

1



2

# 3 Identity Assurance Framework: 4 Service Assessment Criteria

5

6

7

8 **Version:** draft 0.9.1

9 **Date:** 2009-12-31

10 **Editor:** Richard G. Wilsher  
11 Zyigma LLC  
12 Joni Brennan  
13 IEEE-ISTO

## 14 **Contributors**

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

## 17 **Abstract**

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

31

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

## Notice

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  
58

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

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

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

59

60

61 **1 INTRODUCTION .....4**

62 **2 ASSURANCE LEVELS .....5**

63 **3 SERVICE ASSESSMENT CRITERIA .....6**

64 3.1 Context and Scope .....6

65 3.2 Readership .....6

66 3.3 Criteria Descriptions .....7

67 3.4 Terminology .....8

68 3.5 Common Organizational Service Assessment Criteria .....9

69 3.5.1 Assurance Level 1 .....9

70 3.5.2 Assurance Level 2 .....12

71 3.5.3 Assurance Level 3 .....22

72 3.5.4 Assurance Level 4 .....32

73 3.5.5 Compliance Tables .....42

74 3.6 Identity Proofing Service Assessment Criteria .....49

75 3.6.1 Assurance Level 1 .....49

76 3.6.2 Assurance Level 2 .....52

77 3.6.3 Assurance Level 3 .....58

78 3.6.4 Assurance Level 4 .....64

79 3.6.5 Compliance Tables .....69

80 3.7 Credential Management Service Assessment Criteria .....73

81 3.7.1 Part A - Credential Operating Environment .....73

82 3.7.2 Part B - Credential Issuing .....86

83 3.7.3 Part C - Credential Renewal and Re-issuing .....100

84 3.7.4 Part D - Credential Revocation .....104

85 3.7.5 Part E - Credential Status Management .....115

86 3.7.6 Part F - Credential Validation/Authentication .....119

87 3.7.7 Compliance Tables .....125

88 **4 REFERENCES .....133**

89

90

## 91 1 INTRODUCTION

---

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

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

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

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

## 126 **2 ASSURANCE LEVELS**

---

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

## 131 **3 SERVICE ASSESSMENT CRITERIA**

---

### 132 **3.1 Context and Scope**

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

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

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

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

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

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

### 155 **3.2 Readership**

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

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

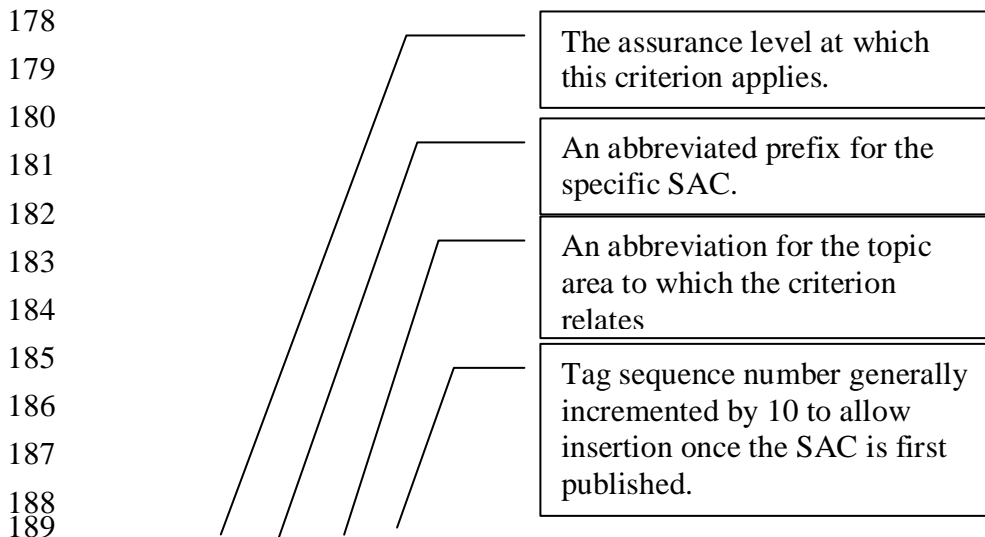
165 This document will also be of interest to those wishing to have a detailed understanding  
166 of the operation of the Identity Assurance Framework but who are not actively involved  
167 in its operations or in services that may fall within the scope of the Framework.

### 168 3.3 Criteria Descriptions

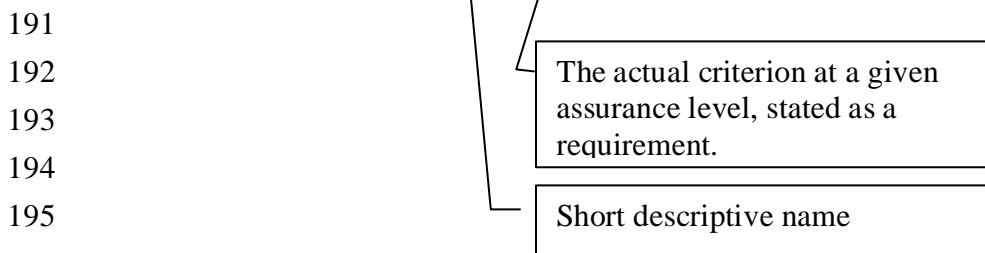
169 The Service Assessment Criteria are organized by AL. Subsections within each level  
170 describe the criteria that apply to specific functions. The subsections are parallel.  
171 Subsections describing the requirements for the same function at different levels of  
172 assurance have the same title.

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

177 The criteria are described as follows:



190 «ALn\_CO\_ZZZ#999»«name»Criterion ALn (i.e., AL1\_CO\_ESM#010)



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

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

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

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

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

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

### 214 **3.4 Terminology**

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

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

219



## 220 3.5 Common Organizational Service Assessment Criteria

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

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

### 228 3.5.1 Assurance Level 1

#### 229 3.5.1.1 Enterprise and Service Maturity

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

233 An enterprise and its specified service must:

234 AL1\_CO\_ESM#010          Established enterprise

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

237 AL1\_CO\_ESM#020          Established service

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

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

246 AL1\_CO\_ESM#030          Legal & Contractual compliance

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

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

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

254 AL1\_CO\_ESM#040 No stipulation

255 AL1\_CO\_ESM#050 No stipulation

256 AL1\_CO\_ESM#055 Termination provisions

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

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

### 267 3.5.1.2 Notices and User information

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

270 An enterprise and its specified service must:

271 AL1\_CO\_NUI#010 General Service Definition

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

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

277 AL1\_CO\_NUI#020 Service Definition inclusions

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

280 a) a Privacy Policy

281

- 282 AL1\_CO\_NUI#030 Due notification
- 283 Have in place and follow appropriate policy and procedures to ensure that it notifies  
284 Users in a timely and reliable fashion of any changes to the Service Definition and any  
285 applicable Terms, Conditions, and Privacy Policy for the specified service.
- 286 AL1\_CO\_NUI#040 User Acceptance
- 287 Require subscribers and subjects to:
- 288 a) indicate, prior to receiving service, that they have read and accept the terms of  
289 service as defined in the Service Definition;
- 290 b) at periodic intervals, determined by significant service provision events (e.g.  
291 issuance, re-issuance, renewal), re-affirm their understanding and observance of  
292 the terms of service;
- 293 c) always provide full and correct responses to requests for information.
- 294 AL1\_CO\_NUI#050 Record of User Acceptance
- 295 Obtain a record (hard-copy or electronic) of the subscriber's and subject's acceptance of  
296 the terms and conditions of service, prior to initiating the service and thereafter at  
297 periodic intervals, determined by significant service provision events (e.g. re-issuance,  
298 renewal).  
299
- 300 **3.5.1.3 Not used**
- 301 **3.5.1.4 Not used**
- 302 **3.5.1.5 Not used**
- 303 **3.5.1.6 Not used**
- 304 **3.5.1.7 Secure Communications**
- 305 AL1\_CO\_SCO#010 No stipulation
- 306 AL1\_CO\_SCO#020 Limited access to shared secrets
- 307 Ensure that:
- 308 a) access to shared secrets shall be subject to discretionary controls which permit  
309 access to those roles/applications needing such access;
- 310 b) stored shared secrets are not held in their plaintext form unless given adequate  
311 physical or logical protection;
- 312 c) any plaintext passwords or secrets are not transmitted across any public or  
313 unsecured network.  
314

315 **3.5.2 Assurance Level 2**

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

319 **3.5.2.1 Enterprise and Service Maturity**

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

322 An enterprise and its specified service must:

323 AL2\_CO\_ESM#010            Established enterprise

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

326 AL2\_CO\_ESM#020            Established service

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

329 AL2\_CO\_ESM#030            Legal & Contractual compliance

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

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

340 AL2\_CO\_ESM#040            Financial Provisions

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

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

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

351 AL2\_CO\_ESM#050 Data Retention and Protection

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

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

363 AL2\_CO\_ESM#055 Termination provisions

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

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

### 374 **3.5.2.2 Notices and User Information/Agreements**

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

378 An enterprise and its specified service must:

379 AL2\_CO\_NUI#010 General Service Definition

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

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

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

386 AL2\_CO\_NUI#020 Service Definition inclusions

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

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

405 AL2\_CO\_NUI#030 Due notification

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

411 AL2\_CO\_NUI#040 User Acceptance

412 Require subscribers and subjects to:

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

- 419 AL2\_CO\_NUI#050 Record of User Acceptance
- 420 Obtain a record (hard-copy or electronic) of the subscriber's and subject's acceptance of  
421 the terms and conditions of service, prior to initiating the service and thereafter at  
422 periodic intervals, determined by significant service provision events (e.g. re-issuance,  
423 renewal) **and otherwise at least once every five years.**
- 424 AL2\_CO\_NUI#060 Withdrawn
- 425 Withdrawn.
- 426 AL2\_CO\_NUI#070 Change of Subscriber Information
- 427 **Require and provide the mechanisms for subscribers and subjects to provide in a**  
428 **timely manner full and correct amendments should any of their recorded**  
429 **information change, as required under the terms of their use of the service, and only**  
430 **after the subscriber's and/or subject's identity has been authenticated.**
- 431 AL2\_CO\_NUI#080 Withdrawn
- 432 Withdrawn.
- 433 **3.5.2.3 Information Security Management**
- 434 These criteria address the way in which the enterprise manages the security of its  
435 business, the specified service, and information it holds relating to its user community.  
436 This section focuses on the key components that comprise a well-established and  
437 effective Information Security Management System (ISMS), or other IT security  
438 management methodology recognized by a government or professional body.
- 439 An enterprise and its specified service must:
- 440 AL2\_CO\_ISM#010 Documented policies and procedures
- 441 **Have documented all security-relevant administrative, management, and technical**  
442 **policies and procedures. The enterprise must ensure that these are based upon**  
443 **recognized standards, published references or organizational guidelines, are**  
444 **adequate for the specified service, and are implemented in the manner intended.**
- 445 AL2\_CO\_ISM#020 Policy Management and Responsibility
- 446 **Have a clearly defined managerial role, at a senior level, in which full responsibility**  
447 **for the business's security policies is vested and from which review, approval, and**  
448 **promulgation of policy and related procedures is applied and managed. The latest**  
449 **approved versions of these policies must be applied at all times.**

- 450 AL2\_CO\_ISM#030 Risk Management
- 451 **Demonstrate a risk management methodology that adequately identifies and**  
452 **mitigates risks related to the specified service and its user community.**
- 453 AL2\_CO\_ISM#040 Continuity of Operations Plan
- 454 **Have and keep updated a Continuity of Operations Plan that covers disaster**  
455 **recovery and the resilience of the specified service.**
- 456 AL2\_CO\_ISM#050 Configuration Management
- 457 **Demonstrate that there is in place a configuration management system that at least**  
458 **includes:**
- 459 a) **version control for software system components;**  
460 b) **timely identification and installation of all organizationally-approved patches**  
461 **for any software used in the provisioning of the specified service.**
- 462 AL2\_CO\_ISM#060 Quality Management
- 463 **Demonstrate that there is in place a quality management system that is appropriate**  
464 **for the specified service.**
- 465 AL2\_CO\_ISM#070 System Installation and Operation Controls
- 466 **Apply controls during system development, procurement installation, and operation**  
467 **that protect the security and integrity of the system environment, hardware,**  
468 **software, and communications.**
- 469 AL2\_CO\_ISM#080 Internal Service Audit
- 470 **Be audited at least once every 12 months for effective provision of the specified**  
471 **service by independent internal audit functions of the enterprise responsible for the**  
472 **specified service, unless it can show that by reason of its organizational size or due to**  
473 **other operational restrictions it is unreasonable to be so audited.**
- 474 AL2\_CO\_ISM#090 Independent Audit
- 475 **Be audited by an independent auditor at least every 24 months to ensure the**  
476 **organization's security-related practices are consistent with the policies and**  
477 **procedures for the specified service and the applicable SAC.**
- 478 **Guidance:** The appointed auditor should have appropriate accreditation or other  
479 acceptable experience and qualification, comparable to that required of Kantara-  
480 Accredited Assessors. It is expected that it will be cost-effective for the organization to



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

483 AL2\_CO\_ISM#100            Audit Records

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

490 AL2\_CO\_ISM#110            Termination provisions

491 This is now AL2\_CO\_ESM#055.

492

#### 493 **3.5.2.4 Security-relevant Event (Audit) Records**

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

496 An enterprise and its specified service must:

497 AL2\_CO\_SER#010            Security event logging

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

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

506

#### 507 **3.5.2.5 Operational infrastructure**

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

511 An enterprise and its specified service must:

512 AL2\_CO\_OPN#010 Technical security

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

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

521 AL2\_CO\_OPN#020 Defined security roles

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

529 AL2\_CO\_OPN#030 Personnel recruitment

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

533 AL2\_CO\_OPN#040 Personnel skills

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

539 AL2\_CO\_OPN#050 Adequacy of Personnel resources

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

542 AL2\_CO\_OPN#060 Physical access control

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

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

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

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

549 AL2\_CO\_OPN#070 Logical access control

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

552

### 553 **3.5.2.6 External Services and Components**

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

557 An enterprise and its specified service must:

558 AL2\_CO\_ESC#010 Contracted policies and procedures

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

564 AL2\_CO\_ESC#020 Visibility of contracted parties

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

570

### 571 **3.5.2.7 Secure Communications**

572 An enterprise and its specified service must:

573 AL2\_CO\_SCO#010 Secure remote communications

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

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

581 AL2\_CO\_SCO#015 Verification / Authentication confirmation messages

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

588 AL2\_CO\_SCO#016 Verification of Revoked Credential

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

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

596 AL2\_CO\_SCO#020 Limited access to shared secrets

597 Ensure that:

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

605  
606 **These roles should be defined and documented by the CSP in accordance with**  
607 **AL2\_CO\_OPN#020 above.**

608 AL2\_CO\_SCO#030 Logical protection of shared secrets

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

- 
- 610 a) concatenation of the password to a salt and/or username which is then hashed  
611 with an Approved algorithm such that the computations used to conduct a  
612 dictionary or exhaustion attack on a stolen password file are not useful to  
613 attack other similar password files, or;
- 614 b) encryption using an Approved algorithm and modes, and the shared secret  
615 decrypted only when immediately required for authentication, or;
- 616 c) any secure method allowed to protect shared secrets at Level 3 or 4.
- 617  
618

619           **3.5.3 Assurance Level 3**

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

622           **3.5.3.1 Enterprise and Service Maturity**

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

625           An enterprise and its specified service must:

626           AL3\_CO\_ESM#010           Established enterprise

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

629           AL3\_CO\_ESM#020           Established service

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

632           AL3\_CO\_ESM#030           Legal & Contractual compliance

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

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

643           AL3\_CO\_ESM#040           Financial Provisions

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

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

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

654 AL3\_CO\_ESM#050 Data Retention and Protection

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

661 AL3\_CO\_ESM#055 Termination provisions

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

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

672 AL3\_CO\_ESM#060 Ownership

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

676 AL3\_CO\_ESM#070 Independent management and operations

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

681

682 **3.5.3.2 Notices and User Information**

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

686 An enterprise and its specified service must:

687 AL3\_CO\_NUI#010 General Service Definition

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

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

694 AL3\_CO\_NUI#020 Service Definition inclusions

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

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

713 AL3\_CO\_NUI#030 Due notification

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



719 AL3\_CO\_NUI#040 User Acceptance

720 Require subscribers and subjects to:

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

727 AL3\_CO\_NUI#050 Record of User Acceptance

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

732 AL3\_CO\_NUI#060 Withdrawn

733 Withdrawn.

734 AL3\_CO\_NUI#070 Change of Subscriber Information

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

739 AL3\_CO\_NUI#080 Withdrawn

740 Withdrawn.

741

### 742 3.5.3.3 Information Security Management

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

748 An enterprise and its specified service must:

- 749 AL3\_CO\_ISM#010 Documented policies and procedures
- 750 Have documented all security-relevant administrative management and technical policies  
751 and procedures. The enterprise must ensure that these are based upon recognized  
752 standards, published references or organizational guidelines, are adequate for the  
753 specified service, and are implemented in the manner intended.
- 754 AL3\_CO\_ISM#020 Policy Management and Responsibility
- 755 Have a clearly defined managerial role, at a senior level, where full responsibility for the  
756 business' security policies is vested and from which review, approval, and promulgation  
757 of policy and related procedures is applied and managed. The latest approved versions of  
758 these policies must be applied at all times.
- 759 AL3\_CO\_ISM#030 Risk Management
- 760 Demonstrate a risk management methodology that adequately identifies and mitigates  
761 risks related to the specified service and its user community **and must show that a risk  
762 assessment review is performed at least once every six months, such as adherence to  
763 SAS 70 or [\[IS27001\]](#) method.**
- 764 AL3\_CO\_ISM#040 Continuity of Operations Plan
- 765 Have and keep updated a continuity of operations plan that covers disaster recovery and  
766 the resilience of the specified service **and must show that a review of this plan is  
767 performed at least once every six months.**
- 768 AL3\_CO\_ISM#050 Configuration Management
- 769 Demonstrate that there is in place a configuration management system that at least  
770 includes:
- 771 a) version control for software system components;  
772 b) timely identification and installation of all organizationally-approved patches for  
773 any software used in the provisioning of the specified service;  
774 c) **version control and managed distribution for all documentation associated  
775 with the specification, management, and operation of the system, covering  
776 both internal and publicly available materials.**
- 777 AL3\_CO\_ISM#060 Quality Management
- 778 Demonstrate that there is in place a quality management system that is appropriate for the  
779 specified service.

