



# Identity Assurance Framework: Service Assessment Criteria

**Version:** 4.0bis  
**Date:** 2014-05-12  
**Status:** Final Recommendation  
**Approval:** KIR20140512

**Editor:** Richard G. Wilsher  
Zygm LLC

**Contributors:** <https://kantarainitiative.org/confluence/x/k4PEAw>

## Abstract

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

The latest versions of each of these documents can be found on Kantara's [Identity Assurance Framework - General Information web page](#).

27 **Notice**

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

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

45 Copyright: The content of this document is copyright of Kantara Initiative.  
46 © 2014 Kantara Initiative.

47

48

49		<b>Contents</b>	
50			
51	<b>1</b>	<b>INTRODUCTION.....</b>	<b>5</b>
52	1.1	Changes in this revision.....	5
53	<b>2</b>	<b>ASSURANCE LEVELS.....</b>	<b>7</b>
54	<b>3</b>	<b>SERVICE ASSESSMENT CRITERIA - GENERAL .....</b>	<b>8</b>
55	3.1	Context and Scope .....	8
56	3.2	Criteria Applicability .....	8
57	3.3	Status and Readership.....	9
58	3.4	Criteria Descriptions .....	9
59	3.5	Terminology.....	11
60	<b>4</b>	<b>COMMON ORGANIZATIONAL SERVICE ASSESSMENT CRITERIA .....</b>	<b>12</b>
61	4.1	Assurance Level 1.....	12
62	4.1.1	Enterprise and Service Maturity .....	12
63	4.1.2	Notices and User information .....	13
64	4.1.3	No stipulation.....	14
65	4.1.4	No stipulation.....	14
66	4.1.5	No stipulation.....	14
67	4.1.6	No stipulation.....	14
68	4.1.7	Secure Communications .....	14
69	4.2	Assurance Level 2.....	15
70	4.2.1	Enterprise and Service Maturity .....	15
71	4.2.2	Notices and User Information/Agreements .....	16
72	4.2.3	Information Security Management .....	18
73	4.2.4	Security-relevant Event (Audit) Records.....	20
74	4.2.5	Operational infrastructure .....	20
75	4.2.6	External Services and Components .....	21
76	4.2.7	Secure Communications .....	22
77	4.3	Assurance Level 3.....	24
78	4.3.1	Enterprise and Service Maturity .....	24
79	4.3.2	Notices and User Information.....	25
80	4.3.3	Information Security Management .....	27
81	4.3.4	Security-Relevant Event (Audit) Records .....	29
82	4.3.5	Operational Infrastructure.....	30
83	4.3.6	External Services and Components .....	31
84	4.3.7	Secure Communications .....	31
85	4.4	Assurance Level 4.....	33
86	4.4.1	Enterprise and Service Maturity .....	33
87	4.4.2	Notices and Subscriber Information/Agreements.....	34
88	4.4.3	Information Security Management .....	36
89	4.4.4	Security-Related (Audit) Records.....	38
90	4.4.5	Operational Infrastructure.....	39
91	4.4.6	External Services and Components .....	40

92	4.4.7	Secure Communications .....	40
93	4.5	Compliance Tables.....	42
94	<b>5</b>	<b>OPERATIONAL SERVICE ASSESSMENT CRITERIA.....</b>	<b>49</b>
95	5.1	Assurance Level 1.....	49
96	5.1.1	Part A - Credential Operating Environment .....	49
97	5.1.2	Part B - Credential Issuing.....	51
98	5.1.3	Part C - Credential Renewal and Re-issuing.....	55
99	5.1.4	Part D - Credential Revocation .....	55
100	5.1.5	Part E - Credential Status Management .....	56
101	5.1.6	Part F - Credential Verification/Authentication.....	56
102	5.2	Assurance Level 2.....	60
103	5.2.1	Part A - Credential Operating Environment .....	60
104	5.2.2	Part B - Credential Issuing.....	63
105	5.2.3	Part C - Credential Renewal and Re-issuing.....	73
106	5.2.4	Part D - Credential Revocation .....	74
107	5.2.5	Part E - Credential Status Management .....	77
108	5.2.6	Part F - Credential Verification/Authentication.....	78
109	5.3	Assurance Level 3.....	82
110	5.3.1	Part A - Credential Operating Environment .....	82
111	5.3.2	Part B - Credential Issuing.....	85
112	5.3.3	Part C - Credential Renewal and Re-issuing.....	97
113	5.3.4	Part D - Credential Revocation .....	98
114	5.3.5	Part E - Credential Status Management .....	100
115	5.3.6	Part F - Credential Verification/Authentication.....	101
116	5.4	Assurance Level 4.....	106
117	5.4.1	Part A - Credential Operating Environment .....	106
118	5.4.2	Part B - Credential Issuing.....	110
119	5.4.3	Part C - Credential Renewal and Re-issuing.....	119
120	5.4.4	Part D - Credential Revocation .....	120
121	5.4.5	Part E - Credential Status Management .....	123
122	5.4.6	Part F - Credential Verification/Authentication.....	124
123	5.5	Compliance Tables.....	128
124	<b>6</b>	<b>REFERENCES.....</b>	<b>143</b>
125	<b>7</b>	<b>REVISION HISTORY.....</b>	<b>146</b>
126			

## 128 **1 INTRODUCTION**

---

129 Kantara Initiative formed the Identity Assurance Work Group (IAWG) to foster adoption  
130 of consistently managed identity trust services. The IAWG's objective is to create a  
131 Framework of baseline policy requirements (criteria) and rules against which identity  
132 trust services can be assessed and evaluated. The goal is to facilitate trusted identity  
133 federation and to promote uniformity and interoperability amongst identity service  
134 providers, with a specific focus on the level of trust, or assurance, associated with identity  
135 assertions. The primary deliverable of IAWG is the Identity Assurance Framework (IAF).

136 The IAF specifies criteria for a harmonized, best-of-breed, industry-recognized identity  
137 assurance standard. The IAF is a Framework supporting mutual acceptance, validation,  
138 and life cycle maintenance across identity federations. It is composed of a set of  
139 documents that includes an [Overview](#) publication, the IAF *Glossary*, a summary  
140 document on *Assurance Levels*, and an *Assurance Assessment Scheme (AAS)* document  
141 supported by *Rules governing Assurance Assessments (RAA)*, which encompasses the  
142 associated assessment and certification program, as well as several subordinate  
143 documents. The present document, subordinate to the AAS, describes the Service  
144 Assessment Criteria component of the IAF.

145 The latest versions of each of these documents can be found on Kantara's [Identity](#)  
146 [Assurance Framework - General Information web page](#).

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

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

### 161 **1.1 Changes in this revision**

162 The principal reason for changes in this revision is to capture results of a mapping  
163 between version 3.0 of the SAC and NIST SP 800-63-2. Historically, AL1 and AL2 were

164 aligned against SP 800-63-1 but no formalized mapping had been conducted at ALs 3  
165 & 4.

166 Additionally, the mapping between v2.0 and v3.0 found in §8 of v3.0 has been removed –  
167 at the time of formal publication of the revisions in the present version of the document  
168 SAC v3.0 had been published for over twelve months.

169 In the course of these revisions the opportunity has been taken to perform incidental tidy-  
170 up where the originally-drafted language no longer reflects practice or terminology.

171 Excepting where text has been moved within the document and is otherwise unchanged,  
172 all revisions between v3.0 and v4.0 are shown with a grey background.

173

174 Additionally, the Compliance Tables now indicate the revision status for each criterion  
175 (italicized and right-justified), indicating whether it has:

- 176 i) been introduced as a *NEW* requirement;
- 177 ii) had its requirement *AMENDED* in any way;
- 178 iii) had merely an *EDITORIAL* change (i.e. no change to the requirement);
- 179 iv) been supplemented with *GUIDANCE*;
- 180 v) been *RE-NUMBERED*;

181 or any combination of the above. If a criterion has not changed, nothing is indicated

182 A reference to the formal approval ballot results has been included on the cover page (*bis*  
183 release).

## 184 **2 ASSURANCE LEVELS**

---

185 The IAF has adopted four Assurance Levels (ALs), based on the four levels of assurance  
186 posited by the U.S. Federal Government and described in OMB M-04-04 [[M-04-04](#)] and  
187 NIST Special Publication 800-63 [[NIST800-63](#)]. These are further described in the  
188 *Identity Assurance Framework: Levels of Assurance* document, which can be found on  
189 Kantara's [Identity Assurance Framework - General Information page](#).

## 190 **3 SERVICE ASSESSMENT CRITERIA - GENERAL**

---

### 191 3.1 Context and Scope

192 The Service Assessment Criteria (SAC) are prepared and maintained by the Identity  
193 Assurance Work Group (IAWG) as part of its Identity Assurance Framework. These  
194 criteria set out the requirements for credential services and their providers at all assurance  
195 levels within the Framework. These criteria focus on the specific requirements, at each  
196 Assurance Level (AL), against which Services must be assessed by Kantara-Accredited  
197 Assessors. They are divided into two parts:

198 1) **Organizational Criteria:**

199 These criteria address the general business and organizational conformity of  
200 services and their providers. They are generally referred-to as the 'CO-SAC';

201 2) **Operational Criteria:**

202 These criteria address operational conformity of credential management services  
203 and the necessary functions which they embrace. They are generally referred-to  
204 as the 'OP-SAC'.

### 205 3.2 Criteria Applicability

206 All criteria (i.e. CO-SAC and OP-SAC, at the applicable level) must be complied-with by  
207 all Full Service Provisions that are submitted for Approval under the Identity Assurance  
208 Framework (IAF).

209 Each Service Component within a Full Service Provision must comply with the CO-SAC  
210 and a defined sub-set of OP-SAC clauses which fall within the component's scope.

