**

2884 These criteria address general revocation functions, such as the processes involved and
2885 the basic requirements for publication.

2886 An enterprise and its specified service must:

2887 AL4_CM_RVP#010 Revocation procedures

2888 a) State the conditions under which revocation of an issued certificate may occur;

2889 b) State the processes by which a revocation request may be submitted;

2890 c) State the persons and organizations from which a revocation request will be
2891 accepted;

2892 d) State the validation steps that will be applied to ensure the validity (identity) of
2893 the Revocant, and;

2894 e) State the response time between a revocation request being accepted and the
2895 publication of revised certificate status.

2896 AL4_CM_RVP#020 Secure status notification

2897 Ensure that published credential status notification information can be relied upon in
2898 terms of the enterprise of its origin (i.e., its authenticity) and its correctness (i.e., its
2899 integrity).

2900 AL4_CM_RVP#030 Revocation publication

2901 Ensure that published credential status notification is revised within **18** hours of the
2902 receipt of a valid revocation request, such that any subsequent attempts to use that
2903 credential in an authentication shall be unsuccessful. The nature of the revocation
2904 mechanism shall be in accordance with the technologies supported by the service.

2905 AL4_CM_RVP#040 No stipulation

2906 AL4_CM_RVP#050 Revocation Records

2907 Retain a record of any revocation of a credential that is related to a specific identity
2908 previously verified, solely in connection to the stated credential. At a minimum, records
2909 of revocation must include:

2910 a) the Revocant's full name;

- 2911 b) the Revocant's authority to revoke (e.g., subscriber themselves, someone acting
2912 with the subscriber's power of attorney, the credential issuer, law enforcement, or
2913 other legal due process);
2914 c) the Credential Issuer's identity (if not directly responsible for the identity
2915 proofing service);
2916 d) the identity associated with the credential (whether the subscriber's name or a
2917 pseudonym);
2918 e) the reason for revocation.

2919 AL4_CM_RVP#060 Record Retention

2920 Retain, securely, the record of the revocation process for a period which is in compliance
2921 with:

2922 c) the records retention policy required by AL2_CM_CPP#010, and;

2923 d) applicable legislation;

2924 and which, in addition, must be not less than the duration of the subscriber's account plus
2925 7.5 years.

2926

2927 **3.7.4.4.2 Verify Revocant's Identity**

2928 Revocation of a credential requires that the requestor and the nature of the request be
2929 verified as rigorously as the original identity proofing. The enterprise should not act on a
2930 request for revocation without first establishing the validity of the request (if it does not,
2931 itself, determine the need for revocation).

2932 In order to do so, the enterprise and its specified service must:

2933 AL4_CM_RVR#010 Verify revocation identity

2934 Establish that the credential for which a revocation request is received is one that was
2935 initially issued by the specified service, applying the same process and criteria as would
2936 apply to an original identity proofing.

2937 AL4_CM_RVR#020 Revocation reason

2938 Establish the reason for the revocation request as being sound and well founded, in
2939 combination with verification of the Revocant, according to AL4_CM_RVR#030,
2940 AL4_CM_RVR#040, or AL4_CM_RVR#050.

2941 AL4_CM_RVR#030 Verify Subscriber as Revocant

2942 Where the subscriber seeks revocation of the subscriber's own credential:

- 2943 a) if in person, require presentation of a primary Government Picture ID document
2944 that shall be [Omitted] verified by a record check against the provided identity
2945 with the specified issuing authority's records;
2946 b) if remote:
2947 i. verify a signature against records (if available), confirmed with a call to a
2948 telephone number of record, or;
2949 ii. as an electronic request, authenticate it as being from the same subscriber,
2950 supported by a **different** credential at **Assurance Level 4**.

2951 AL4_CM_RVR#040 Verify CSP as Revocant

2952 Where a CSP seeks revocation of a subscriber's credential, establish that the request is
2953 either:

- 2954 a) from the specified service itself, with authorization as determined by established
2955 procedures, or;
2956 b) from the client Credential Issuer, by authentication of a formalized request over
2957 the established secure communications network.

2958 AL4_CM_RVR#050 Verify Legal Representative as Revocant

2959 Where the request for revocation is made by a law enforcement officer or presentation of
2960 a legal document:

- 2961 a) if in-person, verify the identity of the person presenting the request, or;
2962 b) if remote:
2963 i. in paper/facsimile form, verify the origin of the legal document by a
2964 database check or by telephone with the issuing authority;
2965 ii. as an electronic request, authenticate it as being from a recognized legal
2966 office, supported by a different credential at **Assurance Level 4**.