780 AL3\_CO\_ISM#070 System Installation and Operation Controls

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

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

793 AL3\_CO\_ISM#080 Internal Service Audit

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

798 AL3\_CO\_ISM#090 Independent Audit

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

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

807 AL3\_CO\_ISM#100 Audit Records

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

814 AL3\_CO\_ISM#110 Termination provisions

815 This is now AL3\_CO\_ESM#055.

816 AL3\_CO\_ISM#120 Best Practice Security Management

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

823

#### 824 **3.5.3.4 Security-Relevant Event (Audit) Records**

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

827 An enterprise and its specified service must:

828 AL3\_CO\_SER#010 Security Event Logging

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

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

837

#### 838 **3.5.3.5 Operational Infrastructure**

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

842 An enterprise and its specified service must:

843 AL3\_CO\_OPN#010 Technical security

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

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

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

852 AL3\_CO\_OPN#020 Defined security roles

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

860 AL3\_CO\_OPN#030 Personnel recruitment

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

866 AL3\_CO\_OPN#040 Personnel skills

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

872 AL3\_CO\_OPN#050 Adequacy of Personnel resources

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

875 AL3\_CO\_OPN#060 Physical access control

876 Apply physical access control mechanisms to ensure that:

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

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

881 AL3\_CO\_OPN#070 Logical access control

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

884

### 885 3.5.3.6 External Services and Components

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

889 An enterprise and its specified service must:

890 AL3\_CO\_ESC#010 Contracted policies and procedures

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

896 AL3\_CO\_ESC#020 Visibility of contracted parties

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

902

### 903 3.5.3.7 Secure Communications

904 An enterprise and its specified service must:

905 AL3\_CO\_SCO#010 Secure remote communications

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

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

914 AL3\_CO\_SCO#020 Limited access to shared secrets

915 Ensure that:

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

933

934 **These roles should be defined and documented by the CSP in accordance with**  
935 **AL3\_CO\_OPN#020 above.**

936

937

938 **3.5.4 Assurance Level 4**

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

941 **3.5.4.1 Enterprise and Service Maturity**

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

944 An enterprise and its specified service must:

945 AL4\_CO\_ESM#010 Established enterprise

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

948 AL4\_CO\_ESM#020 Established service

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

951 AL4\_CO\_ESM#030 Legal & Contractual compliance

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

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

962 AL4\_CO\_ESM#040 Financial Provisions

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

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



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

973 AL4\_CO\_ESM#050 Data Retention and Protection

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

980 Termination provisions

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

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

991 AL4\_CO\_ESM#060 Ownership

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

995 AL4\_CO\_ESM#070 Independent Management and Operations

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

999

#### 1000 **3.5.4.2 Notices and Subscriber Information/Agreements**

1001 Criteria in this section address the publication of information describing the service and  
1002 the manner of and any limitations upon its provision, and how users are required to accept  
1003 those terms.

1004 An enterprise and its specified service must:

1005 AL4\_CO\_NUI#010 General Service Definition

1006 Make available to the intended user community a Service Definition that includes all  
1007 applicable Terms, Conditions, and Fees, including any limitations of its usage, and  
1008 definitions of any terms having specific intention or interpretation. Specific provisions  
1009 are stated in further criteria in this section.

1010 **Guidance:** The intended user community encompasses potential and actual subscribers,  
1011 subjects, and relying parties.

1012 AL4\_CO\_NUI#020 Service Definition inclusions

1013 Make available a Service Definition for the specified service containing clauses that  
1014 provide the following information:

- 1015 a) Privacy, Identity Proofing & Verification, and Revocation and Termination  
1016 Policies;
- 1017 b) the country in or legal jurisdiction under which the service is operated;
- 1018 c) if different to the above, the legal jurisdiction under which subscriber and any  
1019 relying party agreements are entered into;
- 1020 d) applicable legislation with which the service complies;
- 1021 e) obligations incumbent upon the CSP;
- 1022 f) obligations incumbent upon the subscriber;
- 1023 g) notifications and guidance for relying parties, especially in respect of actions they  
1024 are expected to take should they choose to rely upon the service's product;
- 1025 h) statement of warranties;
- 1026 i) statement of liabilities toward both Subjects and Relying Parties;
- 1027 j) procedures for notification of changes to terms and conditions;
- 1028 k) steps the CSP will take in the event that it chooses or is obliged to terminate the  
1029 service;
- 1030 l) availability of the specified service per se and of its help desk facility.

1031 AL4\_CO\_NUI#030 Due Notification

1032 Have in place and follow appropriate policy and procedures to ensure that it notifies  
1033 subscribers and subjects in a timely and reliable fashion of any changes to the Service  
1034 Definition and any applicable Terms, Conditions, Fees, and Privacy Policy for the  
1035 specified service, and provide a clear means by which subscribers and subjects must  
1036 indicate that they wish to accept the new terms or terminate their subscription.

1037 AL4\_CO\_NUI#040 User Acceptance

1038 Require subscribers and subjects to:

- 1039 a) indicate, prior to receiving service, that they have read and accept the terms of  
1040 service as defined in the Service Definition, thereby indicating their properly-  
1041 informed opt-in;  
1042 b) at periodic intervals, determined by significant service provision events (e.g.  
1043 issuance, re-issuance, renewal) and otherwise at least once every five years, re-  
1044 affirm their understanding and observance of the terms of service;  
1045 c) always provide full and correct responses to requests for information.

1046 AL4\_CO\_NUI#050 Record of User Acceptance

1047 Obtain a record (hard-copy or electronic) of the subscriber's and subject's acceptance of  
1048 the terms and conditions of service, prior to initiating the service and thereafter reaffirm  
1049 the agreement at periodic intervals, determined by significant service provision events  
1050 (e.g. issuance, re-issuance, renewal) and otherwise at least once every five years.

1051 AL4\_CO\_NUI#060 Withdrawn

1052 Withdrawn.

1053 AL4\_CO\_NUI#070 Change of Subscriber Information

1054 Require and provide the mechanisms for subscribers and subjects to provide in a timely  
1055 manner full and correct amendments should any of their recorded information change, as  
1056 required under the terms of their use of the service, and only after the subscriber's and/or  
1057 subject's identity has been authenticated.

1058 AL4\_CO\_NUI#080 Withdrawn

1059 Withdrawn.

1060

#### 1061 **3.5.4.3 Information Security Management**

1062 These criteria address the way in which the enterprise manages the security of its  
1063 business, the specified service, and information it holds relating to its user community.

1064 This section focuses on the key components that comprise a well-established and  
1065 effective Information Security Management System (ISMS), or other IT security  
1066 management methodology recognized by a government or professional body.

1067 An enterprise and its specified service must:

1068 AL4\_CO\_ISM#010 Documented policies and procedures

1069 Have documented all security-relevant administrative, management, and technical  
1070 policies and procedures. The enterprise must ensure that these are based upon recognized

- 1071 standards, published references, or organizational guidelines, are adequate for the  
1072 specified service, and are implemented in the manner intended.
- 1073 AL4\_CO\_ISM#020 Policy Management and Responsibility
- 1074 Have a clearly defined managerial role, at a senior level, where full responsibility for the  
1075 business' security policies is vested and from which review, approval, and promulgation  
1076 of policy and related procedures is applied and managed. The latest approved versions of  
1077 these policies must be applied at all times.
- 1078 AL4\_CO\_ISM#030 Risk Management
- 1079 Demonstrate a risk management methodology that adequately identifies and mitigates  
1080 risks related to the specified service and its user community and must show that on-going  
1081 risk assessment review is conducted as a part of the business' procedures, such as  
1082 adherence to SAS 70 or [\[IS27001\]](#) methods.
- 1083 AL4\_CO\_ISM#040 Continuity of Operations Plan
- 1084 Have and keep updated a continuity of operations plan that covers disaster recovery and  
1085 the resilience of the specified service and must show that **on-going review of this plan is**  
1086 **conducted as a part of the business' procedures.**
- 1087 AL4\_CO\_ISM#050 Configuration Management
- 1088 Demonstrate that there is in place a configuration management system that at least  
1089 includes:
- 1090 a) version control for software system components;  
1091 b) timely identification and installation of all organizationally-approved patches for  
1092 any software used in the provisioning of the specified service;  
1093 c) version control and managed distribution for all documentation associated with  
1094 the specification, management, and operation of the system, covering both  
1095 internal and publicly available materials.
- 1096 AL4\_CO\_ISM#060 Quality Management
- 1097 Demonstrate that there is in place a quality management system that is appropriate for the  
1098 specified service.
- 1099 AL4\_CO\_ISM#070 System Installation and Operation Controls
- 1100 Apply controls during system development, procurement, installation, and operation that  
1101 protect the security and integrity of the system environment, hardware, software, and  
1102 communications having particular regard to:

- 1103 a) the software and hardware development environments, for customized  
1104 components;
- 1105 b) the procurement process for commercial off-the-shelf (COTS) components;  
1106 c) contracted consultancy/support services;  
1107 d) shipment of system components;  
1108 e) storage of system components;  
1109 f) installation environment security;  
1110 g) system configuration;  
1111 h) transfer to operational status.
- 1112 AL4\_CO\_ISM#080 Internal Service Audit
- 1113 Be audited at least once every 12 months for effective provision of the specified service  
1114 by independent internal audit functions of the enterprise responsible for the specified  
1115 service, unless it can show that by reason of its organizational size or due to other  
1116 justifiable operational restrictions it is unreasonable to be so audited.
- 1117 AL4\_CO\_ISM#090 Independent Audit
- 1118 Be audited by an independent auditor at least every 24 months to ensure the  
1119 organization's security-related practices are consistent with the policies and procedures  
1120 for the specified service.
- 1121 **Guidance:** The appointed auditor should have appropriate accreditation or other  
1122 acceptable experience and qualification, comparable to that required of Kantara-  
1123 Accredited Assessors. It is expected that it will be cost-effective for the organization to  
1124 use the same Kantara-Accredited Assessor for the purposes of fulfilling this criterion as  
1125 they do for the maintenance of their grant of Kantara Recognition.
- 1126 AL4\_CO\_ISM#100 Audit Records
- 1127 Retain records of all audits, both internal and independent, for a period which, as a  
1128 minimum, fulfills its legal obligations and otherwise for greater periods either as it may  
1129 have committed to in its Service Definition or required by any other obligations it has  
1130 with/to a subscriber, and which in any event is not less than 36 months. Such records  
1131 must be held securely and be protected against unauthorized access loss, alteration, public  
1132 disclosure, or unapproved destruction.
- 1133 AL4\_CO\_ISM#110 Termination provisions
- 1134 This is now AL4\_CO\_ESM#055.

1135 AL4\_CO\_ISM#120 Best Practice Security Management

1136 Have in place a certified Information Security Management System (ISMS), or other IT  
1137 security management methodology recognized by a government or professional body,  
1138 that **has been assessed and found to be in compliance with the requirements of**  
1139 **ISO/IEC 27001 [IS27001] and which applies and is appropriate to the CSP in**  
1140 **question.** All requirements expressed in preceding criteria in this section must *inter alia*  
1141 fall wholly within the scope of this ISMS, or the selected recognized alternative.

1142

#### 1143 3.5.4.4 Security-Related (Audit) Records

1144 The criteria in this section are concerned with the need to provide an auditable log of all  
1145 events that are pertinent to the correct and secure operation of the service.

1146 An enterprise and its specified service must:

1147 AL4\_CO\_SER#010 Security Event Logging

1148 Maintain a log of all relevant security events concerning the operation of the service,  
1149 together with a **precise** record of the time at which the event occurred (time-stamp)  
1150 **provided by a trusted time-source** and retain such records with appropriate protection  
1151 and controls to ensure successful retrieval, accounting for service definition, risk  
1152 management requirements, applicable legislation, and organizational policy.

1153 **Guidance:** The trusted time source could be an external trusted service or a network time  
1154 server or other hardware timing device. The time source must be not only precise but  
1155 authenticatable as well.

1156

#### 1157 3.5.4.5 Operational Infrastructure

1158 The criteria in this section address the infrastructure within which the delivery of the  
1159 specified service takes place. It puts particular emphasis upon the personnel involved,  
1160 and their selection, training, and duties.

1161 An enterprise and its specified service must:

1162 AL4\_CO\_OPN#010 Technical Security

1163 Demonstrate that the technical controls employed will provide the level of security  
1164 protection required by the risk assessment and the ISMS, or other IT security  
1165 management methods recognized by a government or professional body, and that these  
1166 controls are effectively integrated with the applicable procedural and physical security  
1167 measures.

1168 **Guidance:** Appropriate technical controls, suited to this Assurance Level, should be  
1169 selected from [\[NIST800-63\]](#) or its equivalent, as established by a recognized national  
1170 technical authority.

1171 AL4\_CO\_OPN#020 Defined Security Roles

1172 Define, by means of a job description, the roles and responsibilities for each service-  
1173 related security-relevant task, relating it to specific procedures (which shall be set out in  
1174 the ISMS, or other IT security management methodology recognized by a government or  
1175 professional body) and other service-related job descriptions. Where the role is security-  
1176 critical or where special privileges or shared duties exist, these must be specifically  
1177 identified as such, including the applicable access privileges relating to logical and  
1178 physical parts of the service's operations.

1179 AL4\_CO\_OPN#030 Personnel Recruitment

1180 Demonstrate that it has defined practices for the selection, vetting, and contracting of all  
1181 service-related personnel, both direct employees and those whose services are provided  
1182 by third parties. Full records of all searches and supporting evidence of qualifications and  
1183 past employment must be kept for the duration of the individual's employment plus the  
1184 longest lifespan of any credential issued under the Service Policy.

1185 AL4\_CO\_OPN#040 Personnel skills

1186 Ensure that employees are sufficiently trained, qualified, experienced, and current for the  
1187 roles they fulfill. Such measures must be accomplished either by recruitment practices or  
1188 through a specific training program. Where employees are undergoing on-the-job  
1189 training, they must only do so under the guidance of a mentor possessing the defined  
1190 service experiences for the training being provided.

1191 AL4\_CO\_OPN#050 Adequacy of Personnel resources

1192 Have sufficient staff to adequately operate and resource the specified service according to  
1193 its policies and procedures.

1194 AL4\_CO\_OPN#060 Physical access control

1195 Apply physical access control mechanisms to ensure that:

- 1196 a) access to sensitive areas is restricted to authorized personnel;  
1197 b) all removable media and paper documents containing sensitive information as  
1198 plain-text are stored in secure containers;  
1199 c) there is 24/7 monitoring for unauthorized intrusions.  
1200

1201 AL4\_CO\_OPN#070 Logical access control

1202 Employ logical access control mechanisms that ensure access to sensitive system  
1203 functions and controls is restricted to authorized personnel.

1204

1205 **3.5.4.6 External Services and Components**

1206 This section addresses the relationships and obligations upon contracted parties both to  
1207 apply the policies and procedures of the enterprise and also to be available for assessment  
1208 as critical parts of the overall service provision.

1209 An enterprise and its specified service must:

1210 AL4\_CO\_ESC#010 Contracted Policies and Procedures

1211 Where the enterprise uses external suppliers for specific packaged components of the  
1212 service or for resources which are integrated with its own operations and under its  
1213 control, ensure that those parties are engaged through reliable and appropriate contractual  
1214 arrangements which stipulate which critical policies, procedures, and practices sub-  
1215 contractors are required to fulfill.

1216 AL4\_CO\_ESC#020 Visibility of Contracted Parties

1217 Where the enterprise uses external suppliers for specific packaged components of the  
1218 service or for resources which are integrated with its own operations and under its  
1219 control, ensure that the suppliers' compliance with contractually-stipulated policies and  
1220 procedures, and thus with the IAF Service Assessment Criteria, can be independently  
1221 verified, and subsequently monitored if necessary.

1222

1223 **3.5.4.7 Secure Communications**

1224 An enterprise and its specified service must:

1225 AL4\_CO\_SCO#010 Secure remote communications

1226 If the specific service components are located remotely from and communicate over a  
1227 public or unsecured network with other service components or other CSPs it services, the  
1228 communications must be cryptographically authenticated, including long-term and  
1229 session tokens, by an authentication protocol that meets the requirements of AL4 and  
1230 encrypted using either a FIPS 140-2 [FIPS140-2] Level 2 (or higher) validated hardware  
1231 cryptographic module or any FIPS 140-2 Level 3 or 4 validated cryptographic module, or  
1232 equivalent, as established by a recognized national technical authority.



- 1233 AL4\_CO\_SCO#020 Limited access to shared secrets
- 1234 Ensure that:
- 1235 a) access to shared secrets shall be subject to discretionary controls which permit
- 1236 access to those roles/applications which need such access;
- 1237 b) stored shared secrets are encrypted such that:
- 1238 i the encryption key for the shared secret file is encrypted under a key held
- 1239 in a FIPS 140-2 [FIPS140-2] Level 2 (or higher) validated hardware
- 1240 cryptographic module, or equivalent, as established by a recognized
- 1241 national technical authority, or any FIPS 140-2 Level 3 or 4 validated
- 1242 cryptographic module, or equivalent, as established by a recognized
- 1243 national technical authority, and decrypted only as immediately required
- 1244 for an authentication operation;
- 1245 ii they are protected as a key within the boundary of a FIPS 140-2 Level 2
- 1246 (or higher) validated hardware cryptographic module, or equivalent, as
- 1247 established by a recognized national technical authority, or any
- 1248 FIPS 140-2 Level 3 or 4 cryptographic module, or equivalent, as
- 1249 established by a recognized national technical authority, and are not
- 1250 exported in plaintext from the module;
- 1251 iii they are split by an "*n from m*" cryptographic secret-sharing method;
- 1252 c) any long-term (i.e., not session) shared secrets are revealed only to the subscriber
- 1253 and the CSP's direct agents (bearing in mind (a) above).
- 1254
- 1255

1256 **3.5.5 Compliance Tables**

1257 Use the following tables to correlate criteria for a particular Assurance Level (AL) and  
1258 the evidence offered to support compliance.

1259 Service providers preparing for an assessment can use the table appropriate to the AL at  
1260 which they are seeking approval to correlate evidence with criteria or to justify non-  
1261 applicability (e.g., "specific service types not offered").

1262 Assessors can use the tables to record the steps in their assessment and their  
1263 determination of compliance or failure.

1264 **Table 3-1. CO-SAC - AL1 Compliance**

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

1265

1266

1267

**Table 3-2. CO-SAC - AL2 Compliance**

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

---

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

1268

1269

1270

**Table 3-3. CO-SAC - AL3 compliance**

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

---

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

1271

1272

1273

**Table 3-4. CO-SAC - AL4 compliance**

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

---

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

1274

1275



## 1276 **3.6 Identity Proofing Service Assessment Criteria**

1277 The Service Assessment Criteria in this section establish the requirements for the  
1278 technical conformity of identity proofing services at all ALs defined in Section 2 and in  
1279 the [Identity Assurance Framework: Levels of Assurance](#) document. These criteria apply  
1280 to a particular kind of electronic trust service (ETS) recognized by the IAWG and to the  
1281 related credential service provider (CSP)—an identity proofing service for both  
1282 individual identity and institutional identity credentials<sup>1</sup>. (For definitions of terms used in  
1283 this section, see the [Identity Assurance Framework: Glossary](#) document). These criteria  
1284 are generally referred to elsewhere within IAWG documentation as ID-SAC [ID-SAC].

1285 These criteria do not address the delivery of a credential to the applicant/subscriber,  
1286 which is dealt with by the Credential Management SAC (CM-SAC), described in Section  
1287 3.7.

1288 These criteria may only be used in an assessment in one of the following circumstances:

- 1289 • In conjunction with the Common Organizational SAC (CO-SAC), described in  
1290 Section 3.5, for a standalone identity proofing service.
- 1291 • In combination with one or more other SACs that must include the CO-SAC and  
1292 where the identity proofing functions that these criteria address form part of a  
1293 larger service offering.