211 These criteria have been approved under the IAWG's governance rules as being suitable  
212 for use by Kantara-Accredited Assessors in the performance of their assessments of  
213 credentialing services for which a CSP is seeking Kantara Approval.

214 In the context of the Identity Assurance Framework, the status of this document is  
215 normative. An applicant's credential service shall comply with all applicable criteria  
216 within these SAC at their nominated AL(s).

217 This document describes the specific criteria that must be met to achieve each of the four  
218 ALs under the IAF. To be Approved under the IAF Identity Assurance Program and be  
219 granted the right to use Kantara Initiative Trust Mark, credential services must conform to  
220 all applicable criteria at the appropriate level.



### 221 3.3 Status and Readership

222 This document sets out **normative** Kantara requirements and is required reading for  
223 Kantara-Accredited Assessors and applicant Service Providers. It will also be of interest  
224 to those wishing to gain a detailed knowledge of the workings of the Kantara Initiative's  
225 Identity Assurance Framework. It sets out the Service Assessment Criteria to which  
226 credential services must conform in order to be granted Kantara Approval.

227 The description of criteria in this document is required reading for all organizations  
228 wishing to become Kantara-Approved credential services, and also for those wishing to  
229 become Kantara-Accredited Assessors. It is also recommended reading for those  
230 involved in the governance and day-to-day administration of the Identity Assurance  
231 Framework.

232 This document will also be of interest to those seeking a detailed understanding of the  
233 operation of the Identity Assurance Framework but who are not actively involved in its  
234 operations or in services that may fall within the scope of the Framework.

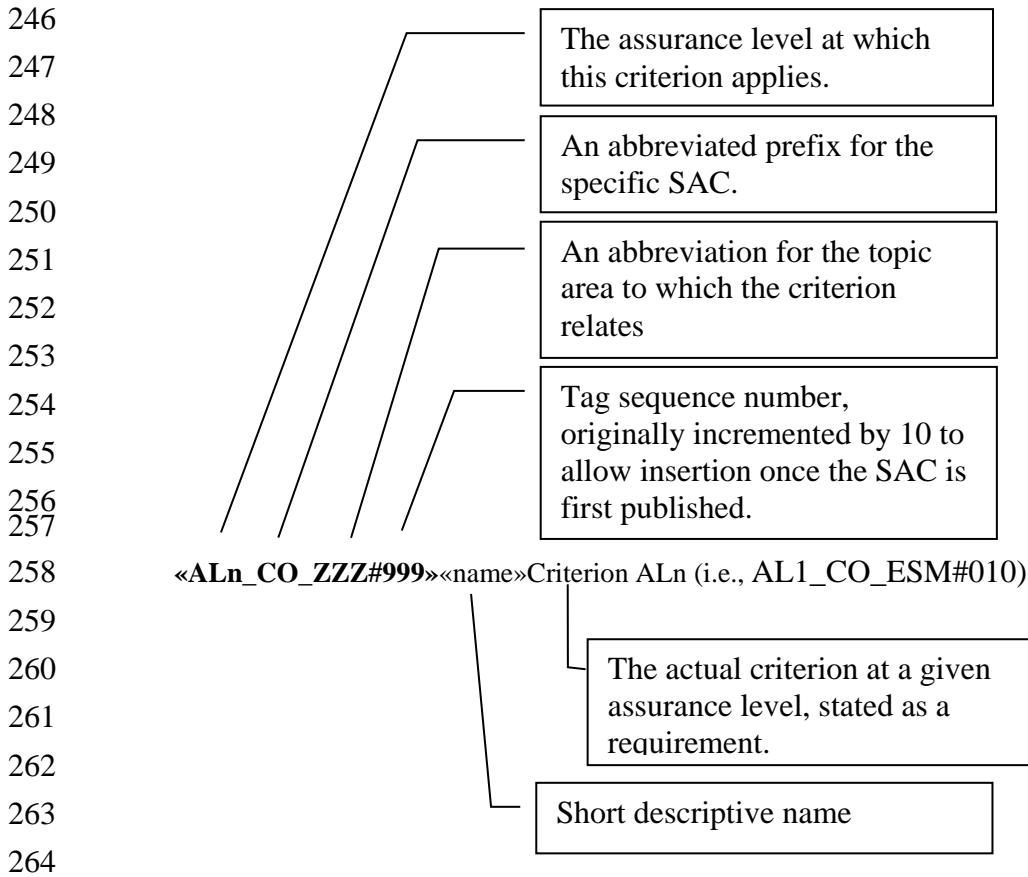
### 235 3.4 Criteria Descriptions

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

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

244

245 The criteria are described as follows:



265 When a given criterion changes (i.e. becomes more rigorous) at higher Assurance Levels

266 the new or revised text is **shown in bold** or '[Omitted]' is indicated where text has been

267 removed. With the obvious exception of AL1, when a criterion is first introduced it is

268 also shown in bold.

269 As noted in the above schematic, when originally prepared, the tags had numbers

270 incrementing in multiples of ten to permit the later insertion of additional criteria. Since

271 then there has been addition and withdrawal of criteria.

272 Where a criterion is not used in a given AL but is used at a higher AL its place is held by

273 the inclusion of a tag which is marked 'No stipulation'. A title and appropriate criteria

274 will be added at the higher AL which occupies that position. Since in general higher ALs

275 have a greater extent of criteria than lower ALs, where a given AL extends no further

276 through the numbering range, criteria beyond that value are by default omitted rather than

277 being included but marked 'No stipulation'.

278 Further, over time, some criteria have been removed, or withdrawn. In order to avoid the

279 re-use of that tag such tags are retained but marked 'Withdrawn'.

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

## 282 3.5 Terminology

283 All special terms used in this document are defined in the *IAF Glossary*, which can be  
284 found on Kantara's [Identity Assurance Framework - General Information page](#).

285 Note that when, in these criteria, the term 'Subscriber' is used it applies equally to  
286 'Subscriber' and 'Subject' as defined in the *IAF Glossary*, according to the context in  
287 which used. The term 'Subject' is used when the reference is explicitly toward that party.

## 288 4 COMMON ORGANIZATIONAL 289 SERVICE ASSESSMENT CRITERIA

---

290 The Service Assessment Criteria in this section establish the general business and  
291 organizational requirements for conformity of services and service providers at all  
292 Assurance Levels (AL) – refer to Section 2. These criteria are generally referred to  
293 elsewhere within IAWG documentation as CO-SAC and can be identified by their tag  
294 “ALn\_CO\_ xxxx”.

295 These criteria must be conformed-to by all applicants for Approval, whether for Service  
296 Components or Full Service Provision.

### 297 4.1 Assurance Level 1

#### 298 4.1.1 Enterprise and Service Maturity

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

302 An enterprise and its specified service must:

303 *ALI\_CO\_ESM#010 Established enterprise*

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

306 *ALI\_CO\_ESM#020 Withdrawn*

307 Withdrawn

308 *ALI\_CO\_ESM#030 Legal & Contractual compliance*

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

312 **Guidance:** ‘Understanding’ is implicitly the correct understanding. Both it and  
313 compliance are required because it could be that understanding is incomplete, incorrect or  
314 even absent, even though compliance is apparent, and similarly, correct understanding  
315 may not necessarily result in full compliance. The two are therefore complementary.

316 *ALI\_CO\_ESM#040 No stipulation*

317 *ALI\_CO\_ESM#050 Data Retention and Protection*

318 Specifically set out and demonstrate that it understands and complies with those legal and  
319 regulatory requirements incumbent upon it concerning the retention and destruction of

320 private and identifiable information (personal and business - i.e. its secure storage and  
321 protection against loss, accidental public exposure, and/or improper destruction) and the  
322 protection of Subjects' private information (against unlawful or unauthorized access,  
323 excepting that permitted by the information owner or required by due process).

324 *ALI\_CO\_ESM#055 Termination provisions*

325 Define the practices in place for the protection of Subjects' private and secret information  
326 related to their use of the service which must ensure the ongoing secure preservation and  
327 protection of legally required records and for the secure destruction and disposal of any  
328 such information whose retention is no longer legally required. Specific details of these  
329 practices must be made available.

330 **Guidance:** Termination covers the cessation of the business activities, the service  
331 provider itself ceasing business operations altogether, change of ownership of the service-  
332 providing business, and other similar events which change the status and/or operations of  
333 the service provider in any way which interrupts the continued provision of the specific  
334 service.

#### 335 **4.1.2 Notices and User information**

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

338 An enterprise and its specified service must:

339 *ALI\_CO\_NUI#010 General Service Definition*

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

343 **Guidance:** The intended user community encompasses potential and actual Subscribers,  
344 Subjects, and relying parties.

345 *ALI\_CO\_NUI#020 Service Definition inclusions*

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

348 a) a Privacy Policy

349

350 *ALI\_CO\_NUI#030 Due notification*

351 Have in place and follow appropriate policy and procedures to ensure that it notifies  
352 Users in a timely and reliable fashion of any changes to the Service Definition and any  
353 applicable Terms, Conditions, and Privacy Policy for the specified service.

354 *ALI\_CO\_NUI#040 User Acceptance*

355 Require Subscribers and Subjects to:

- 356 a) indicate, prior to receiving service, that they have read and accept the terms of  
357 service as defined in the Service Definition;  
358 b) at periodic intervals, determined by significant service provision events (e.g.  
359 issuance, re-issuance, renewal), re-affirm their understanding and observance of  
360 the terms of service;  
361 c) always provide full and correct responses to requests for information.

362 *ALI\_CO\_NUI#050 Record of User Acceptance*

363 Obtain a record (hard-copy or electronic) of the Subscriber's and Subject's acceptance of  
364 the terms and conditions of service, prior to initiating the service and thereafter at  
365 periodic intervals, determined by significant service provision events (e.g. re-issuance,  
366 renewal).