2967 **3.7.4.4.3 Re-keying a credential**

2968 Re-keying of a credential requires that the requestor be verified as the subject with as
2969 much rigor as was applied to the original identity proofing. The enterprise should not act
2970 on a request for re-key without first establishing that the requestor is identical to the
2971 subject.

2972 In order to do so, the enterprise and its specified service must:

2973 AL4_CM_RKY#010 Verify Requestor as Subscriber

2974 **Where the subscriber seeks a re-key for the subscriber's own credential:**

- 2975 a) **if in-person, require presentation of a primary Government Picture ID**
2976 **document that shall be verified by a record check against the provided**
2977 **identity with the specified issuing authority's records;**
2978 b) **if remote:**

- 2979 i. **verify a signature against records (if available), confirmed with a call**
2980 **to a telephone number of record, or;**
2981 ii. **authenticate an electronic request as being from the same subscriber,**
2982 **supported by a different credential at Assurance Level 4.**
2983

2984 AL4_CM_RKY#020 Re-key requests other than subscriber

2985 **Re-key requests from any parties other than the subscriber must not be accepted.**

2986 **3.7.4.4.4 Secure Revocation/Re-key Request**

2987 This criterion applies when revocation **or re-key** requests must be communicated
2988 between remote components of the service organization.

2989 The enterprise and its specified service must:

2990 AL4_CM_SRR#010 Submit Request

2991 Submit a request for the revocation to the Credential Issuer service (function), using a
2992 secured network communication.

2993

2994 **3.7.5 Part E - Credential Status Management**

2995 These criteria deal with credential status management, such as the receipt of requests for
2996 new status information arising from a new credential being issued or a revocation or other
2997 change to the credential that requires notification. They also deal with the provision of
2998 status information to requesting parties (Verifiers, Relying Parties, courts and others
2999 having regulatory authority, etc.) having the right to access such information.

3000 **3.7.5.1 Assurance Level 1**

3001 **3.7.5.1.1 Status Maintenance**

3002 An enterprise and its specified service must:

3003 AL1_CM_CSM#010 Maintain Status Record

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

3005 AL1_CM_CSM#020 No stipulation

3006 AL1_CM_CSM#030 No stipulation

3007 AL1_CM_CSM#040 Status Information Availability

3008 Provide, with 95% availability, a secure automated mechanism to allow relying parties to
3009 determine credential status and authenticate the subject's identity.

3010

3011

3012 **3.7.5.2 Assurance Level 2**

3013 **3.7.5.2.1 Status Maintenance**

3014 An enterprise and its specified service must:

3015 AL2_CM_CSM#010 Maintain Status Record

3016 Maintain a record of the status of all credentials issued.

3017 AL2_CM_CSM#020 Validation of Status Change Requests

3018 **Authenticate all requestors seeking to have a change of status recorded and**
3019 **published and validate the requested change before considering processing the**
3020 **request. Such validation should include:**

3021 a) **the requesting source as one from which the specified service expects to**
3022 **receive such requests;**

3023 b) **if the request is not for a new status, the credential or identity as being one**
3024 **for which a status is already held.**

3025 AL2_CM_CSM#030 Revision to Published Status

3026 **Process authenticated requests for revised status information and have the revised**
3027 **information available for access within a period of 72 hours.**

3028 AL2_CM_CSM#040 Status Information Availability

3029 Provide, with 95% availability, a secure automated mechanism to allow relying parties to
3030 determine credential status and authenticate the subject's identity.

3031 AL2_CM_CSM#050 Inactive Credentials

3032 **Disable any credential that has not been successfully used for authentication during**
3033 **a period of 18 months.**

3034

3035

3036 **3.7.5.3 Assurance Level 3**

3037 **3.7.5.3.1 Status Maintenance**

3038 An enterprise and its specified service must:

3039 AL3_CM_CSM#010 Maintain Status Record

3040 Maintain a record of the status of all credentials issued.

3041 AL3_CM_CSM#020 Validation of Status Change Requests

3042 Authenticate all requestors seeking to have a change of status recorded and published and
3043 validate the requested change before considering processing the request. Such validation
3044 should include:

- 3045 a) the requesting source as one from which the specified service expects to receive
3046 such requests;
3047 b) if the request is not for a new status, the credential or identity as being one for
3048 which a status is already held.