### 1294 **3.6.1 Assurance Level 1**

#### 1295 **3.6.1.1 Policy**

1296 An enterprise or specified service must:

1297 AL1\_ID\_POL#010 Unique service identity

1298 Ensure that a unique identity is attributed to the specific service, such that credentials  
1299 issued by it can be distinguishable from those issued by other services, including services  
1300 operated by the same enterprise.

1301 AL1\_ID\_POL#020 Unique subject identity

1302 Ensure that each applicant's identity is unique within the service's community of subjects  
1303 and uniquely associable with tokens and/or credentials issued to that identity.

---

<sup>1</sup> 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.

1304

1305 **3.6.1.2 Identity Verification**

1306 **3.6.1.2.1 In-Person Public Verification**

1307 An enterprise or specified service must:

1308 AL1\_ID\_IPV#010 Required evidence

1309 Accept a self-assertion of identity.

1310 AL1\_ID\_IPV#020 Evidence checks

1311 Accept self-attestation of evidence.

1312

1313 **3.6.1.2.2 Remote Public Verification**

1314 If the specific service offers remote identity proofing to applicants with whom it has no  
1315 previous relationship, then it must comply with the criteria in this section.

1316 An enterprise or specified service must:

1317 AL1\_ID\_RPV#010 Required evidence

1318 Require the applicant to provide a contact email address. In the case the user does not  
1319 have email address or does not wish to provide an email address a telephone contact is  
1320 required.

1321 AL1\_ID\_RPV#020 Evidence checks

1322 Verify the provided information by either:

1323 a) confirming the request by calling the number;

1324 b) successfully sending a confirmatory email and receiving a positive  
1325 acknowledgement.

1326

1327 **3.6.1.2.3 Secondary Verification**

1328 In each of the above cases, an enterprise or specified service must:

1329 AL1\_ID\_SCV#010 Secondary checks

1330 Have in place additional measures (e.g., require additional documentary evidence, delay  
1331 completion while out-of-band checks are undertaken) to deal with any anomalous  
1332 circumstances that can be reasonably anticipated (e.g., a legitimate and recent change of  
1333 address that has yet to be established as the address of record).

1334

1335

1336 **3.6.2 Assurance Level 2**

1337 **3.6.2.1 Policy**

1338 The specific service must show that it applies identity proofing policies and procedures  
1339 and that it retains appropriate records of identity proofing activities and evidence.

1340 The enterprise or specified service must:

1341 AL2\_ID\_POL#010 Unique service identity

1342 Ensure that a unique identity is attributed to the specific service, such that credentials  
1343 issued by it can be distinguishable from those issued by other services, including services  
1344 operated by the same enterprise.

1345 AL2\_ID\_POL#020 Unique subject identity

1346 Ensure that each applicant's identity is unique within the service's community of subjects  
1347 and uniquely associable with tokens and/or credentials issued to that identity.

1348 AL2\_ID\_POL#030 Published Proofing Policy

1349 **For each service it offers, make available the Identity Proofing Policy under which it**  
1350 **verifies the identity of applicants<sup>2</sup> in form, language, and media accessible to the**  
1351 **declared community of Users.**

1352 AL2\_ID\_POL#040 Adherence to Proofing Policy

1353 **Perform all identity proofing strictly in accordance with its published Identity**  
1354 **Proofing Policy.**

1355

1356 **3.6.2.2 Identity Verification**

1357 The enterprise or specific service must:

---

<sup>2</sup> 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.

- 1358 AL2\_ID\_IDV#000 Identity Proofing classes
- 1359 a) **include in its Service Definition at least one of the following classes of identity**  
1360 **proofing service, and;**
- 1361 b) **may offer any additional classes of identity proofing service it chooses,**  
1362 **subject to the nature and the entitlement of the CSP concerned;**
- 1363 c) **Fulfill the applicable assessment criteria according to its choice of identity**  
1364 **proofing service, i.e. conform to at least one of the criteria sets defined in:**
- 1365 i) §3.6.2.2.1, “[In-Person Public Verification](#)”;
- 1366 ii) §3.6.2.2.2, “[Remote Public Verification](#)”;
- 1367 iii) §3.6.2.2.3, “[Current Relationship Verification](#)”;
- 1368 iv) §3.6.2.2.4, “[Affiliation Verification](#)”.

1369 **3.6.2.2.1 In-Person Public Verification**

1370 If the specific service offers in-person identity proofing to applicants with whom it has no  
1371 previous relationship, then it must comply with the criteria in this section.

1372 The enterprise or specified service must:

1373 AL2\_ID\_IPV#010 Required evidence

1374 **Ensure that the applicant is in possession of a primary Government Picture ID**  
1375 **document that bears a photographic image of the holder.**

1376 AL2\_ID\_IPV#020 Evidence checks

1377 **Have in place and apply processes which ensure that the presented document:**

- 1378 a) **appears to be a genuine document properly issued by the claimed issuing**  
1379 **authority and valid at the time of application;**
- 1380 b) **bears a photographic image of the holder that matches that of the applicant;**
- 1381 c) **provides all reasonable certainty that the identity exists and that it uniquely**  
1382 **identifies the applicant.**  
1383

1384 **3.6.2.2.2 Remote Public Verification**

1385 If the specific service offers remote identity proofing to applicants with whom it has no  
1386 previous relationship, then it must comply with the criteria in this section.

1387 An enterprise or specified service must:

1388 AL2\_ID\_RPV#010 Required evidence

1389 **Ensure that the applicant submits the references of and attests to current possession**  
1390 **of a primary Government Picture ID document, and one of:**

- 1391 a) **a second Government ID;**  
1392 b) **an employee or student ID number;**  
1393 c) **a financial account number (e.g., checking account, savings account, loan or**  
1394 **credit card) or;**  
1395 d) **a utility service account number (e.g., electricity, gas, or water) for an address**  
1396 **matching that in the primary document.**

1397 **Ensure that the applicant provides additional verifiable personal information that at**  
1398 **a minimum must include:**

- 1399 a) **a name that matches the referenced photo-ID;**  
1400 b) **date of birth and;**  
1401 c) **current address or personal email address. In the case the user does not have**  
1402 **email address or does not wish to provide an email address a telephone**  
1403 **contact is required.**

1404 **Additional information may be requested so as to ensure a unique identity, and**  
1405 **alternative information may be sought where the enterprise can show that it leads to**  
1406 **at least the same degree of certitude when verified.**

1407 AL2\_ID\_RPV#020 Evidence checks

1408 **Inspection and analysis of records against the provided identity references with the**  
1409 **specified issuing authorities/institutions or through similar databases:**

- 1410 a) **the existence of such records with matching name and reference numbers;**  
1411 b) **corroboration of date of birth, current address of record, and other personal**  
1412 **information sufficient to ensure a unique identity.**

1413  
1414

1415 **Confirm address of record by at least one of the following means:**

- 1416 a) **RA sends notice to an address of record confirmed in the records check and**  
1417 **receives a mailed or telephonic reply from applicant;**  
1418 b) **RA issues credentials in a manner that confirms the address of record**  
1419 **supplied by the applicant, for example by requiring applicant to enter on-line**  
1420 **some information from a notice sent to the applicant;**  
1421 c) **RA issues credentials in a manner that confirms ability of the applicant to**  
1422 **receive telephone communications at telephone number or email at email**  
1423 **address associated with the applicant in records. Any secret sent over an**  
1424 **unprotected channel shall be reset upon first use.**  
1425

1426 **Additional checks should be performed so as to establish the uniqueness of the**  
1427 **claimed identity.**

1428 **Alternative checks may be performed where the enterprise can show that they lead**  
1429 **to at least the same degree of certitude.**

1430

### 1431 **3.6.2.2.3 Current Relationship Verification**

1432 If the specific service offers identity proofing to applicants with whom it has a current  
1433 relationship, then it must comply with the criteria in this section.

1434 The enterprise or specified service must:

1435 AL2\_ID\_CRV#010 Required evidence

1436 **Ensure that it has previously exchanged with the applicant a shared secret (e.g., a**  
1437 **PIN or password) that meets AL2 (or higher) entropy requirements<sup>3</sup>.**

1438 AL2\_ID\_CRV#020 Evidence checks

1439 **Ensure that it has:**

- 1440 a) **only issued the shared secret after originally establishing the applicant’s**  
1441 **identity with a degree of rigor equivalent to that required under either the**  
1442 **AL2 (or higher) requirements for in-person or remote public verification;**  
1443 b) **an ongoing business relationship sufficient to satisfy the enterprise of the**  
1444 **applicant’s continued personal possession of the shared secret.**  
1445

### 1446 **3.6.2.2.4 Affiliation Verification**

1447 If the specific service offers identity proofing to applicants on the basis of some form of  
1448 affiliation, then it must comply with the criteria in this section for the purposes of  
1449 establishing that affiliation, in addition to the previously stated requirements for the  
1450 verification of the individual’s identity.

1451 The enterprise or specified service must:

1452 AL2\_ID\_AFV#000 Meet preceding criteria

1453 **Meet all the criteria set out above, under §3.6.2.2.3, “[Current Relationship](#)**  
1454 **[Verification](#)”.**

---

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

1455 AL2\_ID\_AFV#010 Required evidence

1456 **Ensure that the applicant possesses:**

- 1457 a) **identification from the organization with which it is claiming affiliation;**  
1458 b) **agreement from the organization that the applicant may be issued a**  
1459 **credential indicating that an affiliation exists.**

1460 AL2\_ID\_AFV#020 Evidence checks

1461 **Have in place and apply processes which ensure that the presented documents:**

- 1462 a) **each appear to be a genuine document properly issued by the claimed issuing**  
1463 **authorities and valid at the time of application;**  
1464 b) **refer to an existing organization with a contact address;**  
1465 c) **indicate that the applicant has some form of recognizable affiliation with the**  
1466 **organization;**  
1467 d) **appear to grant the applicant an entitlement to obtain a credential indicating**  
1468 **its affiliation with the organization.**  
1469

#### 1470 **3.6.2.2.5 Secondary Verification**

1471 In each of the above cases, the enterprise or specified service must:

1472 AL2\_ID\_SCV#010 Secondary checks

1473 Have in place additional measures (e.g., require additional documentary evidence, delay  
1474 completion while out-of-band checks are undertaken) to deal with any anomalous  
1475 circumstances that can be reasonably anticipated (e.g., a legitimate and recent change of  
1476 address that has yet to be established as the address of record).

1477

#### 1478 **3.6.2.3 Verification Records**

1479 The specific service must retain records of the identity proofing (verification) that it  
1480 undertakes and provide them to qualifying parties when so required.

1481 An enterprise or specified service must:

1482 AL2\_ID\_VRC#010 Verification Records for Personal Applicants

1483 **Log, taking account of all applicable legislative and policy obligations, a record of**  
1484 **the facts of the verification process, including a reference relating to the verification**  
1485 **processes and the date and time of verification.**

1486 **Guidance:** The facts of the verification process should include the specific record  
1487 information (source, unique reference, value/content) used in establishing the applicant's  
1488 identity, and will be determined by the specific processes used and documents accepted



1489 by the CSP. The CSP need not retain these records itself if it uses a third-party service  
1490 which retains such records securely and to which the CSP has access when required, in  
1491 which case it must retain a record of the identity of the third-party service providing the  
1492 verification service or the location at which the (in-house) verification was performed.

1493 AL2\_ID\_VRC#020 Verification Records for Affiliated Applicants

1494 **In addition to the foregoing, log, taking account of all applicable legislative and**  
1495 **policy obligations, a record of the additional facts of the verification process must be**  
1496 **performed. At a minimum, records of identity information must include:**

- 1497 a) **the subscriber's full name;**
- 1498 b) **the subscriber's current address of record;**
- 1499 c) **the subscriber's current telephone or email address of record;**
- 1500 d) **the subscriber's acknowledgement for issuing the subject with a credential;**
- 1501 e) **type, issuing authority, and reference number(s) of all documents checked in**  
1502 **the identity proofing process.**

1503 AL2\_ID\_VRC#030 Record Retention

1504 **Either retain, securely, the record of the verification process for the duration of the**  
1505 **subscriber account plus 7.5 years, or submit same record to a client CSP that has**  
1506 **undertaken to retain the record for the requisite period or longer.**

1507

1508

1509           **3.6.3 Assurance Level 3**

1510       **3.6.3.1 Policy**

1511       The specific service must show that it applies identity proofing policies and procedures  
1512       and that it retains appropriate records of identity proofing activities and evidence.

1513       The enterprise or specified service must:

1514       AL3\_ID\_POL#010           Unique service identity

1515       Ensure that a unique identity is attributed to the specific service, such that credentials  
1516       issued by it can be distinguishable from those issued by other services, including services  
1517       operated by the same enterprise.

1518       AL3\_ID\_POL#020           Unique subject identity

1519       Ensure that each applicant's identity is unique within the service's community of subjects  
1520       and uniquely associable with tokens and/or credentials issued to that identity.

1521       AL3\_ID\_POL#030           Published Proofing Policy

1522       Make available the Identity Proofing Policy under which it verifies the identity of  
1523       applicants<sup>4</sup> in form, language, and media accessible to the declared community of Users.

1524       AL3\_ID\_POL#040           Adherence to Proofing Policy

1525       Perform all identity proofing strictly in accordance with its published Identity Proofing  
1526       Policy, through application of the procedures and processes set out in its Identity Proofing  
1527       Practice Statement.

1528

1529       **3.6.3.2 Identity Verification**

1530       The enterprise or specific service must:

---

<sup>4</sup> 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.

- 1531 AL3\_ID\_IDV#000 Identity Proofing classes
- 1532 a) include in its Service Definition at least one of the following classes of identity  
1533 proofing services, and;
- 1534 b) may offer any additional classes of identity proofing service it chooses, subject to  
1535 the nature and the entitlement of the CSP concerned;
- 1536 c) Fulfill the applicable assessment criteria according to its choice of identity  
1537 proofing service, i.e. conform to at least one of the criteria sets defined in:
- 1538 i) §3.6.3.2.1, “[In-Person Public Verification](#)”;
- 1539 ii) §3.6.3.2.2, “[Remote Public Verification](#)”;
- 1540 iii) §3.6.3.2.4, “[Affiliation Verification](#)”.
- 1541

1542 **3.6.3.2.1 In-Person Public Verification**

1543 A specific service that offers identity proofing to applicants with whom it has no previous  
1544 relationship must comply with the criteria in this section.

1545 The enterprise or specified service must:

- 1546 AL3\_ID\_IPV#010 Required evidence
- 1547 Ensure that the applicant is in possession of a primary Government Picture ID document  
1548 that bears a photographic image of the holder.

- 1549 AL3\_ID\_IPV#020 Evidence checks

1550 **Have in place and apply processes which ensure** that the presented document:

- 1551 a) appears to be a genuine document properly issued by the claimed issuing  
1552 authority and valid at the time of application;
- 1553 b) bears a photographic image of the holder that matches that of the applicant;
- 1554 c) **is electronically verified by a record check with the specified issuing  
1555 authority or through similar databases that:**
- 1556 i) **establishes the existence of such records with matching name and  
1557 reference numbers;**
- 1558 ii) **corroborates date of birth, current address of record, and other  
1559 personal information sufficient to ensure a unique identity;**
- 1560 d) provides all reasonable certainty that the identity exists and that it uniquely  
1561 identifies the applicant.
- 1562

1563 **3.6.3.2 Remote Public Verification**

1564 A specific service that offers remote identity proofing to applicants with whom it has no  
1565 previous relationship must comply with the criteria in this section.

1566 The enterprise or specified service must:

1567 AL3\_ID\_RPV#010 Required evidence

1568 Ensure that the applicant submits the references of and attests to current possession of a  
1569 primary Government Picture ID document, and one of:

- 1570 a) a second Government ID;
- 1571 b) an employee or student ID number;
- 1572 c) a financial account number (e.g., checking account, savings account, loan, or  
1573 credit card), or;
- 1574 d) a utility service account number (e.g., electricity, gas, or water) for an address  
1575 matching that in the primary document.

1576 Ensure that the applicant provides additional verifiable personal information that at a  
1577 minimum must include:

- 1578 e) a name that matches the referenced photo-ID;
- 1579 f) date of birth;
- 1580 g) current address or personal email address. In the case the user does not have email  
1581 address or does not wish to provide an email address a telephone contact is required.

1582 Additional information may be requested so as to ensure a unique identity, and alternative  
1583 information may be sought where the enterprise can show that it leads to at least the same  
1584 degree of certitude when verified.

1585

1586 AL3\_ID\_RPV#020 Evidence checks

1587 **Electronically verify by a record check against the provided identity references with**  
1588 **the specified issuing authorities/institutions or through similar databases:**

- 1589 a) the existence of such records with matching name and reference numbers;
- 1590 b) corroboration of date of birth, current address of record, **or personal email**  
1591 **address or telephone number**, and other personal information sufficient to  
1592 ensure a unique identity;
- 1593 c) **dynamic verification of personal information previously provided by or**  
1594 **likely to be known only by the applicant.**

1595

1596

1597 Confirm address of record by at least one of the following means:

- 1598 a) RA sends notice to an address of record confirmed in the records check and  
1599 receives a mailed or telephonic reply from applicant;  
1600 b) RA issues credentials in a manner that confirms the address of record supplied by  
1601 the applicant, for example by requiring applicant to enter on-line some  
1602 information from a notice sent to the applicant;  
1603 c) RA issues credentials in a manner that confirms ability of the applicant to receive  
1604 telephone communications at telephone number or email at email address  
1605 associated with the applicant in records. Any secret sent over an unprotected  
1606 channel shall be reset upon first use.  
1607

1608 Additional checks may be performed so as to establish the uniqueness of the claimed  
1609 identity, and alternative checks may be performed where the enterprise can show that they  
1610 lead to at least the same degree of certitude.

### 1611 **3.6.3.2.3 Current Relationship Verification**

1612 No stipulation.

1613

### 1614 **3.6.3.2.4 Affiliation Verification**

1615 A specific service that offers identity proofing to applicants on the basis of some form of  
1616 affiliation must comply with the criteria in this section to establish that affiliation and  
1617 with the previously stated requirements to verify the individual's identity.

1618 The enterprise or specified service must:

1619 AL3\_ID\_AFV#000 Meet preceding criteria

1620 Meet all the criteria set out above, under §3.6.3.2.2, "[Remote Public Verification](#)".

1621 AL3\_ID\_AFV#010 Required evidence

1622 Ensure that the applicant possesses:

- 1623 a) identification from the organization with which it is claiming affiliation;  
1624 b) agreement from the organization that the applicant may be issued a credential  
1625 indicating that an affiliation exists.