367 **4.1.3 No stipulation**

368 **4.1.4 No stipulation**

369 **4.1.5 No stipulation**

370 **4.1.6 No stipulation**

371 **4.1.7 Secure Communications**

372 *ALI\_CO\_SCO#010 No stipulation*

373 *ALI\_CO\_SCO#015 No stipulation*

374 *ALI\_CO\_SCO#016 No stipulation*

375 *ALI\_CO\_SCO#020 Limited access to shared secrets*

376 Ensure that:

- 377 a) access to shared secrets shall be subject to discretionary controls which permit  
378 access to those roles/applications needing such access;  
379 b) stored shared secrets are not held in their plaintext form unless given adequate  
380 physical or logical protection;  
381 c) any plaintext passwords or secrets are not transmitted across any public or  
382 unsecured network.

383

## 384 4.2 Assurance Level 2

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

### 388 4.2.1 Enterprise and Service Maturity

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

391 An enterprise and its specified service must:

392 *AL2\_CO\_ESM#010 Established enterprise*

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

395 *AL2\_CO\_ESM#020 Withdrawn*

396 Withdrawn

397 *AL2\_CO\_ESM#030 Legal & Contractual compliance*

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

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

408 *AL2\_CO\_ESM#040 Financial Provisions*

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

412 **Guidance:** The organization must show that it has a budgetary provision to operate the  
413 service for at least a twelve-month period, with a clear review of the budgetary planning  
414 within that period so as to keep the budgetary provisions extended. It must also show  
415 how it has determined the degree of liability protection required, in view of its exposure  
416 per 'service' and the number of users it has. This criterion helps ensure that Kantara  
417 Initiative does not grant Recognition to services that are not likely to be sustainable over  
418 at least this minimum period of time.

419 *AL2\_CO\_ESM#050 Data Retention and Protection*

420 Specifically set out and demonstrate that it understands and complies with those legal and  
421 regulatory requirements incumbent upon it concerning the retention and destruction of  
422 private and identifiable information (personal and business - i.e. its secure storage and  
423 protection against loss, accidental public exposure, and/or improper destruction) and the  
424 protection of Subjects' private information (against unlawful or unauthorized access,  
425 excepting that permitted by the information owner or required by due process).

426 **Guidance:** Note that whereas the criterion is intended to address unlawful or  
427 unauthorized access arising from malicious or careless actions (or inaction) some access  
428 may be unlawful UNLESS authorized by the Subscriber or Subject, or effected as a part  
429 of a specifically-executed legal process.

430 *AL2\_CO\_ESM#055 Termination provisions*

431 Define the practices in place for the protection of Subjects' private and secret information  
432 related to their use of the service which must ensure the ongoing secure preservation and  
433 protection of legally required records and for the secure destruction and disposal of any  
434 such information whose retention is no longer legally required. Specific details of these  
435 practices must be made available.

436 **Guidance:** Termination covers the cessation of the business activities, the service  
437 provider itself ceasing business operations altogether, change of ownership of the service-  
438 providing business, and other similar events which change the status and/or operations of  
439 the service provider in any way which interrupts the continued provision of the specific  
440 service.

441 **4.2.2 Notices and User Information/Agreements**

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

445 An enterprise and its specified service must:

446 *AL2\_CO\_NUI#010 General Service Definition*

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

451 **Guidance:** The intended user community encompasses potential and actual Subscribers,  
452 Subjects, and relying parties.

453 *AL2\_CO\_NUI#020 Service Definition inclusions*

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



- 456 a) Privacy, Identity Proofing & Verification, **Renewal/Re-issuance**, and  
457 **Revocation and Termination Policies**;  
458 b) **the country in or legal jurisdiction under which the service is operated**;  
459 c) **if different from the above, the legal jurisdiction under which Subscriber and**  
460 **any relying party agreements are entered into**;  
461 d) **applicable legislation with which the service complies**;  
462 e) **obligations incumbent upon the CSP**;  
463 f) **obligations incumbent upon each class of user of the service, e.g. Relying**  
464 **Parties, Subscribers and Subjects**;  
465 g) **notifications and guidance for relying parties, especially in respect of actions**  
466 **they are expected to take should they choose to rely upon the service**;  
467 h) **statement of warranties**;  
468 i) **statement of liabilities toward Subscribers, Subjects and Relying Parties**;  
469 j) **procedures for notification of changes to terms and conditions**;  
470 k) **steps the CSP will take in the event that it chooses or is obliged to terminate**  
471 **the service**;  
472 l) **availability of the specified service *per se* and of its help desk facility.**

473 *AL2\_CO\_NUI#025 AL2 Configuration Specification*

474 **Make available a detailed specification (accounting for the service specification and**  
475 **architecture) which defines how a user of the service can configure it so as to be**  
476 **assured of receiving at least an AL2 baseline service.**

477 *AL2\_CO\_NUI#030 Due notification*

478 Have in place and follow appropriate policy and procedures to ensure that it notifies  
479 Subscribers and Subjects in a timely and reliable fashion of any changes to the Service  
480 Definition and any applicable Terms, Conditions, Fees, and Privacy Policy for the  
481 specified service, **and provide a clear means by which Subscribers and Subjects must**  
482 **indicate that they wish to accept the new terms or terminate their subscription.**

483 *AL2\_CO\_NUI#040 User Acceptance*

484 Require Subscribers and Subjects to:

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

491 *AL2\_CO\_NUI#050 Record of User Acceptance*

492 Obtain a record (hard-copy or electronic) of the Subscriber's and Subject's acceptance of  
493 the terms and conditions of service, prior to initiating the service and thereafter at  
494 periodic intervals, determined by significant service provision events (e.g. re-issuance,  
495 renewal) **and otherwise at least once every five years.**

496 *AL2\_CO\_NUI#060 Withdrawn*  
497 Withdrawn.

498 *AL2\_CO\_NUI#070 Change of Subscriber Information*  
499 **Require and provide the mechanisms for Subscribers and Subjects to provide in a**  
500 **timely manner full and correct amendments should any of their recorded**  
501 **information change, as required under the terms of their use of the service, and only**  
502 **after the Subscriber's and/or Subject's identity has been authenticated.**

503 *AL2\_CO\_NUI#080 Withdrawn*  
504 Withdrawn.

### 505 **4.2.3 Information Security Management**

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

511 An enterprise and its specified service must:

512 *AL2\_CO\_ISM#010 Documented policies and procedures*  
513 **Have documented all security-relevant administrative, management, and technical**  
514 **policies and procedures. The enterprise must ensure that these are based upon**  
515 **recognized standards, published references or organizational guidelines, are**  
516 **adequate for the specified service, and are implemented in the manner intended.**

517 *AL2\_CO\_ISM#020 Policy Management and Responsibility*  
518 **Have a clearly defined managerial role, at a senior level, in which full responsibility**  
519 **for the business's security policies is vested and from which review, approval, and**  
520 **promulgation of policy and related procedures is applied and managed. The latest**  
521 **approved versions of these policies must be applied at all times.**

522 *AL2\_CO\_ISM#030 Risk Management*  
523 **Demonstrate a risk management methodology that adequately identifies and**  
524 **mitigates risks related to the specified service and its user community.**

525 *AL2\_CO\_ISM#040 Continuity of Operations Plan*  
526 **Have and keep updated a Continuity of Operations Plan that covers disaster**  
527 **recovery and the resilience of the specified service.**

528 *AL2\_CO\_ISM#050 Configuration Management*  
529 **Demonstrate that there is in place a configuration management system that at least**  
530 **includes:**

531 a) **version control for software system components;**

532 **b) timely identification and installation of all organizationally-approved patches**  
533 **for any software used in the provisioning of the specified service.**

534 *AL2\_CO\_ISM#060 Quality Management*

535 **Demonstrate that there is in place a quality management system that is appropriate**  
536 **for the specified service.**

537 *AL2\_CO\_ISM#070 System Installation and Operation Controls*

538 **Apply controls during system development, procurement installation, and operation**  
539 **that protect the security and integrity of the system environment, hardware,**  
540 **software, and communications.**

541 *AL2\_CO\_ISM#080 Internal Service Audit*

542 **Be subjected to a first-party audit at least once every 12 months for the effective**  
543 **provision of the specified service by internal audit functions of the enterprise**  
544 **responsible for the specified service, unless it can show that by reason of its**  
545 **organizational size or due to other operational restrictions it is unreasonable to be so**  
546 **audited.**

547 **Guidance:** ‘First-party’ audits are those undertaken by an independent part of the same  
548 organization which offers the service. The auditors cannot be involved in the  
549 specification, development or operation of the service.

550 Using a ‘third-party’ (i.e. independent) auditor (i.e. one having no relationship with the  
551 Service Provider nor any vested interests in the outcome of the assessment other than  
552 their professional obligations to perform the assessment objectively and independently)  
553 should be considered when the organization cannot easily provide truly independent  
554 internal resources but wishes to benefit from the value which audits can provide, and for  
555 the purposes of fulfilling Kantara’s needs, a formal Kantara Assessment performed by an  
556 Accredited Assessor should be considered as such.

557 *AL2\_CO\_ISM#090 Withdrawn*

558 Withdrawn.

559 *AL2\_CO\_ISM#100 Audit Records*

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

566 *AL2\_CO\_ISM#110 Withdrawn*

567 Withdrawn.

#### 568 4.2.4 Security-relevant Event (Audit) Records

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

571 An enterprise and its specified service must:

572 *AL2\_CO\_SER#010 Security event logging*

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

578 **Guidance:** It is sufficient that the accuracy of the time source is based upon an internal  
579 computer/system clock synchronized to an internet time source. The time source need  
580 not be authenticable.