3049 AL3_CM_CSM#030 Revision to Published Status

3050 Process authenticated requests for revised status information and have the revised
3051 information available for access within a period of 72 hours.

3052 AL3_CM_CSM#040 Status Information Availability

3053 Provide, with **99%** availability, a secure automated mechanism to allow relying parties to
3054 determine credential status and authenticate the subject's identity.

3055 AL3_CM_CSM#050 Inactive Credentials

3056 Disable any credential that has not been successfully used for authentication during a
3057 period of 18 months.

3058

3059

3060 **3.7.5.4 Assurance Level 4**

3061 **3.7.5.4.1 Status Maintenance**

3062 An enterprise and its specified service must:

3063 AL4_CM_CSM#010 Maintain Status Record

3064 Maintain a record of the status of all credentials issued.

3065 AL4_CM_CSM#020 Validation of Status Change Requests

3066 Authenticate all requestors seeking to have a change of status recorded and published and
3067 validate the requested change before considering processing the request. Such validation
3068 should include:

- 3069 a) the requesting source as one from which the specified service expects to receive
3070 such requests;
3071 b) if the request is not for a new status, the credential or identity as being one for
3072 which a status is already held.

3073 AL4_CM_CSM#030 Revision to Published Status

3074 Process authenticated requests for revised status information and have the revised
3075 information available for access within a period of 72 hours.

3076 AL4_CM_CSM#040 Status Information Availability

3077 Provide, with 99% availability, a secure automated mechanism to allow relying parties to
3078 determine credential status and authenticate the subject's identity.

3079 AL4_CM_CSM#050 Inactive Credentials

3080 Disable any credential that has not been successfully used for authentication during a
3081 period of 18 months.

3082

3083 **3.7.6 Part F - Credential Validation/Authentication**

3084 These criteria apply to credential validation and identity authentication.

3085 **3.7.6.1 Assurance Level 1**

3086 **3.7.6.1.1 Assertion Security**

3087 An enterprise and its specified service must:

3088 AL1_CM_ASS#010 Validation and Assertion Security

3089 Provide validation of credentials to a Relying Party using a protocol that:

- 3090 a) requires authentication of the specified service or of the validation source;
- 3091 b) ensures the integrity of the authentication assertion;
- 3092 c) protects assertions against manufacture, modification and substitution, and
- 3093 secondary authenticators from manufacture;

3094 and which, specifically:

- 3095 d) creates assertions which are specific to a single transaction;
- 3096 e) where assertion references are used, generates a new reference whenever a new
- 3097 assertion is created;
- 3098 f) when an assertion is provided indirectly, either signs the assertion or sends it via a
- 3099 protected channel, using a strong binding mechanism between the secondary
- 3100 authenticator and the referenced assertion;
- 3101 g) requires the secondary authenticator to:
 - 3102 i) be signed when provided directly to Relying Party, or;
 - 3103 ii) have a minimum of 64 bits of entropy when provision is indirect (i.e.
 - 3104 through the credential user).

3105 AL1_CM_ASS#015 No stipulation

3106 AL1_CM_ASS#020 No Post Authentication

3107 *Not* authenticate credentials that have been revoked.

3108 AL1_CM_ASS#030 Proof of Possession

3109 Use an authentication protocol that requires the claimant to prove possession and control

3110 of the authentication token.

3111 AL1_CM_ASS#040 Assertion Lifetime

3112 Generate assertions so as to indicate and effect their expiration within:

- 3113 a) 12 hours after their creation, where the service shares a common internet domain
3114 with the Relying Party;
- 3115 b) five minutes after their creation, where the service does not share a common
3116 internet domain with the Relying Party.
- 3117
- 3118

3119 **3.7.6.2 Assurance Level 2**

3120 **3.7.6.2.1 Assertion Security**

3121 An enterprise and its specified service must:

3122 AL2_CM_ASS#010 Validation and Assertion Security

3123 Provide validation of credentials to a Relying Party using a protocol that:

- 3124 a) requires authentication of the specified service, itself, or of the validation source;
- 3125 b) ensures the integrity of the authentication assertion;
- 3126 c) protects assertions against manufacture, modification, **substitution and**
- 3127 **disclosure**, and secondary authenticators from manufacture, **capture and replay**;
- 3128 **d) uses approved cryptography techniques;**