1626 AL3\_ID\_AFV#020 Evidence checks

1627 Have in place and apply processes which ensure that the presented documents:

- 1628 a) each appear to be a genuine document properly issued by the claimed issuing  
1629 authorities and valid at the time of application;  
1630 b) refer to an existing organization with a contact address;

- 1631 c) indicate that the applicant has some form of recognizable affiliation with the  
1632 organization;  
1633 d) appear to grant the applicant an entitlement to obtain a credential indicating an  
1634 affiliation with the organization.  
1635

### 1636 3.6.3.2.5 Secondary Verification

1637 In each of the above cases, the enterprise or specified service must also meet the  
1638 following criteria:

#### 1639 AL3\_ID\_SCV#010 Secondary checks

1640 Have in place additional measures (e.g., require additional documentary evidence, delay  
1641 completion while out-of-band checks are undertaken) to deal with any anomalous  
1642 circumstance that can reasonably be anticipated (e.g., a legitimate and recent change of  
1643 address that has yet to be established as the address of record).

### 1644 3.6.3.3 Verification Records

1645 The specific service must retain records of the identity proofing (verification) that it  
1646 undertakes and provide them to qualifying parties when so required.

1647 The enterprise or specified service must:

#### 1648 AL3\_ID\_VRC#010 Verification Records for Personal Applicants

1649 Log, taking account of all applicable legislative and policy obligations, a record of the  
1650 facts of the verification process **and the identity of the registrar**, including a reference  
1651 relating to the verification processes and the date and time of verification.

1652 **Guidance:** The facts of the verification process should include the specific record  
1653 information (source, unique reference, value/content) used in establishing the applicant's  
1654 identity, and will be determined by the specific processes used and documents accepted  
1655 by the CSP. The CSP need not retain these records itself if it uses a third-party service  
1656 which retains such records securely and to which the CSP has access when required, in  
1657 which case it must retain a record of the identity of the third-party service providing the  
1658 verification service or the location at which the (in-house) verification was performed.

#### 1659 AL3\_ID\_VRC#020 Verification Records for Affiliated Applicants

1660 In addition to the foregoing, log, taking account of all applicable legislative and policy  
1661 obligations, a record of the additional facts of the verification process must be performed.  
1662 At a minimum, records of identity information must include:

- 1663 a) the 'full name;  
1664 b) the subscriber's current address of record;  
1665 c) the subscriber's current telephone or email address of record;

- 1666 d) the subscriber's acknowledgement of issuing the subject with a credential;
- 1667 e) type, issuing authority, and reference number(s) of all documents checked in the
- 1668 identity proofing process;
- 1669 f) **where required, a telephone or email address for related contact and/or**
- 1670 **delivery of credentials/notifications.**

1671 AL3\_ID\_VRC#030 Record Retention

1672 Either retain, securely, the record of the verification/revocation process for the duration of  
1673 the subscriber account plus 7.5 years, or submit the same record to a client CSP that has  
1674 undertaken to retain the record for the requisite period or longer.

1675

1676

1677 **3.6.4 Assurance Level 4**

1678 Identity proofing at Assurance Level 4 requires the physical presence of the applicant in  
1679 front of the registration officer with photo ID or other readily verifiable biometric identity  
1680 information, as well as the requirements set out by the following criteria.

1681 **3.6.4.1 Policy**

1682 The specific service must show that it applies identity proofing policies and procedures  
1683 and that it retains appropriate records of identity proofing activities and evidence.

1684 The enterprise or specified service must:

1685 AL4\_ID\_POL#010 Unique service identity

1686 Ensure that a unique identity is attributed to the specific service, such that credentials  
1687 issued by it can be distinguishable from those issued by other services, including services  
1688 operated by the same enterprise.

1689 AL4\_ID\_POL#020 Unique subject identity

1690 Ensure that each applicant's identity is unique within the service's community of subjects  
1691 and uniquely associable with tokens and/or credentials issued to that identity.

1692 AL4\_ID\_POL#030 Published Proofing Policy

1693 Make available the Identity Proofing Policy under which it verifies the identity of  
1694 applicants<sup>5</sup> in form, language, and media accessible to the declared community of users.

1695 AL4\_ID\_POL#040 Adherence to Proofing Policy

1696 Perform all identity proofing strictly in accordance with its published Identity Proofing  
1697 Policy, through application of the procedures and processes set out in its Identity Proofing  
1698 Practice Statement.

1699

1700 **3.6.4.2 Identity Verification**

1701 The enterprise or specific service may:

---

<sup>5</sup> 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.



- 1702 AL4\_ID\_IDV#000 Identity Proofing classes
- 1703 **[Omitted] offer only face-to-face identity proofing service. Remote verification is not**  
1704 **allowed at this assurance level;**
- 1705
- 1706 The enterprise or specified service must:
- 1707 **3.6.4.2.1 In-Person Public Verification**
- 1708 AL4\_ID\_IPV#010 Required evidence
- 1709 Ensure that the applicant is in possession of:
- 1710 a) a primary Government Picture ID document that bears a photographic image of  
1711 the **holder and either:**
- 1712 i) **secondary Government Picture ID or an account number issued by a**  
1713 **regulated financial institution or;**
- 1714 ii) **two items confirming name, and address or email address, such as:**  
1715 **utility bill, professional license or membership, or other evidence of**  
1716 **equivalent standing. In the case the user does not have email address**  
1717 **or does not wish to provide an email address a telephone contact is**  
1718 **required.**
- 1719 AL4\_ID\_IPV#020 No stipulation
- 1720 AL4\_ID\_IPV#030 Evidence checks – primary ID
- 1721 **Ensure that the presented document:**
- 1722 a) **appears to be a genuine document properly issued by the claimed issuing**  
1723 **authority and valid at the time of application;**
- 1724 b) **bears a photographic image of the holder which matches that of the**  
1725 **applicant;**
- 1726 c) **is electronically verified by a record check with the specified issuing**  
1727 **authority or through similar databases that:**
- 1728 i) **establishes the existence of such records with matching name and**  
1729 **reference numbers;**
- 1730 ii) **corroborates date of birth, current address of record, and other**  
1731 **personal information sufficient to ensure a unique identity;**
- 1732 d) **provides all reasonable certainty, at AL4, that the identity exists and that it**  
1733 **uniquely identifies the applicant.**
- 1734 AL4\_ID\_IPV#040 Evidence checks – secondary ID
- 1735 **Ensure that the presented document meets the following conditions:**

- 1736 a) **If it is secondary Government Picture ID:**  
1737 i) **appears to be a genuine document properly issued by the claimed**  
1738 **issuing authority and valid at the time of application;**  
1739 ii) **bears a photographic image of the holder which matches that of the**  
1740 **applicant;**  
1741 iii) **states an address at which the applicant can be contacted.**  
1742 b) **If it is a financial institution account number, is verified by a record check**  
1743 **with the specified issuing authority or through similar databases that:**  
1744 i) **establishes the existence of such records with matching name and**  
1745 **reference numbers;**  
1746 ii) **corroborates date of birth, current address of record, and other**  
1747 **personal information sufficient to ensure a unique identity.**  
1748 c) **If it is two utility bills or equivalent documents:**  
1749 i) **each appears to be a genuine document properly issued by the**  
1750 **claimed issuing authority;**  
1751 ii) **corroborates current address of record or telephone number**  
1752 **sufficient to ensure a unique identity.**

1753 AL4\_ID\_IPV#050 Applicant knowledge checks

1754 **Where the applicant is unable to satisfy any of the above requirements, that the**  
1755 **applicant can provide a unique identifier, such as a Social Security Number (SSN),**  
1756 **that matches the claimed identity.**

1757

#### 1758 **3.6.4.2.2 Remote Public Verification**

1759 **Not permitted**

#### 1760 **3.6.4.2.3 Affiliation Verification**

1761 A specific service that offers identity proofing to applicants on the basis of some form of  
1762 affiliation must comply with the criteria in this section to establish that affiliation, in  
1763 addition to complying with the previously stated requirements for verifying the  
1764 individual's identity.

1765 The enterprise or specified service must:

1766 AL4\_ID\_AFV#000 Meet preceding criteria

1767 Meet all the criteria set out above, under §3.6.4.2.1, "[In-Person Public Verification](#)".

1768 AL4\_ID\_AFV#010 Required evidence

1769 Ensure that the applicant possesses:

1770 a) identification from the organization with which it is claiming affiliation;

1771 b) agreement from the organization that the applicant may be issued a credential  
1772 indicating that an affiliation exists.

1773 AL4\_ID\_AFV#020 Evidence checks

1774 Have in place and apply processes which ensure that the presented documents:

- 1775 a) each appear to be a genuine document properly issued by the claimed issuing  
1776 authorities and valid at the time of application;  
1777 b) refer to an existing organization with a contact address;  
1778 c) indicate that the applicant has some form of recognizable affiliation with the  
1779 organization;  
1780 d) appear to grant the applicant an entitlement to obtain a credential indicating an  
1781 affiliation with the organization.  
1782

#### 1783 **3.6.4.2.4 Secondary Verification**

1784 In each of the above cases, the enterprise or specified service must also meet the  
1785 following criteria:

1786 AL4\_ID\_SCV#010 Secondary checks

1787 Have in place additional measures (e.g., require additional documentary evidence, delay  
1788 completion while out-of-band checks are undertaken) to deal with any anomalous  
1789 circumstances that can reasonably be anticipated (e.g., a legitimate and recent change of  
1790 address that has yet to be established as the address of record).

1791

#### 1792 **3.6.4.3 Verification Records**

1793 The specific service must retain records of the identity proofing (verification) that it  
1794 undertakes and provide them to qualifying parties when so required.

1795 The enterprise or specified service must:

1796 AL4\_ID\_VRC#010 Verification Records for Personal Applicants

1797 Log, taking account of all applicable legislative and policy obligations, a record of the  
1798 facts of the verification process and the identity of the registrar, including a reference  
1799 relating to the verification processes and the date and time of verification **issued by a**  
1800 **trusted time-source.**

1801 **Guidance:** The facts of the verification process should include the specific record  
1802 information (source, unique reference, value/content) used in establishing the applicant's  
1803 identity, and will be determined by the specific processes used and documents accepted  
1804 by the CSP. The CSP need not retain these records itself if it uses a third-party service

1805 which retains such records securely and to which the CSP has access when required, in  
1806 which case it must retain a record of the identity of the third-party service providing the  
1807 verification service or the location at which the (in-house) verification was performed.

1808 AL4\_ID\_VRC#020 Verification Records for Affiliated Applicants

1809 In addition to the foregoing, log, taking account of all applicable legislative and policy  
1810 obligations, a record of the additional facts of the verification process must be performed.  
1811 At a minimum, records of identity information must include:

- 1812 a) the subscriber's full name;
- 1813 b) the subscriber's current address of record;
- 1814 c) the subscriber's current telephone or email address of record;
- 1815 d) the subscriber's authorization for issuing the subject a credential;
- 1816 e) type, issuing authority, and reference number(s) of all documents checked in the  
1817 identity proofing process;
- 1818 **f) a biometric record of each required representative of the affiliating**  
1819 **organization (e.g., a photograph, fingerprint, voice recording), as determined**  
1820 **by that organization's governance rules/charter.**

1821 AL4\_ID\_VRC#030 Record Retention

1822 Either retain, securely, the record of the verification/revocation process for the duration of  
1823 the subscriber account plus **10.5** years, or submit the record to a client CSP that has  
1824 undertaken to retain the record for the requisite period or longer.

1825

1826

1827 **3.6.5 Compliance Tables**

1828 Use the following tables to correlate criteria for a particular Assurance Level (AL) and  
1829 the evidence offered to support compliance.

1830 Service providers preparing for an assessment can use the table appropriate to the AL at  
1831 which they are seeking approval to correlate evidence with criteria or to justify non-  
1832 applicability (e.g., "specific service types not offered").

1833 Assessors can use the tables to record the steps in their assessment and their  
1834 determination of compliance or failure.

1835 **Table 3-5. ID-SAC - AL1 Compliance**

Clause	Description	Compliance
AL1_ID_POL#010	<a href="#">Unique service identity</a>	
AL1_ID_POL#020	<a href="#">Unique subject identity</a>	
AL1_ID_IPV#010	<a href="#">Required evidence</a>	
AL1_ID_IPV#020	<a href="#">Evidence checks</a>	
AL1_ID_RPV#010	<a href="#">Required evidence</a>	
AL1_ID_RPV#020	<a href="#">Evidence checks</a>	
AL1_ID_SCV#010	<a href="#">Secondary checks</a>	

1836

1837

1838

**Table 3-6. ID-SAC - AL2 Compliance**

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

1839

1840

1841

**Table 3-7. ID-SAC - AL3 compliance**

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

1842

1843

1844

**Table 3-8. ID-SAC - AL4 compliance**

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

1845

1846



## 1847 **3.7 Credential Management Service Assessment Criteria**

1848 The Service Assessment Criteria in this section establish requirements for the functional  
1849 conformity of credential management services and their providers at all ALs defined in  
1850 Section 2 and in the [Identity Assurance Framework: Levels of Assurance](#) document.

1851 These criteria are generally referred to elsewhere within IAF documentation as CM-SAC.

1852 The criteria are divided into five parts. Each part deals with a specific functional aspect  
1853 of the overall credential management process.

1854 This SAC must be used in conjunction with the Common Organizational SAC  
1855 (CO-SAC), described in Section 3.5, and, in addition, must either:

- 1856 • explicitly include the criteria of the Identity Proofing SAC ([ID-SAC]) described  
1857 in Section 3.6, or
- 1858 • rely upon the criteria of the ID-SAC [ID-SAC] being fulfilled by the use of a  
1859 Kantara-approved ID-proofing service.

### 1860 **3.7.1 Part A - Credential Operating Environment**

1861 The criteria in this part deal with the overall operational environment in which the  
1862 credential life-cycle management is conducted. The credential management service  
1863 assessment criteria must be used in conjunction with the Common Organizational criteria  
1864 described in Section 3.5. In addition, they must either explicitly include the identity  
1865 proofing service assessment criteria described in Section 3.6 or rely upon those criteria  
1866 being fulfilled by the use of a Kantara-approved identity proofing service.

1867 These criteria describe requirements for the overall operational environment in which  
1868 credential lifecycle management is conducted. The common organizational criteria  
1869 describe broad requirements. The criteria in this section describe implementation  
1870 specifics. Implementation depends on the AL. The procedures and processes required to  
1871 create a secure environment for management of credentials and the particular  
1872 technologies that are considered strong enough to meet the assurance requirements differ  
1873 considerably from level to level.

#### 1874 **3.7.1.1 Assurance Level 1**

1875 These criteria apply to PINs and passwords, as well as SAML assertions.

##### 1876 **3.7.1.1.1 Not used**

1877 No stipulation.

1878

##### 1879 **3.7.1.1.2 Security Controls**

1880 An enterprise and its specified service must:

- 1881 AL1\_CM\_CTR#010 No stipulation
- 1882 AL1\_CM\_CTR#020 Protocol threat risk assessment and controls
- 1883 Account for at least the following protocol threats and apply appropriate controls:
- 1884 a) password guessing, such that the resistance to an on-line guessing attack against a  
1885 selected user/password is at least 1 in  $2^{10}$  (1,024);
- 1886 b) message replay.
- 1887 AL1\_CM\_CTR#025 No stipulation
- 1888 AL1\_CM\_CTR#030 System threat risk assessment and controls
- 1889 Account for the following system threats and apply appropriate controls:
- 1890 a) the introduction of malicious code;
- 1891 b) compromised authentication arising from insider action;
- 1892 c) out-of-band attacks by other users and system operators (e.g., the ubiquitous  
1893 shoulder-surfing);
- 1894 d) spoofing of system elements/applications;
- 1895 e) malfeasance on the part of subscribers and subjects.
- 1896
- 1897 **3.7.1.1.3 Storage of Long-term Secrets**
- 1898 AL1\_CM\_STS#010 Withdrawn
- 1899 Withdrawn (AL1\_CO\_SCO#020 (a) & (b) enforce this requirement)
- 1900
- 1901 **3.7.1.1.4 Not used**
- 1902 **3.7.1.1.5 Subject Options**
- 1903 AL1\_CM\_OPN#010 Withdrawn
- 1904 Withdrawn – see AL1\_CM\_RNR#010.
- 1905

1906 **3.7.1.2 Assurance Level 2**

1907 These criteria apply to passwords, as well as acceptable SAML assertions.

1908 **3.7.1.2.1 Credential Policy and Practices**

1909 These criteria apply to the policy and practices under which credentials are managed.

1910 An enterprise and its specified service must:

1911 AL2\_CM\_CPP#010 Credential Policy and Practice Statement

1912 **Include in its Service Definition a description of the policy against which it issues**  
1913 **credentials and the corresponding practices it applies in their management. At a**  
1914 **minimum, the Credential Policy and Practice Statement must specify:**

- 1915 a) **if applicable, any OIDs related to the Practice and Policy Statement;**  
1916 b) **how users may subscribe to the service/apply for credentials and how users'**  
1917 **credentials will be delivered to them;**  
1918 c) **how subscribers acknowledge receipt of tokens and credentials and what**  
1919 **obligations they accept in so doing (including whether they consent to**  
1920 **publication of their details in credential status directories);**  
1921 d) **how credentials may be renewed, modified, revoked, and suspended,**  
1922 **including how requestors are authenticated or their identity re-proven;**  
1923 e) **what actions a subscriber must take to terminate a subscription;**  
1924 f) **how records are retained and archived.**

1925 AL2\_CM\_CPP#020 No stipulation

1926 AL2\_CM\_CPP#030 Management Authority

1927 **Have a nominated management body with authority and responsibility for**  
1928 **approving the Credential Policy and Practice Statement and for its implementation.**

1929

1930 **3.7.1.2.2 Security Controls**

1931 An enterprise and its specified service must:

1932 AL2\_CM\_CTR#010 Secret revelation

1933 **Withdrawn.**

1934 AL2\_CM\_CTR#020 Protocol threat risk assessment and controls

1935 Account for at least the following protocol threats **in its risk assessment** and apply  
1936 **[omitted] controls that reduce them to acceptable risk levels:**

- 1937 a) password guessing, such that the resistance to an on-line guessing attack against a  
1938 selected user/password is at least 1 in  $2^{14}$  (**16,384**);  
1939 b) message replay, **showing that it is impractical**;  
1940 c) **eavesdropping, showing that it is impractical.**

1941 AL2\_CM\_CTR#025 Permitted authentication protocols

1942 **Permit only the following authentication protocols:**

- 1943 a) **tunneled password;**  
1944 b) **zero knowledge-base password;**  
1945 c) **SAML assertions.**

1946 AL2\_CM\_CTR#028 One-time passwords

1947 **Use only one-time passwords which:**

- 1948 a) **are generated using an approved block-cipher or hash function to combine a**  
1949 **symmetric key, stored on the device, with a nonce;**  
1950 b) **derive the nonce from a date and time, or a counter generated on the device;**  
1951 c) **have a limited lifetime, in the order of minutes.**  
1952

1953 AL2\_CM\_CTR#030 System threat risk assessment and controls

1954 Account for the following system threats **in its risk assessment** and apply **[omitted]**  
1955 controls **that reduce them to acceptable risk levels:**

- 1956 a) the introduction of malicious code;  
1957 b) compromised authentication arising from insider action;  
1958 c) out-of-band attacks by both users and system operators (e.g., the ubiquitous  
1959 shoulder-surfing);  
1960 d) spoofing of system elements/applications;  
1961 e) malfeasance on the part of subscribers and subjects;  
1962 f) **intrusions leading to information theft.**

1963 AL2\_CM\_CTR#040 Specified Service's Key Management

1964 **Specify and observe procedures and processes for the generation, storage, and**  
1965 **destruction of its own cryptographic keys used for securing the specific service's**  
1966 **assertions and other publicized information. At a minimum, these should address:**

- 1967 a) **the physical security of the environment;**  
1968 b) **access control procedures limiting access to the minimum number of**  
1969 **authorized personnel;**  
1970 c) **public-key publication mechanisms;**  
1971 d) **application of controls deemed necessary as a result of the service's risk**  
1972 **assessment;**

- 1973 e) **destruction of expired or compromised private keys in a manner that**  
1974 **prohibits their retrieval, or their archival in a manner that prohibits their**  
1975 **reuse;**  
1976 f) **applicable cryptographic module security requirements, quoting FIPS 140-2**  
1977 **[FIPS140-2] or equivalent, as established by a recognized national technical**  
1978 **authority.**  
1979

1980 **3.7.1.2.3 Storage of Long-term Secrets**

1981 AL2\_CM\_STS#010 Withdrawn

1982 Withdrawn (AL2\_CO\_SCO#020 (a) & (b) enforce this requirement).

1983

1984 **3.7.1.2.4 Security-Relevant Event (Audit) Records**

1985 **3.7.1.2.5 No stipulation**

1986 AL2\_CM\_OPN#010 Withdrawn

1987 Withdrawn – see AL2\_CM\_RNR#010.

1988

1989

1990 **3.7.1.3 Assurance Level 3**

1991 These criteria apply to one-time password devices and soft crypto applications protected  
1992 by passwords or biometric controls, as well as cryptographically-signed SAML  
1993 assertions.