#### 581 4.2.5 Operational infrastructure

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

585 An enterprise and its specified service must:

586 *AL2\_CO\_OPN#010 Technical security*

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

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

595 *AL2\_CO\_OPN#020 Defined security roles*

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

603 *AL2\_CO\_OPN#030 Personnel recruitment*

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

607 *AL2\_CO\_OPN#040 Personnel skills*

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

613 *AL2\_CO\_OPN#050 Adequacy of Personnel resources*

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

616 *AL2\_CO\_OPN#060 Physical access control*

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

- 618 a) **access to sensitive areas is restricted to authorized personnel;**
- 619 b) **all removable media and paper documents containing sensitive information**  
620 **as plain-text are stored in secure containers;**
- 621 c) **a minimum of two persons is required to enable access to any cryptographic**  
622 **modules.**

623 *AL2\_CO\_OPN#070 Logical access control*

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

#### 626 **4.2.6 External Services and Components**

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

630 An enterprise and its specified service must:

631 *AL2\_CO\_ESC#010 Contracted policies and procedures*

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

637 *AL2\_CO\_ESC#020 Visibility of contracted parties*

638 **Where the enterprise uses external suppliers for specific packaged components of**  
639 **the service or for resources that are integrated with its own operations and under its**  
640 **control, ensure that the suppliers' compliance with contractually-stipulated policies**

641 and procedures, and thus with IAF Service Assessment Criteria, can be  
642 independently verified, and subsequently monitored if necessary.

#### 643 4.2.7 Secure Communications

644 An enterprise and its specified service must:

645 *AL2\_CO\_SCO#010 Secure remote communications*

646 **If the specific service components are located remotely from and communicate over**  
647 **a public or unsecured network with other service components or other CSPs it**  
648 **services, or parties requiring access to the CSP's services, each transaction must be**  
649 **cryptographically protected using an encryption method approved by a national**  
650 **technical authority or other generally-recognized authoritative body, by either:**

- 651 a) **implementing mutually-authenticated protected sessions; or**  
652 b) **time-stamped or sequenced messages signed by their source and encrypted**  
653 **for their recipient.**

654 **Guidance:** The reference to “parties requiring access to the CSP's services” is intended  
655 to cover SP 800-63-2's reference to RPs (see cross-mapped EZP 63-2 clause).

656 *AL2\_CO\_SCO#015 Verification / Authentication confirmation messages*

657 **Ensure that any verification or confirmation of authentication messages, which**  
658 **assert either that a weakly bound credential is valid or that a strongly bound**  
659 **credential has not been subsequently revoked, are logically bound to the credential**  
660 **and that the message, the logical binding, and the credential are all transmitted**  
661 **within a single integrity-protected session between the service and the Verifier /**  
662 **Relying Party.**

663 *AL2\_CO\_SCO#016 Withdrawn*

664 Now AL2\_CM\_RVP#045

665 *AL2\_CO\_SCO#020 Limited access to shared secrets*

666 Ensure that:

- 667 a) access to shared secrets shall be subject to discretionary controls that only permit  
668 access by those roles/applications requiring such access;  
669 b) stored shared secrets are not held in their plaintext form unless given adequate  
670 physical or logical protection;  
671 c) **any long-term (i.e., not session) shared secrets are revealed only to the**  
672 **Subject or to the CSP's direct agents (bearing in mind (a) above).**  
673

674 **In addition, these roles should be defined and documented by the CSP in accordance**  
675 **with AL2\_CO\_OPN#020 above.**

676 *AL2\_CO\_SCO#030 Logical protection of shared secrets*

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

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

685



## 686 4.3 Assurance Level 3

687 Achieving AL3 requires meeting more stringent criteria in addition to all criteria required  
688 to achieve AL2.

### 689 4.3.1 Enterprise and Service Maturity

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

692 An enterprise and its specified service must:

693 *AL3\_CO\_ESM#010 Established enterprise*

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

696 *AL3\_CO\_ESM#020 Withdrawn*

697 Withdrawn

698 *AL3\_CO\_ESM#030 Legal & Contractual compliance*

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

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

709 *AL3\_CO\_ESM#040 Financial Provisions*

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

713 **Guidance:** The organization must show that it has a budgetary provision to operate the  
714 service for at least a twelve-month period, with a clear review of the budgetary planning  
715 within that period so as to keep the budgetary provisions extended. It must also show  
716 how it has determined the degree of liability protection required, in view of its exposure  
717 per 'service' and the number of users it has. This criterion helps ensure that Kantara  
718 Initiative does not grant Recognition to services that are not likely to be sustainable over  
719 at least this minimum period of time.

720 *AL3\_CO\_ESM#050 Data Retention and Protection*



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

727 *AL3\_CO\_ESM#055 Termination provisions*

728 Define the practices in place for the protection of Subjects' private and secret information  
729 related to their use of the service which must ensure the ongoing secure preservation and  
730 protection of legally required records and for the secure destruction and disposal of any  
731 such information whose retention is no longer legally required. Specific details of these  
732 practices must be made available.

733 **Guidance:** Termination covers the cessation of the business activities, the service  
734 provider itself ceasing business operations altogether, change of ownership of the service-  
735 providing business, and other similar events which change the status and/or operations of  
736 the service provider in any way which interrupts the continued provision of the specific  
737 service.

738 *AL3\_CO\_ESM#060 Ownership*

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

742 *AL3\_CO\_ESM#070 Independent management and operations*

743 **Demonstrate that, for the purposes of providing the specified service, its**  
744 **management and operational structures are distinct, autonomous, have discrete**  
745 **legal accountability, and operate according to separate policies, procedures, and**  
746 **controls.**

#### 747 **4.3.2 Notices and User Information**

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

751 An enterprise and its specified service must:

752 *AL3\_CO\_NUI#010 General Service Definition*

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

757 **Guidance:** The intended user community encompasses potential and actual Subscribers,  
758 Subjects and relying parties.

759 *AL3\_CO\_NUI#020 Service Definition inclusions*

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

- 762 a) Privacy, Identity Proofing & Verification, **Renewal/Re-issuance**, and Revocation  
763 and Termination Policies; )
- 764 b) the country in or the legal jurisdiction under which the service is operated;
- 765 c) if different to the above, the legal jurisdiction under which Subscriber and any  
766 relying party agreements are entered into;
- 767 d) applicable legislation with which the service complies;
- 768 e) obligations incumbent upon the CSP;
- 769 f) obligations incumbent upon each class of user of the service, e.g. **Relying Parties**,  
770 **Subscribers** and **Subjects**, ...;
- 771 g) notifications and guidance for relying parties, especially in respect of actions they  
772 are expected to take should they choose to rely upon the service's product;
- 773 h) statement of warranties;
- 774 i) statement of liabilities toward both Subjects and Relying Parties;
- 775 j) procedures for notification of changes to terms and conditions;
- 776 k) steps the CSP will take in the event that it chooses or is obliged to terminate the  
777 service;
- 778 l) availability of the specified service *per se* and of its help desk facility.

779 *AL3\_CO\_NUI#025 AL3 Configuration Specification*

780 Make available a detailed specification (accounting for the service specification and  
781 architecture) which defines how a user of the service can configure it so as to be assured  
782 of receiving at least an **AL3** baseline service.

783 *AL3\_CO\_NUI#030 Due notification*

784 Have in place and follow appropriate policy and procedures to ensure that it notifies  
785 Subscribers and Subjects in a timely and reliable fashion of any changes to the Service  
786 Definition and any applicable Terms, Conditions, Fees, and Privacy Policy for the  
787 specified service, and provide a clear means by which Subscribers and Subjects must  
788 indicate that they wish to accept the new terms or terminate their subscription.

789 *AL3\_CO\_NUI#040 User Acceptance*

790 Require Subscribers and Subjects to:

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

797 *AL3\_CO\_NUI#050 Record of User Acceptance*

798 Obtain a record (hard-copy or electronic) of the Subscriber's and Subject's acceptance of  
799 the terms and conditions of service, prior to initiating the service and thereafter reaffirm  
800 the agreement at periodic intervals, determined by significant service provision events  
801 (e.g. re-issuance, renewal) and otherwise at least once every five years.

802 *AL3\_CO\_NUI#060 Withdrawn*  
803 Withdrawn.

804 *AL3\_CO\_NUI#070 Change of Subscriber Information*  
805 Require and provide the mechanisms for Subscribers and Subjects to provide in a timely  
806 manner full and correct amendments should any of their recorded information change, as  
807 required under the terms of their use of the service, and only after the Subscriber's and/or  
808 Subject's identity has been authenticated.

809 *AL3\_CO\_NUI#080 Withdrawn*  
810 Withdrawn.

### 811 **4.3.3 Information Security Management**

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

817 An enterprise and its specified service must:

818 *AL3\_CO\_ISM#010 Documented policies and procedures*  
819 Have documented all security-relevant administrative management and technical policies  
820 and procedures. The enterprise must ensure that these are based upon recognized  
821 standards, published references or organizational guidelines, are adequate for the  
822 specified service, and are implemented in the manner intended.

823 *AL3\_CO\_ISM#020 Policy Management and Responsibility*  
824 Have a clearly defined managerial role, at a senior level, where full responsibility for the  
825 business' security policies is vested and from which review, approval, and promulgation  
826 of policy and related procedures is applied and managed. The latest approved versions of  
827 these policies must be applied at all times.