3129 and which, specifically:

- 3130 e) creates assertions which are specific to a single transaction;
- 3131 f) where assertion references are used, generates a new reference whenever a new
- 3132 assertion is created;
- 3133 g) when an assertion is provided indirectly, either signs the assertion or sends it via a
- 3134 protected channel, using a strong binding mechanism between the secondary
- 3135 authenticator and the referenced assertion;
- 3136 **h) send assertions either via a channel mutually-authenticated with the Relying**
- 3137 **Party, or signed and encrypted for the Relying Party;**
- 3138 i) requires the secondary authenticator to:
 - 3139 i) be signed when provided directly to Relying Party, or;
 - 3140 ii) have a minimum of 64 bits of entropy when provision is indirect (i.e.
 - 3141 through the credential user);
 - 3142 **iii) be transmitted to the Subject through a protected channel which is**
 - 3143 **linked to the primary authentication process in such a way that**
 - 3144 **session hijacking attacks are resisted;**
 - 3145 **iv) not be subsequently transmitted over an unprotected channel or to an**
 - 3146 **unauthenticated party while it remains valid.**

3147 AL2_CM_ASS#015 No False Authentication

3148 **Employ techniques which ensure that system failures do not result in ‘false positive**

3149 **authentication’ errors.**

3150 AL2_CM_ASS#020 No Post Authentication

3151 *Not* authenticate credentials that have been revoked **unless the time of the transaction**

3152 **for which verification is sought preceeds the time of revocation of the credential.**

-
- 3153 AL2_CM_ASS#030 Proof of Possession
- 3154 Use an authentication protocol that requires the claimant to prove possession and control
3155 of the authentication token.
- 3156 AL2_CM_ASS#040 Assertion Lifetime
- 3157 Generate assertions so as to indicate and effect their expiration:
- 3158 a) 12 hours after their creation, where the service shares a common internet domain
3159 with the Relying Party;
- 3160 b) five minutes after their creation, where the service does not share a common
3161 internet domain with the Relying Party.
- 3162
- 3163

3164 **3.7.6.3 Assurance Level 3**

3165 **3.7.6.3.1 Assertion Security**

3166 An enterprise and its specified service must:

3167 AL3_CM_ASS#010 Validation and Assertion Security

3168 Provide validation of credentials to a Relying Party using a protocol that:

- 3169 a) requires authentication of the specified service, itself, or of the validation source;
3170 b) ensures the integrity of the authentication assertion.

3171 AL3_CM_ASS#015 No False Authentication

3172 Employ techniques which ensure that system failures do not result in ‘false positive
3173 authentication’ errors.

3174 AL3_CM_ASS#020 Post Authentication

3175 *Not* authenticate credentials that have been revoked unless the time of the transaction for
3176 which verification is sought precedes the time of revocation of the credential.

3177 AL3_CM_ASS#030 Proof of Possession

3178 Use an authentication protocol that requires the claimant to prove possession and control
3179 of the authentication token.

3180 AL3_CM_ASS#040 Assertion Lifetime

3181 **For non-cryptographic credentials**, generate assertions so as to indicate and effect their
3182 expiration 12 hours after their creation; **otherwise, notify the relying party of how often**
3183 **the revocation status sources are updated.**

3184

3185

3186 **3.7.6.4 Assurance Level 4**

3187 **3.7.6.4.1 Assertion Security**

3188 An enterprise and its specified service must:

3189 AL4_CM_ASS#010 Validation and Assertion Security

3190 Provide validation of credentials to a Relying Party using a protocol that:

- 3191 a) requires authentication of the specified service, itself, or of the validation source;
- 3192 b) ensures the integrity of the authentication assertion.

3193 AL4_CM_ASS#015 No False Authentication

3194 Employ techniques which ensure that system failures do not result in ‘false positive
3195 authentication’ errors.

3196 AL4_CM_ASS#020 Post Authentication

3197 *Not* authenticate credentials that have been revoked unless the time of the transaction for
3198 which verification is sought precedes the time of revocation of the credential.

3199 AL4_CM_ASS#030 Proof of Possession

3200 Use an authentication protocol that requires the claimant to prove possession and control
3201 of the authentication token.

3202 AL4_CM_ASS#040 Assertion Lifetime

3203 **[Omitted]** Notify the relying party of how often the revocation status sources are
3204 updated.