1994 **3.7.1.3.1 Credential Policy and Practices**

1995 These criteria apply to the policy and practices under which credentials are managed.

1996 An enterprise and its specified service must:

1997 AL3\_CM\_CPP#010 Credential Policy and Practice Statement

1998 Include in its Service Definition a full description of the policy against which it issues  
1999 credentials and the corresponding practices it applies in their issuance. At a minimum,  
2000 the Credential Policy and Practice Statement must specify:

- 2001 a) if applicable, any OIDs related to the Credential Policy and Practice Statement;  
2002 b) how users may subscribe to the service/apply for credentials and how the users'  
2003 credentials will be delivered to them;  
2004 c) how subscribers acknowledge receipt of tokens and credentials and what  
2005 obligations they accept in so doing (including whether they consent to publication  
2006 of their details in credential status directories);  
2007 d) how credentials may be renewed, modified, revoked, and suspended, including  
2008 how requestors are authenticated or their identity proven;  
2009 e) what actions a subscriber must take to terminate a subscription;  
2010 f) how records are retained and archived.

2011 AL3\_CM\_CPP#020 No stipulation

2012 AL3\_CM\_CPP#030 Management Authority

2013 Have a nominated or appointed high-level management body with authority and  
2014 responsibility for approving the Certificate Policy and Certification Practice Statement,  
2015 including ultimate responsibility for their proper implementation.

2016

2017 **3.7.1.3.2 Security Controls**

2018 AL3\_CM\_CTR#010 No stipulation

2019 AL3\_CM\_CTR#020 Protocol threat risk assessment and controls

2020 Account for at least the following protocol threats in its risk assessment and apply  
2021 controls that reduce them to acceptable risk levels:

- 2022 a) password guessing, such that the resistance to an on-line guessing attack against a  
2023 selected user/password is at least 1 in  $2^{14}$  **(16,384)**;  
2024 b) message replay, showing that it is impractical;  
2025 c) eavesdropping, showing that it is impractical;  
2026 **d) relying party (verifier) impersonation, showing that it is impractical;**  
2027 **e) man-in-the-middle attack, showing that it is impractical.**

2028 **The above list shall not be considered to be a complete list of threats to be addressed**  
2029 **by the risk assessment.**

2030 AL3\_CM\_CTR#025 Permitted authentication protocols

2031 For non-PKI credentials, permit only the following authentication protocols:

- 2032 a) tunneled password;  
2033 b) zero knowledge-base password;  
2034 c) SAML assertions.

2035 AL3\_CM\_CTR#030 System threat risk assessment and controls

2036 Account for the following system threats in its risk assessment and apply controls that  
2037 reduce them to acceptable risk levels:

- 2038 a) the introduction of malicious code;  
2039 b) compromised authentication arising from insider action;  
2040 c) out-of-band attacks by both users and system operators (e.g., shoulder-surfing);  
2041 d) spoofing of system elements/applications;  
2042 e) malfeasance on the part of subscribers and subjects;  
2043 f) intrusions leading to information theft.

2044 The above list shall not be considered to be a complete list of threats to be addressed by  
2045 the risk assessment.

2046 AL3\_CM\_CTR#040 Specified Service's Key Management

2047 Specify and observe procedures and processes for the generation, storage, and destruction  
2048 of its own cryptographic keys used for securing the specific service's assertions and other  
2049 publicized information. At a minimum, these should address:

- 2050 a) the physical security of the environment;  
2051 b) access control procedures limiting access to the minimum number of authorized  
2052 personnel;  
2053 c) public-key publication mechanisms;  
2054 d) application of controls deemed necessary as a result of the service's risk  
2055 assessment;  
2056 e) destruction of expired or compromised private keys in a manner that prohibits  
2057 their retrieval or their archival in a manner that prohibits their reuse;

2058 f) applicable cryptographic module security requirements, quoting FIPS 140-2  
2059 [FIPS140-2] or equivalent, as established by a recognized national technical  
2060 authority.  
2061

### 2062 **3.7.1.3.3 Storage of Long-term Secrets**

2063 An enterprise and its specified service must:

2064 AL3\_CM\_STS#010            Withdrawn

2065 Withdrawn (AL3\_CO\_SCO#020 (a) & (b) enforce this requirement).

2066 AL3\_CM\_STS#020            Stored Secret Encryption

2067 Encrypt such shared secret files so that:

- 2068 a) the encryption key for the shared secret file is encrypted under a key held in a  
2069 FIPS 140-2 [FIPS140-2] Level 2 or higher validated hardware or software  
2070 cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module, or  
2071 equivalent, as established by a recognized national technical authority;
- 2072 b) the shared secret file is decrypted only as immediately required for an  
2073 authentication operation;
- 2074 c) shared secrets are protected as a key within the boundary of a FIPS 140-2 Level 2  
2075 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or  
2076 4 cryptographic module and are not exported from the module in plain text, or  
2077 equivalent, as established by a recognized national technical authority;
- 2078 d) shared secrets are split by an "*n from m*" cryptographic secret sharing method.  
2079

### 2080 **3.7.1.3.4 Security-relevant Event (Audit) Records**

2081 These criteria describe the need to provide an auditable log of all events that are pertinent  
2082 to the correct and secure operation of the service. The common organizational criteria  
2083 applying to provision of an auditable log of all security-related events pertinent to the  
2084 correct and secure operation of the service must also be considered carefully. These  
2085 criteria carry implications for credential management operations.

2086 In the specific context of a certificate management service, an enterprise and its specified  
2087 service must:

2088 AL3\_CM\_SER#010            Security event logs

2089 Ensure that such audit records include:

- 2090 a) the identity of the point of registration (irrespective of whether internal or  
2091 outsourced);



- 2092 b) generation of the subscriber's keys or the evidence that the subscriber was in  
2093 possession of both parts of their own key-pair;  
2094 c) generation of the subscriber's certificate;  
2095 d) dissemination of the subscriber's certificate;  
2096 e) any revocation or suspension associated with the subscriber's certificate.  
2097

2098 **3.7.1.3.5 Subject options**

2099 AL3\_CM\_OPN#010 Changeable PIN/Password

2100 Withdrawn – see AL3\_CM\_RNR#010.

2101

2102 **3.7.1.4 Assurance Level 4**

2103 These criteria apply exclusively to cryptographic technology deployed through a Public  
2104 Key Infrastructure. This technology requires hardware tokens protected by password or  
2105 biometric controls. No other forms of credential are permitted at AL4.

2106 **3.7.1.4.1 Certification Policy and Practices**

2107 These criteria apply to the policy and practices under which certificates are managed.

2108 An enterprise and its specified service must:

2109 AL4\_CM\_CPP#010 No stipulation

2110 AL4\_CM\_CPP#020 Certificate Policy/Certification Practice Statement

2111 **Include in its Service Definition its full Certificate Policy and the corresponding**  
2112 **Certification and Practice Statement. The Certificate Policy and Certification**  
2113 **Practice Statement must conform to IETF RFC 3647 (2003-11) [RFC 3647] in their**  
2114 **content and scope or be demonstrably consistent with the content or scope of that**  
2115 **RFC. At a minimum, the Certificate Policy must specify:**

- 2116 a) **applicable OIDs for each certificate type issued;**  
2117 b) **how users may subscribe to the service/apply for certificates, and how**  
2118 **certificates will be issued to them;**  
2119 c) **if users present their own keys, how they will be required to demonstrate**  
2120 **possession of the private key;**  
2121 d) **if users' keys are generated for them, how the private keys will be delivered**  
2122 **to them;**  
2123 e) **how subscribers acknowledge receipt of tokens and credentials and what**  
2124 **obligations they accept in so doing (including whether they consent to**  
2125 **publication of their details in certificate status directories);**  
2126 f) **how certificates may be renewed, re-keyed, modified, revoked, and**  
2127 **suspended, including how requestors are authenticated or their identity**  
2128 **proven;**  
2129 g) **what actions a subscriber must take to terminate their subscription.**

2130 AL4\_CM\_CPP#030 Management Authority

2131 Have a nominated or appointed high-level management body with authority and  
2132 responsibility for approving the Certificate Policy and Certification Practice Statement,  
2133 including ultimate responsibility for their proper implementation.

2134

2135 **3.7.1.4.2 Security Controls**

2136 An enterprise and its specified service must:

- 2137 AL4\_CM\_CTR#010 No stipulation
- 2138 AL4\_CM\_CTR#020 Protocol threat risk assessment and controls
- 2139 Account for at least the following protocol threats in its risk assessment and apply  
2140 controls that reduce them to acceptable risk levels:
- 2141 a) password guessing, showing that there is sufficient entropy;  
2142 b) message replay, showing that it is impractical;  
2143 c) eavesdropping, showing that it is impractical;  
2144 d) relying party (verifier) impersonation, showing that it is impractical;  
2145 e) man-in-the-middle attack, showing that it is impractical;  
2146 **f) session hijacking, showing that it is impractical.**
- 2147 The above list shall not be considered to be a complete list of threats to be addressed by  
2148 the risk assessment.
- 2149 AL4\_CM\_CTR#025 No stipulation
- 2150 AL4\_CM\_CTR#030 System threat risk assessment and controls
- 2151 Account for the following system threats in its risk assessment and apply controls that  
2152 reduce them to acceptable risk levels:
- 2153 a) the introduction of malicious code;  
2154 b) compromised authentication arising from insider action;  
2155 c) out-of-band attacks by both users and system operators (e.g., shoulder-surfing);  
2156 d) spoofing of system elements/applications;  
2157 e) malfeasance on the part of subscribers and subjects;  
2158 f) intrusions leading to information theft.
- 2159 The above list shall not be considered to be a complete list of threats to be addressed by  
2160 the risk assessment.
- 2161 AL4\_CM\_CTR#040 Specified Service's Key Management
- 2162 Specify and observe procedures and processes for the generation, storage, and destruction  
2163 of its own cryptographic keys used for securing the specific service's assertions and other  
2164 publicized information. At a minimum, these should address:
- 2165 a) the physical security of the environment;  
2166 b) access control procedures limiting access to the minimum number of authorized  
2167 personnel;  
2168 c) public-key publication mechanisms;  
2169 d) application of controls deemed necessary as a result of the service's risk  
2170 assessment;

- 2171 e) destruction of expired or compromised private keys in a manner that prohibits  
2172 their retrieval, or their archival in a manner which prohibits their reuse;  
2173 f) applicable cryptographic module security requirements, quoting FIPS 140-2  
2174 [FIPS140-2] or equivalent, as established by a recognized national technical  
2175 authority.  
2176

#### 2177 **3.7.1.4.3 Storage of Long-term Secrets**

2178 The enterprise and its specified service must meet the following criteria:

2179 AL4\_CM\_STS#010 Stored Secrets

- 2180 a) Withdrawn (AL4\_CO\_SCO#020 (a) & (b) enforce this requirement)  
2181 b) **apply discretionary access controls that limit access to trusted administrators**  
2182 **and to those applications that require access.**

2183 AL4\_CM\_STS#020 Stored Secret Encryption

2184 Encrypt such [omitted] secret files so that:

- 2185 a) the encryption key for the [omitted] secret file is encrypted under a key held in a  
2186 FIPS 140-2 [FIPS140-2] Level 2 or higher validated hardware cryptographic  
2187 module or any FIPS 140-2 Level 3 or 4 cryptographic module, or equivalent, as  
2188 established by a recognized national technical authority;  
2189 b) the [omitted] secret file is decrypted only as immediately required for a key  
2190 recovery operation;  
2191 c) [omitted] secrets are protected as a key within the boundary of a FIPS 140-2  
2192 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2  
2193 Level 3 or 4 cryptographic module and are not exported from the module in  
2194 plaintext, or equivalent, as established by a recognized national technical  
2195 authority;  
2196 d) escrowed secrets are split by an "n from m" cryptographic secret **storing** method.  
2197

#### 2198 **3.7.1.4.4 Security-relevant Event (Audit) Records**

2199 These criteria describe the need to provide an auditable log of all events that are pertinent  
2200 to the correct and secure operation of the service. The common organizational criteria  
2201 relating to the recording of all security-related events must also be considered carefully.  
2202 These criteria carry implications for credential management operations.

2203 In the specific context of a certificate management service, an enterprise and its specified  
2204 service must:

- 2205 AL4\_CM\_SER#010 Security event logs
- 2206 Ensure that such audit records include:
- 2207 a) the identity of the point of registration (irrespective of whether internal or  
2208 outsourced);
- 2209 b) generation of the subscriber's keys or evidence that the subscriber was in  
2210 possession of both parts of the key-pair;
- 2211 c) generation of the subscriber's certificate;
- 2212 d) dissemination of the subscriber's certificate;
- 2213 e) any revocation or suspension associated with the subscriber's credential.  
2214

2215 **3.7.1.4.5 Subject Options**

- 2216 AL4\_CM\_OPN#010 Changeable PIN/Password
- 2217 Withdrawn – see AL4\_CM\_RNR#010.
- 2218

2219           **3.7.2 Part B - Credential Issuing**

2220       These criteria apply to the verification of the identity of the subject of a credential and  
2221       with token strength and credential delivery mechanisms. They address requirements  
2222       levied by the use of various technologies to achieve the appropriate AL<sup>6</sup>. These criteria  
2223       include by reference all applicable criteria in Section 3.6.

2224       **3.7.2.1 Assurance Level 1**

2225       **3.7.2.1.1 Identity Proofing**

2226       These criteria determine how the enterprise shows compliance with the criteria for  
2227       fulfilling identity proofing functions.

2228       The enterprise and its specified service must:

2229       AL1\_CM\_IDP#010           Self-managed Identity Proofing

2230       If the enterprise assumes direct responsibility for identity proofing functions, show, by  
2231       direct inclusion, compliance with all applicable identity proofing service assessment  
2232       criteria<sup>7</sup> (**ID-SAC**) for AL1 or higher.

2233       AL1\_CM\_IDP#020           Kantara-Recognized outsourced service

2234       If the enterprise outsources responsibility for identity proofing functions and uses a  
2235       service already Kantara-Recognized, show that the service in question has been approved  
2236       at AL1 or higher.

2237       AL1\_CM\_IDP#030           Non-recognized outsourced service

2238       If the enterprise outsources responsibility for identity proofing functions, ensure that each  
2239       provider of such a service demonstrates compliance with all applicable identity proofing  
2240       service assessment criteria for AL1 or higher, and that the enterprise, itself, has in place  
2241       controls to ensure the continued fulfillment of those criteria by the provider to which the  
2242       functions have been outsourced.

2243       AL1\_CM\_IDP#040           Revision to subscriber information

2244       Provide a means for subscribers to amend their stored information after registration.

2245

---

<sup>6</sup> Largely driven by the guidance in NIST SP 800-63 [[NIST800-63](#)].

<sup>7</sup> 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.

- 2246 **3.7.2.1.2 Credential Creation**
- 2247 These criteria address the requirements for creation of credentials that can only be used at  
2248 AL1. Any credentials/tokens that comply with the criteria stipulated for AL2 and higher  
2249 are acceptable at AL1.
- 2250 An enterprise and its specified service must:
- 2251 AL1\_CM\_CRN#010          Authenticated Request
- 2252 Only accept a request to generate a credential and bind it to an identity if the source of the  
2253 request can be authenticated as being authorized to perform identity proofing at AL1 or  
2254 higher.
- 2255 AL1\_CM\_CRN#020          No stipulation
- 2256 AL1\_CM\_CRN#030          Credential uniqueness
- 2257 Allow the subscriber to select a credential (e.g., UserID) that is verified to be unique  
2258 within the specified service's community and assigned uniquely to a single identity  
2259 subject.
- 2260 **3.7.2.1.3 Not used**
- 2261 **3.7.2.1.4 Not used**
- 2262
- 2263

2264 **3.7.2.2 Assurance Level 2**

2265 **3.7.2.2.1 Identity Proofing**

2266 These criteria determine how the enterprise shows compliance with the criteria for  
2267 fulfilling identity proofing functions.

2268 The enterprise and its specified service must:

2269 AL2\_CM\_IDP#010 Self-managed Identity Proofing

2270 If the enterprise assumes direct responsibility for identity proofing functions, show, by  
2271 direct inclusion, compliance with all applicable identity proofing service assessment  
2272 criteria ([\[ID-SAC\]](#)) for AL2 or higher.

2273 AL2\_CM\_IDP#020 Kantara-Recognized outsourced service

2274 If the enterprise outsources responsibility for identity proofing functions and uses a  
2275 service already Kantara-Recognized, show that the service in question has been approved  
2276 at AL2 or higher **and that its approval has at least six months of remaining validity.**

2277 AL2\_CM\_IDP#030 Non- Kantara-Recognized outsourced service

2278 If the enterprise outsources responsibility for identity proofing functions, ensure that each  
2279 provider of such a service demonstrates compliance with all applicable identity proofing  
2280 service assessment criteria for AL2 or higher, and that the enterprise, itself, has in place  
2281 controls to ensure the continued fulfillment of those criteria by the provider to which the  
2282 functions have been outsourced.

2283 AL2\_CM\_IDP#040 Revision to subscriber information

2284 Provide a means for subscribers to **securely** amend their stored information after  
2285 registration, **either by re-proving their identity, as in the initial registration process,**  
2286 **or by using their credentials to authenticate their revision.**

2287

2288 **3.7.2.2.2 Credential Creation**

2289 These criteria define the requirements for creation of credentials whose highest use is at  
2290 AL2. Credentials/tokens that comply with the criteria stipulated at AL3 and higher are  
2291 also acceptable at AL2 and below.