828 *AL3\_CO\_ISM#030 Risk Management*  
829 Demonstrate a risk management methodology that adequately identifies and mitigates  
830 risks related to the specified service and its user community **and must show that a risk**  
831 **assessment review is performed at least once every six months, such as adherence to**  
832 **CobIT or [IS27001] practices.**

833 *AL3\_CO\_ISM#040 Continuity of Operations Plan*

834 Have and keep updated a continuity of operations plan that covers disaster recovery and  
835 the resilience of the specified service **and must show that a review of this plan is**  
836 **performed at least once every six months.**

837 *AL3\_CO\_ISM#050 Configuration Management*

838 Demonstrate that there is in place a configuration management system that at least  
839 includes:

- 840 a) version control for software system components;
- 841 b) timely identification and installation of all organizationally-approved patches for  
842 any software used in the provisioning of the specified service;
- 843 c) **version control and managed distribution for all documentation associated**  
844 **with the specification, management, and operation of the system, covering**  
845 **both internal and publicly available materials.**

846 *AL3\_CO\_ISM#060 Quality Management*

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

849 *AL3\_CO\_ISM#070 System Installation and Operation Controls*

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

- 853 a) **the software and hardware development environments, for customized**  
854 **components;**
- 855 b) **the procurement process for commercial off-the-shelf (COTS) components;**
- 856 c) **contracted consultancy/support services;**
- 857 d) **shipment of system components;**
- 858 e) **storage of system components;**
- 859 f) **installation environment security;**
- 860 g) **system configuration;**
- 861 h) **transfer to operational status.**

862 *AL3\_CO\_ISM#080 Internal Service Audit*

863 Be subjected to a first-party audit at least once every 12 months for the effective  
864 provision of the specified service by internal audit functions of the enterprise responsible  
865 for the specified service, unless it can show that by reason of its organizational size or due  
866 to other **justifiable** operational restrictions it is unreasonable to be so audited.

867 **Guidance:** 'First-party' audits are those undertaken by an independent part of the same  
868 organization which offers the service. The auditors cannot be involved in the  
869 specification, development or operation of the service.

870 Management systems require that there be internal audit conducted as an inherent part of  
871 management review processes. Any third-party (i.e. independent) audit of the  
872 management system is intended to show that the internal management system controls are

873 being appropriately applied, and for the purposes of fulfilling Kantara's needs, a formal  
874 Kantara Assessment performed by an Accredited Assessor should be considered as such.

875 *AL3\_CO\_ISM#090 Withdrawn*  
876 Withdrawn.

877 *AL3\_CO\_ISM#100 Audit Records*

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

884 *AL3\_CO\_ISM#110 Withdrawn*  
885 Withdrawn.

886 *AL3\_CO\_ISM#120 Best Practice Security Management*

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

893 **Guidance:** The auditors determining that this ISMS meets the above requirement must  
894 be appropriately qualified in assessing the specific management system or methodology  
895 applied.

#### 896 **4.3.4 Security-Relevant Event (Audit) Records**

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

899 An enterprise and its specified service must:

900 *AL3\_CO\_SER#010 Security Event Logging*

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

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

### 909 4.3.5 Operational Infrastructure

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

913 An enterprise and its specified service must:

#### 914 *AL3\_CO\_OPN#010 Technical security*

915 Demonstrate that the technical controls employed will provide the level of security  
916 protection required by the risk assessment and the ISMS, or other IT security  
917 management methods recognized by a government or professional body, and that these  
918 controls are effectively integrated with the applicable procedural and physical security  
919 measures.

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

#### 923 *AL3\_CO\_OPN#020 Defined security roles*

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

#### 931 *AL3\_CO\_OPN#030 Personnel recruitment*

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

#### 937 *AL3\_CO\_OPN#040 Personnel skills*

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

#### 943 *AL3\_CO\_OPN#050 Adequacy of Personnel resources*

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

#### 946 *AL3\_CO\_OPN#060 Physical access control*

947 Apply physical access control mechanisms to ensure that:



- 948 a) access to sensitive areas is restricted to authorized personnel;  
949 b) all removable media and paper documents containing sensitive information as  
950 plain-text are stored in secure containers;  
951 c) a minimum of two persons are required to enable access to any cryptographic  
952 modules;  
953 d) there is 24/7 monitoring for unauthorized intrusions.

954 *AL3\_CO\_OPN#070 Logical access control*

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

### 957 **4.3.6 External Services and Components**

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

961 An enterprise and its specified service must:

962 *AL3\_CO\_ESC#010 Contracted policies and procedures*

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

968 *AL3\_CO\_ESC#020 Visibility of contracted parties*

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

### 974 **4.3.7 Secure Communications**

975 An enterprise and its specified service must:

976 *AL3\_CO\_SCO#010 Secure remote communications*

977 If the specific service components are located remotely from and communicate over a  
978 public or unsecured network with other service components or other CSPs it services, or  
979 parties requiring access to the CSP's services, each transaction must be cryptographically  
980 protected using an encryption method approved by a recognized national technical  
981 authority or other generally-recognized authoritative body, by either:

- 982 a) implementing mutually-authenticated protected sessions; or  
983 b) time-stamped or sequenced messages signed by their source and encrypted for their  
984 recipient.

985 **Guidance:** The reference to “parties requiring access to the CSP’s services” is intended  
986 to cover SP 800-63-2’s reference to RPs (see cross-mapped EZP 63-2 clause ).

987 *AL3\_CO\_SCO#015 Verification / Authentication confirmation messages*  
988 Ensure that any verification or confirmation of authentication messages, which assert  
989 either that a weakly bound credential is valid or that a strongly bound credential has not  
990 been subsequently revoked, is logically bound to the credential and that the message, the  
991 logical binding, and the credential are all transmitted within a single integrity-protected  
992 session between the service and the Verifier / Relying Party.

993 *AL3\_CO\_SCO#016 Withdrawn*

994 *AL3\_CO\_SCO#020 Limited access to shared secrets*  
995 Ensure that:

- 996 a) access to shared secrets shall be subject to discretionary controls that permit  
997 access to those roles/applications requiring such access;
- 998 b) stored shared secrets are **encrypted such that:**
- 999 **i the encryption key for the shared secret file is encrypted under a key**  
1000 **held in either a FIPS 140-2 [FIPS140-2] Level 2 (or higher) validated**  
1001 **hardware cryptographic module or any FIPS 140-2 Level 3 or 4**  
1002 **validated cryptographic module, or equivalent, as established by a**  
1003 **recognized national technical authority, and decrypted only as**  
1004 **immediately required for an authentication operation;**
- 1005 **ii they are protected as a key within the boundary of either a FIPS 140-2**  
1006 **Level 2 (or higher) validated hardware cryptographic module or any**  
1007 **FIPS 140-2 Level 3 or 4 validated cryptographic module, or**  
1008 **equivalent, as established by a recognized national technical**  
1009 **authority, and are not exported from the module in plaintext;**
- 1010 **iii Omitted;**
- 1011 c) any long-term (i.e., not session) shared secrets are revealed only to the Subject  
1012 and the CSP’s direct agents (bearing in mind (a) above).

1013  
1014 **These roles should be defined and documented by the CSP in accordance with**  
1015 **AL3\_CO\_OPN#020 above.**

1016



## 1017 4.4 Assurance Level 4

1018 Achieving AL4 requires meeting even more stringent criteria in addition to the criteria  
1019 required to achieve AL3.

### 1020 4.4.1 Enterprise and Service Maturity

1021 Criteria in this section address the establishment of the enterprise offering the service and  
1022 its basic standing as a legal and operational business entity.

1023 An enterprise and its specified service must:

1024 *ALA\_CO\_ESM#010 Established enterprise*

1025 Be a valid legal entity and a person with legal authority to commit the organization must  
1026 submit the signed assessment package.

1027 *ALA\_CO\_ESM#020 Withdrawn*

1028 Withdrawn

1029 *ALA\_CO\_ESM#030 Legal & Contractual compliance*

1030 Demonstrate that it understands and complies with any legal requirements incumbent on  
1031 it in connection with operation and delivery of the specified service, accounting for all  
1032 jurisdictions within which its services may be offered. Any specific contractual  
1033 requirements shall also be identified.

1034 **Guidance:** Kantara Initiative will not recognize a service which is not fully released for  
1035 the provision of services to its intended user/client community. Systems, or parts thereof,  
1036 which are not fully proven and released shall not be considered in an assessment and  
1037 therefore should not be included within the scope of the assessment package. Parts of  
1038 systems still under development, or even still being planned, are therefore ineligible for  
1039 inclusion within the scope of assessment.

1040 *ALA\_CO\_ESM#040 Financial Provisions*

1041 Provide documentation of financial resources that allow for the continued operation of the  
1042 service and demonstrate appropriate liability processes and procedures that satisfy the  
1043 degree of liability exposure being carried.

1044 **Guidance:** The organization must show that it has a budgetary provision to operate the  
1045 service for at least a twelve-month period, with a clear review of the budgetary planning  
1046 within that period so as to keep the budgetary provisions extended. It must also show  
1047 how it has determined the degree of liability protection required, in view of its exposure  
1048 per 'service' and the number of users it has. This criterion helps ensure that Kantara  
1049 Initiative does not grant Recognition to services that are not likely to be sustainable over  
1050 at least this minimum period of time.

1051 *ALA\_CO\_ESM#050 Data Retention and Protection*

1052 Specifically set out and demonstrate that it understands and complies with those legal and  
1053 regulatory requirements incumbent upon it concerning the retention and destruction of  
1054 private and identifiable information (personal and business) (i.e. its secure storage and  
1055 protection against loss, accidental public exposure, and/or improper destruction) and the  
1056 protection of private information (against unlawful or unauthorized access excepting that  
1057 permitted by the information owner or required by due process).

1058 *ALA\_CO\_ESM#055 Termination provisions*

1059 Define the practices in place for the protection of Subjects' private and secret information  
1060 related to their use of the service which must ensure the ongoing secure preservation and  
1061 protection of legally required records and for the secure destruction and disposal of any  
1062 such information whose retention is no longer legally required. Specific details of these  
1063 practices must be made available.

1064 **Guidance:** Termination covers the cessation of the business activities, the service  
1065 provider itself ceasing business operations altogether, change of ownership of the service-  
1066 providing business, and other similar events which change the status and/or operations of  
1067 the service provider in any way which interrupts the continued provision of the specific  
1068 service.