3205

3206

3207 **3.7.7 Compliance Tables**

3208 Use the following tables to correlate criteria for a particular Assurance Level (AL) and
3209 the evidence offered to support compliance.

3210 Service providers preparing for an assessment can use the table appropriate to the AL at
3211 which they are seeking approval to correlate evidence with criteria or to justify non-
3212 applicability (e.g., “specific service types not offered”).

3213 Assessors can use the tables to record the steps in their assessment and their
3214 determination of compliance or failure.

3215 **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	

3216

3217

3218

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	

3219

3220

3221

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	

3222

3223

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	

3224

3225 4 REFERENCES

3226

3227 [CAF] Louden, Chris, Spencer, Judy, Burr, Bill, Hawkins, Kevin, Temoshok, David,
3228 Cornell, John, Wilsher, Richard G., Timchak, Steve, Sill, Stephen, Silver, Dave, Harrison,
3229 Von, eds., "E-Authentication Credential Assessment Framework (CAF)," E-
3230 Authentication Initiative, Version 2.0.0 (March 16, 2005).
3231 <http://www.cio.gov/eauthentication/documents/CAF.pdf>

3232

3233 [EAP CSAC 04011] "EAP working paper: Identity Proofing Service Assessment Criteria
3234 (ID-SAC)," Electronic Authentication Partnership, Draft 0.1.3 (July 20, 2004)
3235 http://eap.projectliberty.org/docs/Jul2004/EAP_CSAC_04011_0-1-3_ID-SAC.doc

3236

3237 [EAPTrustFramework] "Electronic Authentication Partnership Trust Framework"
3238 Electronic Authentication Partnership, Version 1.0. (January 6, 2005)
3239 http://eap.projectliberty.org/docs/Trust_Framework_010605_final.pdf

3240

3241 [FIPS140-2] "Security Requirements for Cryptographic Modules" Federal Information
3242 Processing Standards. (May 25, 2001) <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>

3244

3245 [IS27001] ISO/IEC 27001:2005 "Information technology - Security techniques -
3246 Requirements for information security management systems" International Organization
3247 for Standardization.
3248 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

3249

3250 [M-04-04] Bolton, Joshua B., eds., "E-Authentication Guidance for Federal Agencies,"
3251 Office of Management and Budget, (December 16, 2003).
3252 <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>

3253

3254 [NIST800-63] Burr, William E., Dodson, Donna F., Polk, W. Timothy, eds., "Electronic
3255 Authentication Guideline: : Recommendations of the National Institute of Standards and
3256 Technology," Version 1.0.2, National Institute of Standards and Technology, (April,
3257 2006). http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

3258

- 3259 [RFC 3647] Chokhani, S., Ford, W., Sabett, R., Merrill, C., Wu, S., eds., "Internet X.509
3260 Public Key Infrastructure Certificate Policy and Certification Practices Framework," The
3261 Internet Engineering Task Force (November, 2003). <http://www.ietf.org/rfc/rfc3647.txt>
3262
3263

Revision History

- 3264
- 3265 1. 8May2008 – Identity Assurance Framework Version 1.0 Initial Draft
- 3266 a. Released by Liberty Alliance
- 3267 b. Revision and scoping of Initial Draft release
- 3268 2. 23JUNE 2008 – Identity Assurance Framework Version 1.1 Final Draft
- 3269 a. Released by Liberty Alliance
- 3270 b. Inclusion of comments to Final Draft
- 3271 3. 1OCTOBER2009 – Identity Assurance Framework Version 1.1 Final Draft
- 3272 a. Documents contributed to Kantara Initiative by Liberty Alliance
- 3273 4. XAPRIL2010 – Identity Assurance Framework Version 2.0
- 3274 a. Released by Kantara Initiative
- 3275 b. Significant scope build
- 3276 c. Original Identity Assurance Framework all inclusive document broken in
- 3277 to a set of documents with specific focus:
- 3278 i. Kantara IAF-1000-Overview
- 3279 ii. Kantara IAF-1100-Glossary
- 3280 iii. Kantara IAF-1200-Levels of Assurance
- 3281 iv. Kantara IAF-1300-Assurance Assessment Scheme
- 3282 v. Kantara IAF-1400-Service Assessment Criteria
- 3283 vi. Kantara IAF-1600-Assessor Qualifications and Requirements
- 3284