2292 Note, however, that a token and credential required by a higher AL but created according  
2293 to these criteria may not necessarily provide that higher level of assurance for the claimed  
2294 identity of the subscriber. Authentication can only be provided at the assurance level at  
2295 which the identity is proven.



- 2296 An enterprise and its specified service must:
- 2297 AL2\_CM\_CRN#010 Authenticated Request
- 2298 Only accept a request to generate a credential and bind it to an identity if the source of the  
2299 request can be authenticated, **i.e., Registration Authority (RA), as being authorized to**  
2300 **perform identity proofing at AL2 or higher.**
- 2301 AL2\_CM\_CRN#020 Unique identity
- 2302 **Ensure that the identity which relates to a specific applicant is unique within the**  
2303 **specified service, including identities previously used and that are now cancelled,**  
2304 **other than its re-assignment to the same applicant.**
- 2305 Guidance: This requirement is intended to prevent identities that may exist in a Relying  
2306 Party's access control list from possibly representing a different physical person.
- 2307 AL2\_CM\_CRN#030 Credential uniqueness
- 2308 Allow the subscriber to select a credential (e.g., UserID) that is verified to be unique  
2309 within the specified service's community and assigned uniquely to a single identity  
2310 subject.
- 2311 AL2\_CM\_CRN#035 Convey credential
- 2312 **Be capable of conveying the unique identity information associated with a credential**  
2313 **to Verifiers and Relying Parties.**
- 2314 AL2\_CM\_CRN#040 Password strength
- 2315 **Only allow passwords that, over the life of the password, have resistance to an on-**  
2316 **line guessing attack against a selected user/password of at least 1 in  $2^{14}$  (16,384),**  
2317 **accounting for state-of-the-art attack strategies, and at least 10 bits of min-entropy<sup>8</sup>.**
- 2318 AL2\_CM\_CRN#050 One-time password strength
- 2319 **Only allow password tokens that have a resistance to online guessing attack against**  
2320 **a selected user/password of at least 1 in  $2^{14}$  (16,384), accounting for state-of-the-art**  
2321 **attack strategies, and at least 10 bits of min-entropy<sup>8</sup>.**

---

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

- 2322 AL2\_CM\_CRN#060 Software cryptographic token strength
- 2323 **Ensure that software cryptographic keys stored on general-purpose devices:**
- 2324 a) **are protected by a key and cryptographic protocol that are evaluated against**
- 2325 **FIPS 140-2 [[FIPS140-2](#)] Level 2, or equivalent, as established by a recognized**
- 2326 **national technical authority;**
- 2327 b) **require password or biometric activation by the subscriber or employ a**
- 2328 **password protocol when being used for authentication.**
- 2329 AL2\_CM\_CRN#070 Hardware token strength
- 2330 **Ensure that hardware tokens used to store cryptographic keys:**
- 2331 a) **employ a cryptographic module that is evaluated against FIPS 140-2**
- 2332 **[[FIPS140-2](#)] Level 1 or higher, or equivalent, as established by a recognized**
- 2333 **national technical authority;**
- 2334 b) **require password or biometric activation by the subscriber or also employ a**
- 2335 **password when being used for authentication.**
- 2336 AL2\_CM\_CRN#080 No stipulation
- 2337 AL2\_CM\_CRN#090 Nature of subject
- 2338 **Record the nature of the subject of the credential (which must correspond to the**
- 2339 **manner of identity proofing performed), i.e., physical person, a named person acting**
- 2340 **on behalf of a corporation or other legal entity, corporation or legal entity, or**
- 2341 **corporate machine entity, in a manner that can be unequivocally associated with the**
- 2342 **credential and the identity that it asserts. If the credential is based upon a**
- 2343 **pseudonym this must be indicated in the credential.**
- 2344 **3.7.2.2.3 Subject Key Pair Generation**
- 2345 No stipulation.
- 2346 **3.7.2.2.4 Credential Delivery**
- 2347 An enterprise and its specified service must:
- 2348 AL2\_CM\_CRD#010 Notify Subject of Credential Issuance
- 2349 **Notify the subject of the credential's issuance and, if necessary, confirm the**
- 2350 **Subject's contact information by:**
- 2351 a) **sending notice to the address of record confirmed during identity proofing**
- 2352 **or;**
- 2353 b) **issuing the credential(s) in a manner that confirms the address of record**
- 2354 **supplied by the applicant during identity proofing or;**

2355 c) **issuing the credential(s) in a manner that confirms the ability of the applicant**  
2356 **to receive telephone communications at a fixed-line telephone number or**  
2357 **postal address supplied by the applicant during identity proofing.**

2358 AL2\_CM\_CRD#015 Confirm Applicant's identity (in person)

2359 **Prior to delivering the credential, require the Applicant to identify themselves in**  
2360 **person in any new electronic transaction (beyond the first transaction or encounter)**  
2361 **by either:**

2362 (a) **using a secret which was established during a prior transaction or**  
2363 **encounter, or sent to the Applicant's phone number, email address, or**  
2364 **physical address of record, or;**

2365 (b) **through the use of a biometric that was recorded during a prior**  
2366 **encounter.**

2367 AL2\_CM\_CRD#016 Confirm Applicant's identity (remotely)

2368 **Prior to delivering the credential, require the Applicant to identify themselves in any**  
2369 **new electronic transaction (beyond the first transaction or encounter) by presenting**  
2370 **a temporary secret which was established during a prior transaction or encounter,**  
2371 **or sent to the Applicant's phone number, email address, or physical address of**  
2372 **record.**

2373

2374

2375 **3.7.2.3 Assurance Level 3**

2376 **3.7.2.3.1 Identity Proofing**

2377 These criteria in this section determine how the enterprise shows compliance with the  
2378 criteria for fulfilling identity proofing functions.

2379 The enterprise and its specified service must:

2380 AL3\_CM\_IDP#010 Self-managed Identity Proofing

2381 If the enterprise assumes direct responsibility for identity proofing functions, show, by  
2382 direct inclusion, compliance with all applicable identity proofing service assessment  
2383 criteria for **AL3 or AL4**.

2384 AL3\_CM\_IDP#020 Kantara-Recognized outsourced service

2385 If the enterprise outsources responsibility for identity proofing functions and uses a  
2386 service already Kantara-Recognized, show that the service in question has been certified  
2387 at **AL3 or AL4** and that its approval has at least six months of remaining validity.

2388 AL3\_CM\_IDP#030 Non- Kantara-Recognized outsourced service

2389 **Not use any non- Kantara-Recognized services for identity proofing unless they can**  
2390 **be demonstrated to have satisfied equivalently rigorous requirements established by**  
2391 **another scheme recognized by IAWG.**

2392 AL3\_CM\_IDP#040 Revision to subscriber information

2393 Provide a means for subscribers to securely amend their stored information after  
2394 registration, either by re-proving their identity as in the initial registration process or by  
2395 using their credentials to authenticate their revision. **Successful revision must, where**  
2396 **necessary, instigate the re-issuance of the credential.**

2397

2398 **3.7.2.3.2 Credential Creation**

2399 These criteria define the requirements for creation of credentials whose highest use is  
2400 AL3. Any credentials/tokens that comply with the criteria stipulated at AL4 are also  
2401 acceptable at AL3 and below.

2402 Note, however, that a token and credential type required by a higher AL but created  
2403 according to these criteria may not necessarily provide that higher level of assurance for  
2404 the claimed identity of the subscriber. Authentication can only be provided at the  
2405 assurance level at which the identity is proven.

2406 An enterprise and its specified service must:

- 2407 AL3\_CM\_CRN#010 Authenticated Request
- 2408 Only accept a request to generate a credential and bind it to an identity if the source of the  
2409 request, i.e., Registration Authority (RA), can be authenticated as being authorized to  
2410 perform identity proofing at AL3 or higher.
- 2411 AL3\_CM\_CRN#020 Unique identity
- 2412 Ensure that the identity which relates to a specific applicant is unique within the specified  
2413 service, including identities previously used and that are now cancelled other than its re-  
2414 assignment to the same applicant.
- 2415 **Guidance:** This requirement is intended to prevent identities that may exist in a Relying  
2416 Party's access control lists from possibly representing a different physical person.
- 2417
- 2418 AL3\_CM\_CRN#030 Credential uniqueness
- 2419 Allow the subscriber to select a credential (e.g., UserID) that is verified to be unique  
2420 within the specified service's community and assigned uniquely to a single identity  
2421 subject.
- 2422 AL3\_CM\_CRN#035 Convey credential
- 2423 Be capable of conveying the unique identity information associated with a credential to  
2424 Verifiers and Relying Parties.
- 2425 AL3\_CM\_CRN#040 PIN/Password strength
- 2426 **Not use PIN/password tokens.**
- 2427 AL3\_CM\_CRN#050 One-time password strength
- 2428 Only allow one-time password tokens that:
- 2429 a) **depend on a symmetric key stored on a personal hardware device evaluated**  
2430 **against FIPS 140-2 [FIPS140-2] Level 1 or higher, or equivalent, as**  
2431 **established by a recognized national technical authority;**
- 2432 b) **permit at least 10<sup>6</sup> possible password values;**
- 2433 c) **require password or biometric activation by the subscriber.**
- 2434 AL3\_CM\_CRN#060 Software cryptographic token strength
- 2435 Ensure that software cryptographic keys stored on general-purpose devices:

- 2436 a) are protected by a key and cryptographic protocol that are evaluated against  
2437 FIPS 14-2 [FIPS140-2] Level 2, or equivalent, as established by a recognized  
2438 national technical authority;  
2439 b) require password or biometric activation by the subscriber or employ a password  
2440 protocol when being used for authentication.

2441 AL3\_CM\_CRN#070 Hardware token strength

2442 Ensure that hardware tokens used to store cryptographic keys:

- 2443 a) employ a cryptographic module that is evaluated against FIPS 140-2 [FIPS140-2]  
2444 Level 1 or higher, or equivalent, as established by a recognized national technical  
2445 authority;  
2446 b) require password or biometric activation by the subscriber or also employ a  
2447 password when being used for authentication.

2448 AL3\_CM\_CRN#080 Binding of key

2449 **If the specified service generates the subject's key pair, that the key generation**  
2450 **process securely and uniquely binds that process to the certificate generation and**  
2451 **maintains at all times the secrecy of the private key, until it is accepted by the**  
2452 **subject.**

2453 AL3\_CM\_CRN#090 Nature of subject

2454 Record the nature of the subject of the credential (which must correspond to the manner  
2455 of identity proofing performed), i.e., private person, a named person acting on behalf of a  
2456 corporation or other legal entity, corporation or legal entity, or corporate machine entity,  
2457 in a manner that can be unequivocally associated with the credential and the identity that  
2458 it asserts. [Omitted]

2459

### 2460 **3.7.2.3.3 Subject Key Pair Generation**

2461 An enterprise and its specified service must:

2462 AL3\_CM\_SKP#010 Key generation by Specified Service

2463 **If the specified service generates the subject's keys:**

- 2464 a) use a FIPS 140-2 [FIPS140-2] compliant algorithm, or equivalent, as  
2465 established by a recognized national technical authority, that is recognized as  
2466 being fit for the purposes of the service;  
2467 b) only create keys of a key length and for use with a FIPS 140-2 [FIPS140-2]  
2468 compliant public key algorithm, or equivalent, as established by a recognized

- 2469            **national technical authority, recognized as being fit for the purposes of the**  
2470            **service;**  
2471    c)        **generate and store the keys securely until delivery to and acceptance by the**  
2472            **subject;**  
2473    d)        **deliver the subject’s private key in a manner that ensures that the privacy of**  
2474            **the key is not compromised and only the subject has access to the private**  
2475            **key.**

2476    AL3\_CM\_SKP#020            Key generation by Subject

2477    **If the subject generates and presents its own keys, obtain the subject’s written**  
2478    **confirmation that it has:**

- 2479    a)        **used a FIPS 140-2 [FIPS140-2] compliant algorithm, or equivalent, as**  
2480            **established by a recognized national technical authority, that is recognized as**  
2481            **being fit for the purposes of the service;**  
2482    b)        **created keys of a key length and for use with a FIPS 140-2 [FIPS140-2]**  
2483            **compliant public key algorithm, or equivalent, as established by a recognized**  
2484            **national technical authority, recognized as being fit for the purposes of the**  
2485            **service.**  
2486

#### 2487    **3.7.2.3.4 Credential Delivery**

2488    An enterprise and its specified service must:

2489    AL3\_CM\_CRD#010,            Notify Subject of Credential Issuance

2490    Notify the subject of the credential’s issuance and, if necessary, confirm Subject’s contact  
2491    information by:

- 2492    a)        **sending notice to the address of record confirmed during identity proofing, and**  
2493            **either:**  
2494            **i)        issuing the credential(s) in a manner that confirms the address of**  
2495            **record supplied by the applicant during identity proofing, or;**  
2496            **ii)       issuing the credential(s) in a manner that confirms the ability of the**  
2497            **applicant to receive telephone communications at a phone number**  
2498            **supplied by the applicant during identity proofing, while recording**  
2499            **the applicant’s voice.**

2500    AL3\_CM\_CRD#020            Subject’s acknowledgement

2501    **Receive acknowledgement of receipt of the credential before it is activated and its**  
2502    **directory status record is published (and thereby the subscription becomes active or**  
2503    **re-activated, depending upon the circumstances of issue).**

2504

2505

2506 **3.7.2.4 Assurance Level 4**

2507 **3.7.2.4.1 Identity Proofing**

2508 These criteria determine how the enterprise shows compliance with the criteria for  
2509 fulfilling identity proofing functions.

2510 An enterprise and its specified service must:

2511 AL4\_CM\_IDP#010 Self-managed Identity Proofing

2512 If the enterprise assumes direct responsibility for identity proofing functions, show, by  
2513 direct inclusion, compliance with all applicable identity proofing service assessment  
2514 criteria for **[omitted]** AL4.

2515 AL4\_CM\_IDP#020 Kantara-Recognized outsourced service

2516 If the enterprise outsources responsibility for identity proofing functions and uses a  
2517 service already Kantara-Recognized, show that the service in question has been certified  
2518 at **[omitted]** AL4 and that its approval has at least **12** months of remaining validity.

2519 AL4\_CM\_IDP#030 Non- Kantara-Recognized outsourced service

2520 Not use any non- Kantara-Recognized outsourced services for identity proofing unless  
2521 they can be demonstrated to have satisfied equivalently rigorous requirements established  
2522 by another scheme recognized by IAWG.

2523 AL4\_CM\_IDP#040 Revision to subscriber information

2524 Provide a means for subscribers to securely amend their stored information after  
2525 registration, either by re-proving their identity as in the initial registration process or by  
2526 using their credentials to authenticate their revision. Successful revision must, where  
2527 necessary, instigate the re-issuance of the credential.

2528

2529 **3.7.2.4.2 Credential Creation**

2530 These criteria define the requirements for creation of credentials whose highest use is  
2531 AL4.

2532 Note, however, that a token and credential created according to these criteria may not  
2533 necessarily provide that level of assurance for the claimed identity of the subscriber.  
2534 Authentication can only be provided at the assurance level at which the identity is proven.

2535 An enterprise and its specified service must:



- 
- 2536 AL4\_CM\_CRN#010 Authenticated Request
- 2537 Only accept a request to generate a credential and bind it to an identity if the source of the  
2538 request, i.e., Registration Authority (RA), can be authenticated as being authorized to  
2539 perform identity proofing at AL4.
- 2540 AL4\_CM\_CRN#020 Unique identity
- 2541 Ensure that the identity which relates to a specific applicant is unique within the specified  
2542 service, including identities previously used and that are now cancelled, other than its re-  
2543 assignment to the same applicant.
- 2544 **Guidance:** This requirement is intended to prevent identities that may exist in a Relying  
2545 Party's access control lists from possibly representing a different physical person.
- 2546 AL4\_CM\_CRN#030 Credential uniqueness
- 2547 Allow the subscriber to select a credential (e.g., UserID) that is verified to be unique  
2548 within the specified service's community and assigned uniquely to a single identity  
2549 subject.
- 2550 AL4\_CM\_CRN#035 Convey credential
- 2551 Be capable of conveying the unique identity information associated with a credential to  
2552 Verifiers and Relying Parties.
- 2553 AL4\_CM\_CRN#040 PIN/Password strength
- 2554 *Not* use PIN/password tokens.
- 2555 AL4\_CM\_CRN#050 One-time password strength
- 2556 **Not use one-time password tokens.**
- 2557 AL4\_CM\_CRN#060 Software cryptographic token strength
- 2558 **Not use software cryptographic tokens.**
- 2559 AL4\_CM\_CRN#070 Hardware token strength
- 2560 Ensure that hardware tokens used to store cryptographic keys:
- 2561 a) employ a cryptographic module that is validated against FIPS 140-2 [[FIPS140-2](#)]  
2562 Level 2 or higher, or equivalent, as determined by a recognized national technical  
2563 authority;

- 2564 b) are evaluated against FIPS 140-2 Level 3 or higher, or equivalent, as  
2565 determined by a recognized national technical authority, for their physical  
2566 security;  
2567 c) require password or biometric activation by the subscriber [omitted].

2568 AL4\_CM\_CRN#080 Binding of key

2569 If the specified service generates the subject's key pair, that the key generation process  
2570 securely and uniquely binds that process to the certificate generation and maintains at all  
2571 times the secrecy of the private key, until it is accepted by the subject.

2572 AL4\_CM\_CRN#090 Nature of subject

2573 Record the nature of the subject of the credential [omitted], i.e., private person, a named  
2574 person acting on behalf of a corporation or other legal entity, corporation or legal entity,  
2575 or corporate machine entity, in a manner that can be unequivocally associated with the  
2576 credential and the identity that it asserts.

2577

#### 2578 **3.7.2.4.3 Subject Key Pair Generation**

2579 An enterprise and its specified service must:

2580 AL4\_CM\_SKP#010 Key generation by Specified Service

2581 If the specified service generates the subject's keys:

- 2582 a) use a FIPS 140-2 [FIPS140-2] compliant algorithm, or equivalent, as established  
2583 by a recognized national technical authority, that is recognized as being fit for the  
2584 purposes of the service;  
2585 b) only create keys of a key length and for use with a FIPS 140-2 [FIPS140-2]  
2586 compliant public key algorithm, or equivalent, as established by a recognized  
2587 national technical authority, recognized as being fit for the purposes of the  
2588 service;  
2589 c) generate and store the keys securely until delivery to and acceptance by the  
2590 subject;  
2591 d) deliver the subject's private key in a manner that ensures that the privacy of the  
2592 key is not compromised and only the subject has access to the private key.