1069 *ALA\_CO\_ESM#060 Ownership*

1070 If the enterprise named as the CSP is a part of a larger entity, the nature of the relationship  
1071 with its parent organization, shall be disclosed to the assessors and, on their request, to  
1072 customers.

1073 *ALA\_CO\_ESM#070 Independent Management and Operations*

1074 Demonstrate that, for the purposes of providing the specified service, its management and  
1075 operational structures are distinct, autonomous, have discrete legal accountability, and  
1076 operate according to separate policies, procedures, and controls.

1077 **4.4.2 Notices and Subscriber Information/Agreements**

1078 Criteria in this section address the publication of information describing the service and  
1079 the manner of and any limitations upon its provision, and how users are required to accept  
1080 those terms.

1081 An enterprise and its specified service must:

1082 *ALA\_CO\_NUI#010 General Service Definition*

1083 Make available to the intended user community a Service Definition that includes all  
1084 applicable Terms, Conditions, and Fees, including any limitations of its usage, and  
1085 definitions of any terms having specific intention or interpretation. Specific provisions  
1086 are stated in further criteria in this section.

1087 **Guidance:** The intended user community encompasses potential and actual Subscribers,  
1088 Subjects, and relying parties.

1089 *ALA\_CO\_NUI#020 Service Definition inclusions*

- 1090 Make available a Service Definition for the specified service containing clauses that  
1091 provide the following information:
- 1092 a) Privacy, Identity Proofing & Verification, **Renewal/Re-issuance**, and Revocation  
1093 and Termination Policies;
  - 1094 b) the country in or legal jurisdiction under which the service is operated;
  - 1095 c) if different to the above, the legal jurisdiction under which Subscriber and any  
1096 relying party agreements are entered into;
  - 1097 d) applicable legislation with which the service complies;
  - 1098 e) obligations incumbent upon the CSP;
  - 1099 f) obligations incumbent upon the Subscriber and Subject;
  - 1100 g) notifications and guidance for relying parties, especially in respect of actions they  
1101 are expected to take should they choose to rely upon the service's product;
  - 1102 h) statement of warranties;
  - 1103 i) statement of liabilities toward both Subjects and Relying Parties;
  - 1104 j) procedures for notification of changes to terms and conditions;
  - 1105 k) steps the CSP will take in the event that it chooses or is obliged to terminate the  
1106 service;
  - 1107 l) availability of the specified service per se and of its help desk facility.

1108 *ALA\_CO\_NUI#025 ALA Configuration Specification*

1109 Make available a detailed specification (accounting for the service specification and  
1110 architecture) which defines how a user of the service can configure it so as to be assured  
1111 of receiving at least an **AL4** baseline service.

1112 *ALA\_CO\_NUI#030 Due Notification*

1113 Have in place and follow appropriate policy and procedures to ensure that it notifies  
1114 Subscribers and Subjects in a timely and reliable fashion of any changes to the Service  
1115 Definition and any applicable Terms, Conditions, Fees, and Privacy Policy for the  
1116 specified service, and provide a clear means by which Subscribers and Subjects must  
1117 indicate that they wish to accept the new terms or terminate their subscription.

1118 *ALA\_CO\_NUI#040 User Acceptance*

1119 Require Subscribers and Subjects to:

- 1120 a) indicate, prior to receiving service, that they have read and accept the terms of  
1121 service as defined in the Service Definition, thereby indicating their properly-  
1122 informed opt-in;
- 1123 b) at periodic intervals, determined by significant service provision events (e.g.  
1124 issuance, re-issuance, renewal) and otherwise at least once every five years, re-  
1125 affirm their understanding and observance of the terms of service;
- 1126 c) always provide full and correct responses to requests for information.

1127 *ALA\_CO\_NUI#050 Record of User Acceptance*

1128 Obtain a record (hard-copy or electronic) of the Subscriber's and Subject's acceptance of  
1129 the terms and conditions of service, prior to initiating the service and thereafter reaffirm

1130 the agreement at periodic intervals, determined by significant service provision events  
1131 (e.g. issuance, re-issuance, renewal) and otherwise at least once every five years.

1132 *ALA\_CO\_NUI#060 Withdrawn*  
1133 Withdrawn.

1134 *ALA\_CO\_NUI#070 Change of Subscriber Information*  
1135 *Require and provide the mechanisms for Subscribers and Subjects to provide in a timely*  
1136 *manner full and correct amendments should any of their recorded information change, as*  
1137 *required under the terms of their use of the service, and only after the Subscriber's and/or*  
1138 *Subject's identity has been authenticated.*

1139 *ALA\_CO\_NUI#080 Withdrawn*  
1140 Withdrawn.

#### 1141 **4.4.3 Information Security Management**

1142 These criteria address the way in which the enterprise manages the security of its  
1143 business, the specified service, and information it holds relating to its user community.  
1144 This section focuses on the key components that comprise a well-established and  
1145 effective Information Security Management System (ISMS), or other IT security  
1146 management methodology recognized by a government or professional body.

1147 An enterprise and its specified service must:

1148 *ALA\_CO\_ISM#010 Documented policies and procedures*  
1149 Have documented all security-relevant administrative, management, and technical  
1150 policies and procedures. The enterprise must ensure that these are based upon recognized  
1151 standards, published references, or organizational guidelines, are adequate for the  
1152 specified service, and are implemented in the manner intended.

1153 *ALA\_CO\_ISM#020 Policy Management and Responsibility*  
1154 Have a clearly defined managerial role, at a senior level, where full responsibility for the  
1155 business' security policies is vested and from which review, approval, and promulgation  
1156 of policy and related procedures is applied and managed. The latest approved versions of  
1157 these policies must be applied at all times.

1158 *ALA\_CO\_ISM#030 Risk Management*  
1159 Demonstrate a risk management methodology that adequately identifies and mitigates  
1160 risks related to the specified service and its user community and must show that on-going  
1161 risk assessment review is conducted as a part of the business' procedures, such as  
1162 adherence to **CobIT** or [[IS27001](#)] methods.

1163 *ALA\_CO\_ISM#040 Continuity of Operations Plan*

1164 Have and keep updated a continuity of operations plan that covers disaster recovery and  
1165 the resilience of the specified service and must show that **on-going review of this plan is**  
1166 **conducted as a part of the business' procedures.**

1167 *ALA\_CO\_ISM#050 Configuration Management*

1168 Demonstrate that there is in place a configuration management system that at least  
1169 includes:

- 1170 a) version control for software system components;
- 1171 b) timely identification and installation of all organizationally-approved patches for  
1172 any software used in the provisioning of the specified service;
- 1173 c) version control and managed distribution for all documentation associated with  
1174 the specification, management, and operation of the system, covering both  
1175 internal and publicly available materials.

1176 *ALA\_CO\_ISM#060 Quality Management*

1177 Demonstrate that there is in place a quality management system that is appropriate for the  
1178 specified service.

1179 *ALA\_CO\_ISM#070 System Installation and Operation Controls*

1180 Apply controls during system development, procurement, installation, and operation that  
1181 protect the security and integrity of the system environment, hardware, software, and  
1182 communications having particular regard to:

- 1183 a) the software and hardware development environments, for customized  
1184 components;
- 1185 b) the procurement process for commercial off-the-shelf (COTS) components;
- 1186 c) contracted consultancy/support services;
- 1187 d) shipment of system components;
- 1188 e) storage of system components;
- 1189 f) installation environment security;
- 1190 g) system configuration;
- 1191 h) transfer to operational status.

1192 *ALA\_CO\_ISM#080 Internal Service Audit*

1193 Be subjected to a first-party audit at least once every 12 months for the effective  
1194 provision of the specified service by internal audit functions of the enterprise responsible  
1195 for the specified service, unless it can show that by reason of its organizational size or due  
1196 to other justifiable operational restrictions it is unreasonable to be so audited.

1197 **Guidance:** 'First-party' audits are those undertaken by an independent part of the same  
1198 organization which offers the service. The auditors cannot be involved in the  
1199 specification, development or operation of the service.

1200 Management systems require that there be internal audit conducted as an inherent part of  
1201 management review processes. **Any third-party (i.e. independent)** audit of the  
1202 management system is intended to show that the internal management system controls are

1203 being appropriately applied, and for the purposes of fulfilling Kantara's needs, a formal  
1204 Kantara Assessment performed by an Accredited Assessor should be considered as such.

1205 *ALA\_CO\_ISM#090 Withdrawn*  
1206 Withdrawn.

1207 *ALA\_CO\_ISM#100 Audit Records*

1208 Retain records of all audits, both internal and independent, for a period which, as a  
1209 minimum, fulfills its legal obligations and otherwise for greater periods either as it may  
1210 have committed to in its Service Definition or required by any other obligations it has  
1211 with/to a Subscriber or Subject, and which in any event is not less than 36 months. Such  
1212 records must be held securely and be protected against unauthorized access loss,  
1213 alteration, public disclosure, or unapproved destruction.

1214 *ALA\_CO\_ISM#110 Withdrawn*  
1215 Withdrawn.

1216 *ALA\_CO\_ISM#120 Best Practice Security Management*

1217 Have in place a **certified** Information Security Management System (ISMS), or other IT  
1218 security management methodology recognized by a government or professional body, that  
1219 **has been assessed and found to be in compliance with the requirements of**  
1220 **ISO/IEC 27001 [IS27001] and which applies and is appropriate to the CSP in**  
1221 **question.** All requirements expressed in preceding criteria in this section must *inter alia*  
1222 fall wholly within the scope of this ISMS, or the selected recognized alternative.