2593 AL4\_CM\_SKP#020 Key generation by Subject

2594 If the subject generates and presents its own keys, obtain the subject's written  
2595 confirmation that it has:

- 2596 a) used a FIPS 140-2 [FIPS140-2] compliant algorithm, or equivalent, as established  
2597 by a recognized national technical authority, that is recognized as being fit for the  
2598 purposes of the service;  
2599 b) created keys of a key length and for use with a FIPS 140-2 [FIPS140-2] compliant  
2600 public key algorithm, or equivalent, as established by a recognized national  
2601 technical authority, recognized as being fit for the purposes of the service.  
2602

#### 2603 **3.7.2.4.4 Credential Delivery**

2604 An enterprise and its specified service must:

2605 AL4\_CM\_CRD#010 Notify Subject of Credential Issuance

2606 Notify the subject of the credential's issuance and, if necessary, confirm Subject's contact  
2607 information by:

- 2608 a) sending notice to the address of record confirmed during identity proofing;  
2609 b) **unless the subject presented with a private key, issuing the hardware token**  
2610 **to the subject in a manner that confirms the address of record supplied by**  
2611 **the applicant during identity proofing;**  
2612 c) **issuing the certificate to the subject over a separate channel in a manner that**  
2613 **confirms either the address of record or the email address supplied by the**  
2614 **applicant during identity proofing.**

2615 AL4\_CM\_CRD#020 Subject's acknowledgement

2616 Receive acknowledgement of receipt of the **hardware token** before it is activated and **the**  
2617 **corresponding certificate and** its directory status record are published (and thereby the  
2618 subscription becomes active or re-activated, depending upon the circumstances of issue).

2619

2620           **3.7.3 Part C - Credential Renewal and Re-issuing**

2621       These criteria apply to the renewal and re-issuing of credentials. They address  
2622       requirements levied by the use of various technologies to achieve the appropriate AL<sup>9</sup>.  
2623       These criteria include by reference all applicable criteria in Section 3.6 and the renewal  
2624       and re-issuing processes shall comply in all practical senses with the applicable criteria  
2625       set forth in Part B of this section.

2626

2627       **3.7.3.1 Assurance Level 1**

2628       **3.7.3.1.1 Renewal/Re-issuance Procedures**

2629       These criteria address general renewal and re-issuance functions, to be exercised as  
2630       specific controls in these circumstances while continuing to observe the general  
2631       requirements established for initial credential issuance.

2632       An enterprise and its specified service must:

2633       AL1\_CM\_RNR#010           Changeable PIN/Password

2634       Permit subjects to change their PINs/passwords.

2635

2636

---

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

2637 **3.7.3.2 Assurance Level 2**

2638 **3.7.3.2.1 Renewal/Re-issuance Procedures**

2639 These criteria address general renewal and re-issuance functions, to be exercised as  
2640 specific controls in these circumstances while continuing to observe the general  
2641 requirements established for initial credential issuance.

2642 An enterprise and its specified service must:

2643 AL2\_CM\_RNR#010 Changeable PIN/Password

2644 Permit subjects to change their [omitted] passwords, **but employ reasonable practices**  
2645 **with respect to password resets and repeated password failures.**

2646 AL2\_CM\_RNR#020 Proof-of-possession on Renewal/Re-issuance

2647 **Subjects wishing to change their passwords must demonstrate that they are in**  
2648 **possession of the unexpired current token prior to the CSP proceeding to renew or**  
2649 **re-issue it.**

2650 AL2\_CM\_RNR#030 Renewal/Re-issuance limitations

2651 **a. not renew but may re-issue Passwords;**

2652 **b. neither renew nor re-issue expired tokens;**

2653 **c. conduct all renewal / re-issuance interactions with the Subject over a**  
2654 **protected channel such as SSL/TLS.**

2655 **Guidance:** Renewal is considered as an extension of usability, whereas re-issuance  
2656 requires a change.

2657

2658

2659 **3.7.3.3 Assurance Level 3**

2660 **3.7.3.3.1 Renewal/Re-issuance Procedures**

2661 These criteria address general renewal and re-issuance functions, to be exercised as  
2662 specific controls in these circumstances while continuing to observe the general  
2663 requirements established for initial credential issuance.

2664 An enterprise and its specified service must:

2665 AL3\_CM\_RNR#010 Changeable PIN/Password

2666 Permit subjects to change **the passwords used to activate their credentials.**

2667

2668 *Further criteria may be determined after AL3 comparability assessment against Federal*  
2669 *CAF and NIST SP 800-63.*

2670

2671

2672 **3.7.3.4 Assurance Level 4**

2673 **3.7.3.4.1 Renewal/Re-issuance Procedures**

2674 These criteria address general renewal and re-issuance functions, to be exercised as  
2675 specific controls in these circumstances while continuing to observe the general  
2676 requirements established for initial credential issuance.

2677 An enterprise and its specified service must:

2678 AL4\_CM\_RNR#010 Changeable PIN/Password

2679 Permit subjects to change the passwords used to activate their credentials.

2680

2681 *Further criteria may be determined after AL4 comparability assessment against Federal*  
2682 *CAF and NIST SP 800-63.*

2683

2684

2685 **3.7.4 Part D - Credential Revocation**

2686 These criteria deal with credential revocation and the determination of the legitimacy of a  
2687 revocation request.

2688 **3.7.4.1 Assurance Level 1**

2689 An enterprise and its specified service must:

2690 **3.7.4.1.1 Not used**

2691 **3.7.4.1.2 Not used**

2692 **3.7.4.1.3 Secure Revocation Request**

2693 This criterion applies when revocation requests between remote components of a service  
2694 are made over a secured communication.

2695 An enterprise and its specified service must:

2696 AL1\_CM\_SRR#010 Submit Request

2697 Submit a request for revocation to the Credential Issuer service (function), using a  
2698 secured network communication, if necessary.

2699

2700



2701 **3.7.4.2 Assurance Level 2**

2702 **3.7.4.2.1 Revocation Procedures**

2703 These criteria address general revocation functions, such as the processes involved and  
2704 the basic requirements for publication.

2705 An enterprise and its specified service must:

2706 AL2\_CM\_RVP#010 Revocation procedures

2707 a) **State the conditions under which revocation of an issued credential may**  
2708 **occur;**

2709 b) **State the processes by which a revocation request may be submitted;**

2710 c) **State the persons and organizations from which a revocation request will be**  
2711 **accepted;**

2712 d) **State the validation steps that will be applied to ensure the validity (identity)**  
2713 **of the Revocant, and;**

2714 e) **State the response time between a revocation request being accepted and the**  
2715 **publication of revised certificate status.**

2716 AL2\_CM\_RVP#020 Secure status notification

2717 **Ensure that published credential status notification information can be relied upon**  
2718 **in terms of the enterprise of its origin (i.e., its authenticity) and its correctness (i.e.,**  
2719 **its integrity).**

2720 AL2\_CM\_RVP#030 Revocation publication

2721 **Unless the credential will expire automatically within 72 hours:**

2722 **Ensure that published credential status notification is revised within 72 hours of the**  
2723 **receipt of a valid revocation request, such that any subsequent attempts to use that**  
2724 **credential in an authentication shall be unsuccessful.**

2725 AL2\_CM\_RVP#040 Verify revocation identity

2726 **Establish that the identity for which a revocation request is received is one that was**  
2727 **issued by the specified service.**

2728 AL2\_CM\_RVP#050 Revocation Records

2729 **Retain a record of any revocation of a credential that is related to a specific identity**  
2730 **previously verified, solely in connection to the stated credential. At a minimum,**  
2731 **records of revocation must include:**

- 2732 a) **the Revocant's full name;**  
2733 b) **the Revocant's authority to revoke (e.g., subscriber themselves, someone**  
2734 **acting with the subscriber's power of attorney, the credential issuer, law**  
2735 **enforcement, or other legal due process);**  
2736 c) **the Credential Issuer's identity (if not directly responsible for the identity**  
2737 **proofing service);**  
2738 d) **the identity associated with the credential (whether the subscriber's name or**  
2739 **a pseudonym);**  
2740 e) **the reason for revocation.**

2741 AL2\_CM\_RVP#060 Record Retention

2742 **Retain, securely, the record of the revocation process for the duration of the**  
2743 **subscriber's account plus 7.5 years.**

2744

#### 2745 **3.7.4.2.2 Verify Revocant's Identity**

2746 Revocation of a credential requires that the requestor and the nature of the request be  
2747 verified as rigorously as the original identity proofing. The enterprise should not act on a  
2748 request for revocation without first establishing the validity of the request (if it does not,  
2749 itself, determine the need for revocation).

2750 In order to do so, the enterprise and its specified service must:

2751 AL2\_CM\_RVR#010 Verify revocation identity

2752 **Establish that the credential for which a revocation request is received was one that**  
2753 **was issued by the specified service, applying the same process and criteria as would**  
2754 **be applied to an original identity proofing.**

2755 AL2\_CM\_RVR#020 Revocation reason

2756 **Establish the reason for the revocation request as being sound and well founded, in**  
2757 **combination with verification of the Revocant, according to AL2\_ID\_RVR#030,**  
2758 **AL2\_ID\_RVR#040, or AL2\_ID\_RVR#050.**

2759 AL2\_CM\_RVR#030 Verify Subscriber as Revocant

2760 **When the subscriber seeks revocation of the subscriber's own credential, the**  
2761 **enterprise must:**

- 2762 a) **if in person, require presentation of a primary Government Picture ID**  
2763 **document that shall be electronically verified by a record check against the**  
2764 **provided identity with the specified issuing authority's records;**  
2765 b) **if remote:**  
2766 i. **electronically verify a signature against records (if available),**  
2767 **confirmed with a call to a telephone number of record, or;**  
2768 ii. **authenticate an electronic request as being from the same subscriber,**  
2769 **supported by a credential at Assurance Level 2 or higher.**

2770 AL2\_CM\_RVR#040 CSP as Revocant

2771 **Where a CSP seeks revocation of a subscriber's credential, the enterprise must**  
2772 **establish that the request is either:**

- 2773 a) **from the specified service itself, with authorization as determined by**  
2774 **established procedures, or;**  
2775 b) **from the client Credential Issuer, by authentication of a formalized request**  
2776 **over the established secure communications network.**

2777 AL2\_CM\_RVR#050 Verify Legal Representative as Revocant

2778 **Where the request for revocation is made by a law enforcement officer or**  
2779 **presentation of a legal document, the enterprise must:**

- 2780 a) **if in-person, verify the identity of the person presenting the request;**  
2781 b) **if remote:**  
2782 i. **in paper/facsimile form, verify the origin of the legal document by a**  
2783 **database check or by telephone with the issuing authority, or;**  
2784 ii. **as an electronic request, authenticate it as being from a recognized**  
2785 **legal office, supported by a credential at Assurance Level 2 or higher.**  
2786

#### 2787 **3.7.4.2.3 Secure Revocation Request**

2788 This criterion applies when revocation requests must be communicated between remote  
2789 components of the service organization.

2790 An enterprise and its specified service must:

2791 AL2\_CM\_SRR#010 Submit Request

2792 Submit a request for the revocation to the Credential Issuer service (function), using a  
2793 secured network communication.

2794

2795 **3.7.4.3 Assurance Level 3**

2796 **3.7.4.3.1 Revocation Procedures**

2797 These criteria address general revocation functions, such as the processes involved and  
2798 the basic requirements for publication.

2799 An enterprise and its specified service must:

2800 AL3\_CM\_RVP#010 Revocation procedures

2801 a) State the conditions under which revocation of an issued credential may occur;

2802 b) State the processes by which a revocation request may be submitted;

2803 c) State the persons and organizations from which a revocation request will be  
2804 accepted;

2805 d) State the validation steps that will be applied to ensure the validity (identity) of  
2806 the Revocant, and;

2807 e) State the response time between a revocation request being accepted and the  
2808 publication of revised certificate status.

2809 AL3\_CM\_RVP#020 Secure status notification

2810 Ensure that published credential status notification information can be relied upon in  
2811 terms of the enterprise being its origin (i.e., its authenticity) and its correctness (i.e., its  
2812 integrity).

2813 AL3\_CM\_RVP#030 Revocation publication

2814 **[Omitted]** Ensure that published credential status notification is revised within **24** hours  
2815 of the receipt of a valid revocation request, such that any subsequent attempts to use that  
2816 credential in an authentication shall be unsuccessful. **The nature of the revocation**  
2817 **mechanism shall be in accord with the technologies supported by the service.**

2818 AL3\_CM\_RVP\_#040 Verify Revocation Identity

2819 Establish that the identity for which a revocation request is received is one that was  
2820 issued by the specified service.

2821 AL3\_CM\_RVP#050 Revocation Records

2822 Retain a record of any revocation of a credential that is related to a specific identity  
2823 previously verified, solely in connection to the stated credential. At a minimum, records  
2824 of revocation must include:

- 2825 a) the Revocant's full name;  
2826 b) the Revocant's authority to revoke (e.g., subscriber themselves, someone acting  
2827 with the subscriber's power of attorney, the credential issuer, law enforcement, or  
2828 other legal due process);  
2829 c) the Credential Issuer's identity (if not directly responsible for the identity  
2830 proofing service);  
2831 d) the identity associated with the credential (whether the subscriber's name or a  
2832 pseudonym);  
2833 e) the reason for revocation.

2834 AL3\_CM\_RVP#060 Record Retention

2835 Retain, securely, the record of the revocation process for a period which is in compliance  
2836 with:

- 2837 a) the records retention policy required by AL2\_CM\_CPP#010, and;  
2838 b) applicable legislation;

2839 and which, in addition, must be not less than the duration of the subscriber's account plus  
2840 7.5 years.

2841

#### 2842 **3.7.4.3.2 Verify Revocant's Identity**

2843 Revocation of a credential requires that the requestor and the nature of the request be  
2844 verified as rigorously as the original identity proofing. The enterprise should not act on a  
2845 request for revocation without first establishing the validity of the request (if it does not,  
2846 itself, determine the need for revocation).

2847 In order to do so, the enterprise and its specified service must:

2848 AL3\_CM\_RVR#010 Verify revocation identity

2849 Establish that the credential for which a revocation request is received is one that was  
2850 initially issued by the specified service, applying the same process and criteria as would  
2851 be applied to an original identity proofing.

2852 AL3\_CM\_RVR#020 Revocation reason

2853 Establish the reason for the revocation request as being sound and well founded, in  
2854 combination with verification of the Revocant, according to AL3\_ID\_RVR#030,  
2855 AL3\_ID\_RVR#040, or AL3\_ID\_RVR#050.

2856 AL3\_CM\_RVR#030 Verify Subscriber as Revocant

2857 When the subscriber seeks revocation of the subscriber's own credential:

- 2858 a) if in-person, require presentation of a primary Government Picture ID document  
2859 that shall be electronically verified by a record check against the provided identity  
2860 with the specified issuing authority's records;  
2861 b) if remote:  
2862 i. electronically verify a signature against records (if available), confirmed  
2863 with a call to a telephone number of record, or;  
2864 ii. as an electronic request, authenticate it as being from the same subscriber,  
2865 supported by a credential at Assurance Level **3** or higher.

2866 AL3\_CM\_RVR#040 Verify CSP as Revocant

2867 Where a CSP seeks revocation of a subscriber's credential, establish that the request is  
2868 either:

- 2869 a) from the specified service itself, with authorization as determined by established  
2870 procedures, or;  
2871 b) from the client Credential Issuer, by authentication of a formalized request over  
2872 the established secure communications network.

2873 AL3\_CM\_RVR#050 Verify Legal Representative as Revocant

2874 Where the request for revocation is made by a law enforcement officer or presentation of  
2875 a legal document:

- 2876 a) if in person, verify the identity of the person presenting the request, or;  
2877 b) if remote:  
2878 i. in paper/facsimile form, verify the origin of the legal document by a  
2879 database check or by telephone with the issuing authority, or;  
2880 ii. as an electronic request, authenticate it as being from a recognized legal  
2881 office, supported by a credential at Assurance Level **3** or higher.  
2882

### 2883 **3.7.4.3.3 Secure Revocation Request**

2884 This criterion applies when revocation requests must be communicated between remote  
2885 components of the service organization.

2886 An enterprise and its specified service must:

2887 AL3\_CM\_SRR#010 Submit Request

2888 Submit a request for the revocation to the Credential Issuer service (function), using a  
2889 secured network communication.

2890

2891 **3.7.4.4 Assurance Level 4**

2892 **3.7.4.4.1 Revocation Procedures**

2893 These criteria address general revocation functions, such as the processes involved and  
2894 the basic requirements for publication.

2895 An enterprise and its specified service must:

2896 AL4\_CM\_RVP#010 Revocation procedures

2897 a) State the conditions under which revocation of an issued certificate may occur;

2898 b) State the processes by which a revocation request may be submitted;

2899 c) State the persons and organizations from which a revocation request will be  
2900 accepted;

2901 d) State the validation steps that will be applied to ensure the validity (identity) of  
2902 the Revocant, and;

2903 e) State the response time between a revocation request being accepted and the  
2904 publication of revised certificate status.

2905 AL4\_CM\_RVP#020 Secure status notification

2906 Ensure that published credential status notification information can be relied upon in  
2907 terms of the enterprise of its origin (i.e., its authenticity) and its correctness (i.e., its  
2908 integrity).

2909 AL4\_CM\_RVP#030 Revocation publication

2910 Ensure that published credential status notification is revised within **18** hours of the  
2911 receipt of a valid revocation request, such that any subsequent attempts to use that  
2912 credential in an authentication shall be unsuccessful. The nature of the revocation  
2913 mechanism shall be in accordance with the technologies supported by the service.

2914 AL4\_CM\_RVP#040 No stipulation

2915 AL4\_CM\_RVP#050 Revocation Records

2916 Retain a record of any revocation of a credential that is related to a specific identity  
2917 previously verified, solely in connection to the stated credential. At a minimum, records  
2918 of revocation must include:

2919 a) the Revocant's full name;

- 2920 b) the Revocant's authority to revoke (e.g., subscriber themselves, someone acting  
2921 with the subscriber's power of attorney, the credential issuer, law enforcement, or  
2922 other legal due process);  
2923 c) the Credential Issuer's identity (if not directly responsible for the identity  
2924 proofing service);  
2925 d) the identity associated with the credential (whether the subscriber's name or a  
2926 pseudonym);  
2927 e) the reason for revocation.

2928 AL4\_CM\_RVP#060 Record Retention

2929 Retain, securely, the record of the revocation process for a period which is in compliance  
2930 with:

2931 c) the records retention policy required by AL2\_CM\_CPP#010, and;

2932 d) applicable legislation;

2933 and which, in addition, must be not less than the duration of the subscriber's account plus  
2934 7.5 years.

2935

#### 2936 **3.7.4.4.2 Verify Revocant's Identity**

2937 Revocation of a credential requires that the requestor and the nature of the request be  
2938 verified as rigorously as the original identity proofing. The enterprise should not act on a  
2939 request for revocation without first establishing the validity of the request (if it does not,  
2940 itself, determine the need for revocation).

2941 In order to do so, the enterprise and its specified service must:

2942 AL4\_CM\_RVR#010 Verify revocation identity

2943 Establish that the credential for which a revocation request is received is one that was  
2944 initially issued by the specified service, applying the same process and criteria as would  
2945 apply to an original identity proofing.

2946 AL4\_CM\_RVR#020 Revocation reason

2947 Establish the reason for the revocation request as being sound and well founded, in  
2948 combination with verification of the Revocant, according to AL4\_CM\_RVR#030,  
2949 AL4\_CM\_RVR#040, or AL4\_CM\_RVR#050.

2950 AL4\_CM\_RVR#030 Verify Subscriber as Revocant

2951 Where the subscriber seeks revocation of the subscriber's own credential:



- 2952 a) if in person, require presentation of a primary Government Picture ID document  
2953 that shall be [Omitted] verified by a record check against the provided identity  
2954 with the specified issuing authority's records;  
2955 b) if remote:  
2956 i. verify a signature against records (if available), confirmed with a call to a  
2957 telephone number of record, or;  
2958 ii. as an electronic request, authenticate it as being from the same subscriber,  
2959 supported by a **different** credential at **Assurance Level 4**.

2960 AL4\_CM\_RVR#040 Verify CSP as Revocant

2961 Where a CSP seeks revocation of a subscriber's credential, establish that the request is  
2962 either:

- 2963 a) from the specified service itself, with authorization as determined by established  
2964 procedures, or;  
2965 b) from the client Credential Issuer, by authentication of a formalized request over  
2966 the established secure communications network.

2967 AL4\_CM\_RVR#050 Verify Legal Representative as Revocant

2968 Where the request for revocation is made by a law enforcement officer or presentation of  
2969 a legal document:

- 2970 a) if in-person, verify the identity of the person presenting the request, or;  
2971 b) if remote:  
2972 i. in paper/facsimile form, verify the origin of the legal document by a  
2973 database check or by telephone with the issuing authority;  
2974 ii. as an electronic request, authenticate it as being from a recognized legal  
2975 office, supported by a different credential at **Assurance Level 4**.

#### 2976 **3.7.4.4.3 Re-keying a credential**

2977 Re-keying of a credential requires that the requestor be verified as the subject with as  
2978 much rigor as was applied to the original identity proofing. The enterprise should not act  
2979 on a request for re-key without first establishing that the requestor is identical to the  
2980 subject.

2981 In order to do so, the enterprise and its specified service must:

2982 AL4\_CM\_RKY#010 Verify Requestor as Subscriber

2983 **Where the subscriber seeks a re-key for the subscriber's own credential:**

- 2984 a) **if in-person, require presentation of a primary Government Picture ID**  
2985 **document that shall be verified by a record check against the provided**  
2986 **identity with the specified issuing authority's records;**  
2987 b) **if remote:**

- 2988           i.       **verify a signature against records (if available), confirmed with a call**  
2989                   **to a telephone number of record, or;**  
2990           ii.       **authenticate an electronic request as being from the same subscriber,**  
2991                   **supported by a different credential at Assurance Level 4.**  
2992

2993   AL4\_CM\_RKY#020       Re-key requests other than subscriber

2994   **Re-key requests from any parties other than the subscriber must not be accepted.**

2995   **3.7.4.4.4 Secure Revocation/Re-key Request**

2996   This criterion applies when revocation **or re-key** requests must be communicated  
2997   between remote components of the service organization.

2998   The enterprise and its specified service must:

2999   AL4\_CM\_SRR#010       Submit Request

3000   Submit a request for the revocation to the Credential Issuer service (function), using a  
3001   secured network communication.

3002

3003           **3.7.5 Part E - Credential Status Management**

3004       These criteria deal with credential status management, such as the receipt of requests for  
3005       new status information arising from a new credential being issued or a revocation or other  
3006       change to the credential that requires notification. They also deal with the provision of  
3007       status information to requesting parties (Verifiers, Relying Parties, courts and others  
3008       having regulatory authority, etc.) having the right to access such information.

3009       **3.7.5.1 Assurance Level 1**

3010       **3.7.5.1.1 Status Maintenance**

3011       An enterprise and its specified service must:

3012       AL1\_CM\_CSM#010           Maintain Status Record

3013       Maintain a record of the status of all credentials issued.

3014       AL1\_CM\_CSM#020           No stipulation

3015       AL1\_CM\_CSM#030           No stipulation

3016       AL1\_CM\_CSM#040           Status Information Availability

3017       Provide, with 95% availability, a secure automated mechanism to allow relying parties to  
3018       determine credential status and authenticate the subject's identity.

3019

3020

3021 **3.7.5.2 Assurance Level 2**

3022 **3.7.5.2.1 Status Maintenance**

3023 An enterprise and its specified service must:

3024 AL2\_CM\_CSM#010 Maintain Status Record

3025 Maintain a record of the status of all credentials issued.

3026 AL2\_CM\_CSM#020 Validation of Status Change Requests

3027 **Authenticate all requestors seeking to have a change of status recorded and**  
3028 **published and validate the requested change before considering processing the**  
3029 **request. Such validation should include:**

3030 a) **the requesting source as one from which the specified service expects to**  
3031 **receive such requests;**

3032 b) **if the request is not for a new status, the credential or identity as being one**  
3033 **for which a status is already held.**

3034 AL2\_CM\_CSM#030 Revision to Published Status

3035 **Process authenticated requests for revised status information and have the revised**  
3036 **information available for access within a period of 72 hours.**

3037 AL2\_CM\_CSM#040 Status Information Availability

3038 Provide, with 95% availability, a secure automated mechanism to allow relying parties to  
3039 determine credential status and authenticate the subject's identity.

3040 AL2\_CM\_CSM#050 Inactive Credentials

3041 **Disable any credential that has not been successfully used for authentication during**  
3042 **a period of 18 months.**

3043

3044

3045 **3.7.5.3 Assurance Level 3**

3046 **3.7.5.3.1 Status Maintenance**

3047 An enterprise and its specified service must:

3048 AL3\_CM\_CSM#010 Maintain Status Record

3049 Maintain a record of the status of all credentials issued.

3050 AL3\_CM\_CSM#020 Validation of Status Change Requests

3051 Authenticate all requestors seeking to have a change of status recorded and published and  
3052 validate the requested change before considering processing the request. Such validation  
3053 should include:

- 3054 a) the requesting source as one from which the specified service expects to receive  
3055 such requests;  
3056 b) if the request is not for a new status, the credential or identity as being one for  
3057 which a status is already held.

3058 AL3\_CM\_CSM#030 Revision to Published Status

3059 Process authenticated requests for revised status information and have the revised  
3060 information available for access within a period of 72 hours.

3061 AL3\_CM\_CSM#040 Status Information Availability

3062 Provide, with **99%** availability, a secure automated mechanism to allow relying parties to  
3063 determine credential status and authenticate the subject's identity.

3064 AL3\_CM\_CSM#050 Inactive Credentials

3065 Disable any credential that has not been successfully used for authentication during a  
3066 period of 18 months.

3067

3068

3069 **3.7.5.4 Assurance Level 4**

3070 **3.7.5.4.1 Status Maintenance**

3071 An enterprise and its specified service must:

3072 AL4\_CM\_CSM#010 Maintain Status Record

3073 Maintain a record of the status of all credentials issued.

3074 AL4\_CM\_CSM#020 Validation of Status Change Requests

3075 Authenticate all requestors seeking to have a change of status recorded and published and  
3076 validate the requested change before considering processing the request. Such validation  
3077 should include:

- 3078 a) the requesting source as one from which the specified service expects to receive  
3079 such requests;  
3080 b) if the request is not for a new status, the credential or identity as being one for  
3081 which a status is already held.

3082 AL4\_CM\_CSM#030 Revision to Published Status

3083 Process authenticated requests for revised status information and have the revised  
3084 information available for access within a period of 72 hours.

3085 AL4\_CM\_CSM#040 Status Information Availability

3086 Provide, with 99% availability, a secure automated mechanism to allow relying parties to  
3087 determine credential status and authenticate the subject's identity.

3088 AL4\_CM\_CSM#050 Inactive Credentials

3089 Disable any credential that has not been successfully used for authentication during a  
3090 period of 18 months.

3091

3092 **3.7.6 Part F - Credential Validation/Authentication**

3093 These criteria apply to credential validation and identity authentication.

3094 **3.7.6.1 Assurance Level 1**

3095 **3.7.6.1.1 Assertion Security**

3096 An enterprise and its specified service must:

3097 AL1\_CM\_ASS#010 Validation and Assertion Security

3098 Provide validation of credentials to a Relying Party using a protocol that:

3099 a) requires authentication of the specified service or of the validation source;

3100 b) ensures the integrity of the authentication assertion;

3101 c) protects assertions against manufacture, modification and substitution, and  
3102 secondary authenticators from manufacture;

3103 and which, specifically:

3104 d) creates assertions which are specific to a single transaction;

3105 e) where assertion references are used, generates a new reference whenever a new  
3106 assertion is created;

3107 f) when an assertion is provided indirectly, either signs the assertion or sends it via a  
3108 protected channel, using a strong binding mechanism between the secondary  
3109 authenticator and the referenced assertion;

3110 g) requires the secondary authenticator to:

3111 i) be signed when provided directly to Relying Party, or;

3112 ii) have a minimum of 64 bits of entropy when provision is indirect (i.e.  
3113 through the credential user).

3114 AL1\_CM\_ASS#015 No stipulation

3115 AL1\_CM\_ASS#020 No Post Authentication

3116 *Not* authenticate credentials that have been revoked.

3117 AL1\_CM\_ASS#030 Proof of Possession

3118 Use an authentication protocol that requires the claimant to prove possession and control  
3119 of the authentication token.

3120 AL1\_CM\_ASS#040 Assertion Lifetime

3121 Generate assertions so as to indicate and effect their expiration within:

- 3122 a) 12 hours after their creation, where the service shares a common internet domain  
3123 with the Relying Party;
- 3124 b) five minutes after their creation, where the service does not share a common  
3125 internet domain with the Relying Party.
- 3126
- 3127



3128 **3.7.6.2 Assurance Level 2**

3129 **3.7.6.2.1 Assertion Security**

3130 An enterprise and its specified service must:

3131 AL2\_CM\_ASS#010 Validation and Assertion Security

3132 Provide validation of credentials to a Relying Party using a protocol that:

- 3133 a) requires authentication of the specified service, itself, or of the validation source;
- 3134 b) ensures the integrity of the authentication assertion;
- 3135 c) protects assertions against manufacture, modification, **substitution and**
- 3136 **disclosure**, and secondary authenticators from manufacture, **capture and replay**;
- 3137 **d) uses approved cryptography techniques;**

3138 and which, specifically:

- 3139 e) creates assertions which are specific to a single transaction;
- 3140 f) where assertion references are used, generates a new reference whenever a new
- 3141 assertion is created;
- 3142 g) when an assertion is provided indirectly, either signs the assertion or sends it via a
- 3143 protected channel, using a strong binding mechanism between the secondary
- 3144 authenticator and the referenced assertion;
- 3145 **h) send assertions either via a channel mutually-authenticated with the Relying**
- 3146 **Party, or signed and encrypted for the Relying Party;**
- 3147 i) requires the secondary authenticator to:
  - 3148 i) be signed when provided directly to Relying Party, or;
  - 3149 ii) have a minimum of 64 bits of entropy when provision is indirect (i.e.
  - 3150 through the credential user);
  - 3151 **iii) be transmitted to the Subject through a protected channel which is**
  - 3152 **linked to the primary authentication process in such a way that**
  - 3153 **session hijacking attacks are resisted;**
  - 3154 **iv) not be subsequently transmitted over an unprotected channel or to an**
  - 3155 **unauthenticated party while it remains valid.**

3156 AL2\_CM\_ASS#015 No False Authentication

3157 **Employ techniques which ensure that system failures do not result in ‘false positive**

3158 **authentication’ errors.**

3159 AL2\_CM\_ASS#020 No Post Authentication

3160 *Not* authenticate credentials that have been revoked **unless the time of the transaction**

3161 **for which verification is sought precedes the time of revocation of the credential.**

- 
- 3162 AL2\_CM\_ASS#030 Proof of Possession
- 3163 Use an authentication protocol that requires the claimant to prove possession and control  
3164 of the authentication token.
- 3165 AL2\_CM\_ASS#040 Assertion Lifetime
- 3166 Generate assertions so as to indicate and effect their expiration:
- 3167 a) 12 hours after their creation, where the service shares a common internet domain  
3168 with the Relying Party;
- 3169 b) five minutes after their creation, where the service does not share a common  
3170 internet domain with the Relying Party.
- 3171
- 3172

3173 **3.7.6.3 Assurance Level 3**

3174 **3.7.6.3.1 Assertion Security**

3175 An enterprise and its specified service must:

3176 AL3\_CM\_ASS#010 Validation and Assertion Security

3177 Provide validation of credentials to a Relying Party using a protocol that:

- 3178 a) requires authentication of the specified service, itself, or of the validation source;
- 3179 b) ensures the integrity of the authentication assertion.

3180 AL3\_CM\_ASS#015 No False Authentication

3181 Employ techniques which ensure that system failures do not result in ‘false positive  
3182 authentication’ errors.

3183 AL3\_CM\_ASS#020 Post Authentication

3184 *Not* authenticate credentials that have been revoked unless the time of the transaction for  
3185 which verification is sought precedes the time of revocation of the credential.

3186 AL3\_CM\_ASS#030 Proof of Possession

3187 Use an authentication protocol that requires the claimant to prove possession and control  
3188 of the authentication token.

3189 AL3\_CM\_ASS#040 Assertion Lifetime

3190 **For non-cryptographic credentials**, generate assertions so as to indicate and effect their  
3191 expiration 12 hours after their creation; **otherwise, notify the relying party of how often**  
3192 **the revocation status sources are updated.**

3193

3194

3195 **3.7.6.4 Assurance Level 4**

3196 **3.7.6.4.1 Assertion Security**

3197 An enterprise and its specified service must:

3198 AL4\_CM\_ASS#010 Validation and Assertion Security

3199 Provide validation of credentials to a Relying Party using a protocol that:

- 3200 a) requires authentication of the specified service, itself, or of the validation source;  
3201 b) ensures the integrity of the authentication assertion.

3202 AL4\_CM\_ASS#015 No False Authentication

3203 Employ techniques which ensure that system failures do not result in ‘false positive  
3204 authentication’ errors.

3205 AL4\_CM\_ASS#020 Post Authentication

3206 *Not* authenticate credentials that have been revoked unless the time of the transaction for  
3207 which verification is sought precedes the time of revocation of the credential.

3208 AL4\_CM\_ASS#030 Proof of Possession

3209 Use an authentication protocol that requires the claimant to prove possession and control  
3210 of the authentication token.

3211 AL4\_CM\_ASS#040 Assertion Lifetime

3212 **[Omitted]** Notify the relying party of how often the revocation status sources are  
3213 updated.

3214

3215

3216 **3.7.7 Compliance Tables**

3217 Use the following tables to correlate criteria for a particular Assurance Level (AL) and  
3218 the evidence offered to support compliance.

3219 Service providers preparing for an assessment can use the table appropriate to the AL at  
3220 which they are seeking approval to correlate evidence with criteria or to justify non-  
3221 applicability (e.g., “specific service types not offered”).

3222 Assessors can use the tables to record the steps in their assessment and their  
3223 determination of compliance or failure.

3224 **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	<a href="#">Protocol threat risk assessment and controls</a>	
AL1_CM_CTR#025	No stipulation	No conformity requirement
AL1_CM_CTR#030	<a href="#">System threat risk assessment and controls</a>	
AL1_CM_STS#010	Withdrawn	No conformity requirement
AL1_CM_OPN#010	<a href="#">Changeable PIN/Password</a>	
Part B – Credential Issuing		
AL1_CM_IDP#010	<a href="#">Self-managed Identity Proofing</a>	
AL1_CM_IDP#020	<a href="#">Kantara-Recognized outsourced service</a>	
AL1_CM_IDP#030	<a href="#">Non-recognized outsourced service</a>	
AL1_CM_IDP#040	<a href="#">Revision to subscriber information</a>	
AL1_CM_CRN#010	<a href="#">Authenticated Request</a>	
AL1_CM_CRN#020	No stipulation	No conformity requirement
AL1_CM_CRN#030	<a href="#">Credential uniqueness</a>	
Part C – Credential Renewal and Re-issuing		
AL1_CM_RNR#010	<a href="#">Changeable PIN/Password</a>	
Part D – Credential Revocation		
AL1_CM_SRR#010	<a href="#">Submit Request</a>	
Part E – Credential Status Management		
AL1_CM_CSM#010	<a href="#">Maintain Status Record</a>	
AL1_CM_CSM#020	No stipulation	No conformity requirement
AL1_CM_CSM#030	No stipulation	No conformity requirement

---

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

3225

3226

3227

**Table 3-10 CM-SAC - AL2 Compliance**

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

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

3228

3229



3230

**Table 3-11 CM-SAC - AL3 Compliance**

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

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

3231

3232

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

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

3233

## 3234 4 REFERENCES

---

3235

3236 [CAF] Louden, Chris, Spencer, Judy, Burr, Bill, Hawkins, Kevin, Temoshok, David,  
3237 Cornell, John, Wilsher, Richard G., Timchak, Steve, Sill, Stephen, Silver, Dave, Harrison,  
3238 Von, eds., "E-Authentication Credential Assessment Framework (CAF)," E-  
3239 Authentication Initiative, Version 2.0.0 (March 16, 2005).  
3240 <http://www.cio.gov/eauthentication/documents/CAF.pdf>

3241

3242 [EAP CSAC 04011] "EAP working paper: Identity Proofing Service Assessment Criteria  
3243 (ID-SAC)," Electronic Authentication Partnership, Draft 0.1.3 (July 20, 2004)  
3244 [http://eap.projectliberty.org/docs/Jul2004/EAP\\_CSAC\\_04011\\_0-1-3\\_ID-SAC.doc](http://eap.projectliberty.org/docs/Jul2004/EAP_CSAC_04011_0-1-3_ID-SAC.doc)

3245

3246 [EAPTrustFramework] "Electronic Authentication Partnership Trust Framework"  
3247 Electronic Authentication Partnership, Version 1.0. (January 6, 2005)  
3248 [http://eap.projectliberty.org/docs/Trust\\_Framework\\_010605\\_final.pdf](http://eap.projectliberty.org/docs/Trust_Framework_010605_final.pdf)

3249

3250 [FIPS140-2] "Security Requirements for Cryptographic Modules" Federal Information  
3251 Processing Standards. (May 25, 2001) <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>

3252

3253  
3254 [IS27001] ISO/IEC 27001:2005 "Information technology - Security techniques -  
3255 Requirements for information security management systems" International Organization  
3256 for Standardization.  
3257 [http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=42103](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103)

3258

3259 [M-04-04] Bolton, Joshua B., eds., "E-Authentication Guidance for Federal Agencies,"  
3260 Office of Management and Budget, (December 16, 2003).  
3261 <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>

3262

3263 [NIST800-63] Burr, William E., Dodson, Donna F., Polk, W. Timothy, eds., "Electronic  
3264 Authentication Guideline: : Recommendations of the National Institute of Standards and  
3265 Technology," Version 1.0.2, National Institute of Standards and Technology, (April,  
3266 2006). [http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1\\_0\\_2.pdf](http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf)

3267

- 3268 [RFC 3647] Chokhani, S., Ford, W., Sabett, R., Merrill, C., Wu, S., eds., "Internet X.509  
3269 Public Key Infrastructure Certificate Policy and Certification Practices Framework," The  
3270 Internet Engineering Task Force (November, 2003). <http://www.ietf.org/rfc/rfc3647.txt>  
3271  
3272