#### 1223 **4.4.4 Security-Related (Audit) Records**

1224 The criteria in this section are concerned with the need to provide an auditable log of all  
1225 events that are pertinent to the correct and secure operation of the service.

1226 An enterprise and its specified service must:

1227 *ALA\_CO\_SER#010 Security Event Logging*

1228 Maintain a log of all relevant security events concerning the operation of the service,  
1229 together with a **precise** record of the time at which the event occurred (time-stamp)  
1230 **provided by a trusted time-source** and retain such records with appropriate protection  
1231 and controls to ensure successful retrieval, accounting for service definition, risk  
1232 management requirements, applicable legislation, and organizational policy.

1233 **Guidance:** The trusted time source could be an external trusted service or a network time  
1234 server or other hardware timing device. The time source must be not only precise but  
1235 authenticatable as well.



#### 1236 4.4.5 Operational Infrastructure

1237 The criteria in this section address the infrastructure within which the delivery of the  
1238 specified service takes place. It puts particular emphasis upon the personnel involved,  
1239 and their selection, training, and duties.

1240 An enterprise and its specified service must:

##### 1241 *ALA\_CO\_OPN#010 Technical Security*

1242 Demonstrate that the technical controls employed will provide the level of security  
1243 protection required by the risk assessment and the ISMS, or other IT security  
1244 management methods recognized by a government or professional body, and that these  
1245 controls are effectively integrated with the applicable procedural and physical security  
1246 measures.

1247 **Guidance:** Appropriate technical controls, suited to this Assurance Level, should be  
1248 selected from [[NIST800-63](#)] or its equivalent, as established by a recognized national  
1249 technical authority.

##### 1250 *ALA\_CO\_OPN#020 Defined Security Roles*

1251 Define, by means of a job description, the roles and responsibilities for each service-  
1252 related security-relevant task, relating it to specific procedures (which shall be set out in  
1253 the ISMS, or other IT security management methodology recognized by a government or  
1254 professional body) and other service-related job descriptions. Where the role is security-  
1255 critical or where special privileges or shared duties exist, these must be specifically  
1256 identified as such, including the applicable access privileges relating to logical and  
1257 physical parts of the service's operations.

##### 1258 *ALA\_CO\_OPN#030 Personnel Recruitment*

1259 Demonstrate that it has defined practices for the selection, vetting, and contracting of all  
1260 service-related personnel, both direct employees and those whose services are provided  
1261 by third parties. Full records of all searches and supporting evidence of qualifications and  
1262 past employment must be kept for the duration of the individual's employment plus the  
1263 longest lifespan of any credential issued under the Service Policy.

##### 1264 *ALA\_CO\_OPN#040 Personnel skills*

1265 Ensure that employees are sufficiently trained, qualified, experienced, and current for the  
1266 roles they fulfill. Such measures must be accomplished either by recruitment practices or  
1267 through a specific training program. Where employees are undergoing on-the-job  
1268 training, they must only do so under the guidance of a mentor possessing the defined  
1269 service experiences for the training being provided.

##### 1270 *ALA\_CO\_OPN#050 Adequacy of Personnel resources*

1271 Have sufficient staff to adequately operate and resource the specified service according to  
1272 its policies and procedures.

##### 1273 *ALA\_CO\_OPN#060 Physical access control*

1274 Apply physical access control mechanisms to ensure that:

- 1275 a) access to sensitive areas is restricted to authorized personnel;
- 1276 b) all removable media and paper documents containing sensitive information as
- 1277 plain-text are stored in secure containers;
- 1278 c) a minimum of two persons are required to enable access to any cryptographic
- 1279 modules;
- 1280 d) there is 24/7 monitoring for unauthorized intrusions.

1281 *ALA\_CO\_OPN#070 Logical access control*

1282 Employ logical access control mechanisms that ensure access to sensitive system  
1283 functions and controls is restricted to authorized personnel.

#### 1284 **4.4.6 External Services and Components**

1285 This section addresses the relationships and obligations upon contracted parties both to  
1286 apply the policies and procedures of the enterprise and also to be available for assessment  
1287 as critical parts of the overall service provision.

1288 An enterprise and its specified service must:

1289 *ALA\_CO\_ESC#010 Contracted Policies and Procedures*

1290 Where the enterprise uses external suppliers for specific packaged components of the  
1291 service or for resources which are integrated with its own operations and under its  
1292 control, ensure that those parties are engaged through reliable and appropriate contractual  
1293 arrangements which stipulate which critical policies, procedures, and practices sub-  
1294 contractors are required to fulfill.

1295 *ALA\_CO\_ESC#020 Visibility of Contracted Parties*

1296 Where the enterprise uses external suppliers for specific packaged components of the  
1297 service or for resources which are integrated with its own operations and under its  
1298 control, ensure that the suppliers' compliance with contractually-stipulated policies and  
1299 procedures, and thus with the IAF Service Assessment Criteria, can be independently  
1300 verified, and subsequently monitored if necessary.

#### 1301 **4.4.7 Secure Communications**

1302 An enterprise and its specified service must:

1303 *ALA\_CO\_SCO#010 Secure remote communications*

1304 If the specific service components are located remotely from and communicate over a  
1305 public or unsecured network with other service components or other CSPs it services, or  
1306 parties requiring access to the CSP's services, each transaction must be cryptographically  
1307 protected using an encryption method approved by a recognized national technical  
1308 authority or other generally-recognized authoritative body, by either:

- 1309 a) implementing mutually-authenticated protected sessions; or
- 1310 b) time-stamped or sequenced messages signed by their source and encrypted for their  
1311 recipient.



1312 **Guidance:** The reference to “parties requiring access to the CSP’s services” is intended  
1313 to cover SP 800-63-2’s reference to RPs (see cross-mapped EZP 63-2 clause).

1314 *ALA\_CO\_SCO#015 Verification / Authentication confirmation messages*  
1315 Ensure that any verification or confirmation of authentication messages, which assert  
1316 either that a weakly bound credential is valid or that a strongly bound credential has not  
1317 been subsequently revoked, is logically bound to the credential and that the message, the  
1318 logical binding, and the credential are all transmitted within a single integrity-protected  
1319 session between the service and the Verifier / Relying Party.

1320 *ALA\_CO\_SCO#016 No stipulation*

1321 *ALA\_CO\_SCO#020 Limited access to shared secrets*

1322 Ensure that:

- 1323 a) access to shared secrets shall be subject to discretionary controls which permit  
1324 access to those roles/applications which need such access;
- 1325 b) stored shared secrets are encrypted such that:
- 1326 i the encryption key for the shared secret file is encrypted under a key held  
1327 in a FIPS 140-2 [FIPS140-2] Level 2 (or higher) validated hardware  
1328 cryptographic module, or equivalent, as established by a recognized  
1329 national technical authority, or any FIPS 140-2 Level 3 or 4 validated  
1330 cryptographic module, or equivalent, as established by a recognized  
1331 national technical authority, and decrypted only as immediately required  
1332 for an authentication operation;
- 1333 ii they are protected as a key within the boundary of a FIPS 140-2 Level 2  
1334 (or higher) validated hardware cryptographic module, or equivalent, as  
1335 established by a recognized national technical authority, or any  
1336 FIPS 140-2 Level 3 or 4 cryptographic module, or equivalent, as  
1337 established by a recognized national technical authority, and are not  
1338 exported from the module in plaintext;
- 1339 iii they are split by an "n from m" cryptographic secret-sharing method;
- 1340 c) any long-term (i.e., not session) shared secrets are revealed only to the Subject  
1341 and the CSP's direct agents (bearing in mind (a) above).

1342 **These roles should be defined and documented by the CSP in accordance with**  
1343 **AL4\_CO\_OPN#020 above.**

1344

1345 **4.5 Compliance Tables**

1346 Use the following tables to correlate criteria for a particular Assurance Level (AL) and  
1347 the evidence offered to support compliance.

1348 Service providers preparing for an assessment can use the table appropriate to the AL at  
1349 which they are seeking approval to correlate evidence with criteria or to justify non-  
1350 applicability (e.g., "specific service types not offered").

1351 Assessors can use the tables to record the steps in their assessment and their  
1352 determination of compliance or failure.

1353 These tables also provide an overview of any revisions made to criteria in comparison to  
1354 v3.0 of this document (see §1.1).

1355 **Table 3-1. CO-SAC - AL1 Compliance**

Clause	Description	Compliance
AL1_CO_ESM#010	<a href="#">Established enterprise</a>	
AL1_CO_ESM#020	Withdrawn	No conformity requirement
AL1_CO_ESM#030	<a href="#">Legal &amp; Contractual compliance</a>	
AL1_CO_ESM#040	No stipulation	
AL1_CO_ESM#050	<a href="#">Data Retention and Protection</a>	<i>New</i>
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#010	No stipulation	No conformity requirement
AL1_CO_SCO#015	No stipulation	No conformity requirement
AL1_CO_SCO#016	No stipulation	No conformity requirement
AL1_CO_SCO#020	<a href="#">Limited access to shared secrets</a>	<i>Editorial</i>

1356

1357

1358

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

Clause	Description	Compliance
AL2_CO_ESM#010	<a href="#">Established enterprise</a>	
AL2_CO_ESM#020	Data Retention and Protection	<i>Added</i>
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>	<i>Editorial</i>
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>	<i>Amended</i>
AL2_CO_NUI#025	<a href="#">AL2 Configuration Specification</a>	<i>New</i>
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>	<i>Guidance</i>
AL2_CO_ISM#090	Withdrawn	No conformity requirement
AL2_CO_ISM#100	<a href="#">Audit Records</a>	
AL2_CO_ISM#110	Withdrawn	No conformity requirement
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>	<i>Amended</i>

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>	<i>Amended; Guidance</i>
AL2_CO_SCO#015	<a href="#">Verification / Authentication confirmation messages</a>	<i>Amended</i>
AL2_CO_SCO#016	Withdrawn	<i>Re-numbered as AL2_CM_RVP#045</i>
AL2_CO_SCO#020	<a href="#">Limited access to shared secrets</a>	<i>Amended</i>
AL2_CO_SCO#030	<a href="#">Logical protection of shared secrets</a>	

1359

1360

1361

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

Clause	Description	Compliance
AL3_CO_ESM#010	<a href="#">Established enterprise</a>	
AL3_CO_ESM#020	Withdrawn	No conformity requirement
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>	<i>Amended</i>
AL3_CO_NUI#025	<a href="#">AL3 Configuration Specification</a>	<i>New</i>
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>	<i>Guidance</i>
AL3_CO_ISM#090	Withdrawn	No conformity requirement
AL3_CO_ISM#100	<a href="#">Audit Records</a>	
AL3_CO_ISM#110	Withdrawn	No conformity requirement
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>	<i>Amended</i>
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>	<i>Amended; Guidance</i>
AL3_CO_SCO#015	<a href="#">Verification / Authentication confirmation messages</a>	<i>New</i>
AL3_CO_SCO#016	Withdrawn	<i>Re-numbered as AL2_CM_RVP#045</i>
AL3_CO_SCO#020	<a href="#">Limited access to shared secrets</a>	<i>Amended</i>

1362

1363

1364

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

Clause	Description	Compliance
AL4_CO_ESM#010	<a href="#">Established enterprise</a>	
AL4_CO_ESM#020	Withdrawn	No conformity requirement
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>	<i>Editorial</i>
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>	<i>Amended</i>
AL4_CO_NUI#025	<a href="#">AL4 Configuration Specification</a>	<i>New</i>
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>	<i>Amended</i>
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>	<i>Guidance</i>
AL4_CO_ISM#090	Withdrawn	No conformity requirement
AL4_CO_ISM#100	<a href="#">Audit Records</a>	
AL4_CO_ISM#110	Withdrawn	No conformity requirement
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>	<i>Amended</i>
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>	<i>Amended; Guidance</i>
AL4_CO_SCO#015	<a href="#">Verification / Authentication confirmation messages</a>	<i>New</i>
AL4_CO_SCO#016	No stipulation	No conformity requirement
AL4_CO_SCO#020	<a href="#">Limited access to shared secrets</a>	<i>Amended</i>

1365



## 1366 **5 OPERATIONAL SERVICE ASSESSMENT CRITERIA**

---

1367 The Service Assessment Criteria in this section establish requirements for the operational  
1368 conformity of credential management services and their providers at all Assurance Levels  
1369 (AL) – refer to Section 2. These criteria are generally referred to elsewhere within IAF  
1370 documentation as OP-SAC.

1371 Previous editions of this document have these criteria set out in two distinct sections and  
1372 have used the terms CM-SAC and ID-SAC: the OP-SAC is the combination of those two  
1373 previous SAC sections, with optimizations necessary for their integration. To ensure  
1374 backwards compatibility with assessments already performed against previous editions of  
1375 this document the criteria within the OP-SAC continue to be identified either by a tag  
1376 “ALn\_ID\_ xxxx” or “ALn\_CM\_ xxxx”.

1377 Within each Assurance Level the criteria are divided into six Parts. Each part deals with a  
1378 specific functional aspect of the overall credential management process, including  
1379 identity proofing services (see Parts B, at each Assurance Level).

1380 Full Service Provision requires conformity to all of the following operational criteria at  
1381 the chosen Assurance Level. This may be demonstrated either by the Full Service  
1382 Provider fulfilling all of these criteria itself or by its service being a composition of  
1383 Service Components which must, collectively, fulfill all of these criteria, under the overall  
1384 management of the Full Service Provider. Providers of Service Components may  
1385 conform to a defined sub-set of these criteria (although, within Part A at each Assurance  
1386 Level, there is a small number of criteria which are mandatory for Component Services,  
1387 which are marked as such).

1388 The procedures and processes required to create a secure environment for management of  
1389 credentials and the particular technologies that are considered strong enough to meet the  
1390 assurance requirements differ considerably from level to level.

### 1391 **5.1 Assurance Level 1**

#### 1392 **5.1.1 Part A - Credential Operating Environment**

1393 These criteria describe requirements for the overall operational environment in which  
1394 credential lifecycle management is conducted. The Common Organizational criteria  
1395 describe broad requirements. The criteria in this Part describe operational  
1396 implementation specifics

1397 These criteria apply to PINs and passwords, as well as SAML assertions.

1398 The criterion AL1\_CM\_CTR#030 is marked as **MANDATORY** for all Component  
1399 Services.

1400 **5.1.1.1 Not used**

1401 No stipulation.

1402 **5.1.1.2 Security Controls**

1403 An enterprise and its specified service must:

1404 *ALI\_CM\_CTR#010* *Withdrawn*

1405 *ALI\_CM\_CTR#020* *Protocol threat risk assessment and controls*

1406 Account for at least the following protocol threats and apply appropriate controls:

- 1407 a) password guessing, such that there are at least 14 bits of entropy to resist an on-
- 1408 line guessing attack against a selected user/password;
- 1409 b) message replay.

1410 **Guidance:** Organizations should consider potential protocol threats identified in other  
1411 sources, e.g. ISO/IEC 29115:2013 “Information technology -- Security techniques –  
1412 Entity authentication assurance framework”.

1413 *ALI\_CM\_CTR#025* *No stipulation*

1414 *ALI\_CM\_CTR#028* *No stipulation*

1415 *ALI\_CM\_CTR#030* *System threat risk assessment and controls*

1416 **MANDATORY.**

1417 Account for the following system threats and apply appropriate controls:

- 1418 a) the introduction of malicious code;
- 1419 b) compromised authentication arising from insider action;
- 1420 c) out-of-band attacks by other users and system operators (e.g., the ubiquitous
- 1421 shoulder-surfing);
- 1422 d) spoofing of system elements/applications;
- 1423 e) malfeasance on the part of Subscribers and Subjects.

1424 **Guidance:** the risk assessment should address these threats from any perspective in  
1425 which they might adversely affect the operation of the service, whether they be from  
1426 within the organization (e.g. in its development environment, the hosting environment) or  
1427 without (e.g. network attacks, hackers).

1428 **5.1.1.3 Storage of Long-term Secrets**

1429 *ALI\_CM\_STS#010* *Withdrawn*

1430 Withdrawn (AL1\_CO\_SCO#020 (a) & (b) enforce this requirement)

1431 **5.1.1.4 No stipulation**

1432 **5.1.1.5 Subject Options**

1433 *ALI\_CM\_OPN#010 Withdrawn*

1434 Withdrawn – see AL1\_CM\_RNR#010.

1435 **5.1.2 Part B - Credential Issuing**

1436 These criteria apply to the verification of the identity of the Subject of a credential and  
1437 with token strength and credential delivery mechanisms. They address requirements  
1438 levied by the use of various technologies to achieve Assurance Level 1.

1439 **5.1.2.1 Identity Proofing Policy**

1440 The specific service must show that it applies identity proofing policies and procedures  
1441 and that it retains appropriate records of identity proofing activities and evidence.

1442 The enterprise and its specified service must:

1443 *ALI\_ID\_POL#010 Unique service identity*

1444 Ensure that a unique identity is attributed to the specific service, such that credentials  
1445 issued by it can be distinguishable from those issued by other services, including services  
1446 operated by the same enterprise.

1447 *ALI\_ID\_POL#020 Unique Subject identity*

1448 Ensure that each applicant’s identity is unique within the service’s community of Subjects  
1449 and uniquely associable with tokens and/or credentials issued to that identity.

1450 **5.1.2.2 Identity Verification**

1451 The enterprise or specific service:

1452 *ALI\_ID\_IDV#000 Identity Proofing classes*

1453 a) must include in its Service Definition at least one of the following classes of  
1454 identity proofing service, and;

1455 b) may offer any additional classes of identity proofing service it chooses, subject to  
1456 the nature and the entitlement of the CSP concerned;

1457 c) must fulfill the applicable assessment criteria according to its choice of identity  
1458 proofing service, i.e. conform to at least one of the criteria sets defined in:

1459 i) §Error! Reference source not found., “In-Person Public Identity  
1460 Proofing”;

1461 ii) §Error! Reference source not found., “Remote Public Identity  
1462 Proofing”.

### 1463 5.1.2.3 In-Person Public Identity Verification

1464 If the specific service offers in-person identity proofing to applicants with whom it has no  
1465 previous relationship, then it must comply with the criteria in this section.

1466 An enterprise or specified service must:

1467 *ALI\_ID\_IPV#010 Required evidence*

1468 Accept a self-assertion of identity.

1469 *ALI\_ID\_IPV#020 Evidence checks*

1470 Accept self-attestation of evidence.

### 1471 5.1.2.4 Remote Public Identity Verification

1472 If the specific service offers remote identity proofing to applicants with whom it has no  
1473 previous relationship, then it must comply with the criteria in this section.

1474 An enterprise or specified service must:

1475 *ALI\_ID\_RPV#010 Required evidence*

1476 Require the applicant to provide a contact telephone number or email address.

1477 *ALI\_ID\_RPV#020 Evidence checks*

1478 Verify the provided information by either:

1479 a) confirming the request by calling the number;

1480 b) successfully sending a confirmatory email and receiving a positive

1481 acknowledgement.

### 1482 5.1.2.5 No stipulation

### 1483 5.1.2.6 No stipulation

### 1484 5.1.2.7 Issuing Derived Credentials

1485 Where the Applicant already possesses recognized original credentials the CSP may  
1486 choose to accept the verified identity of the Applicant as a substitute for identity proofing,  
1487 subject to the following specific provisions. All other requirements of Assurance Level 1  
1488 identity proofing must also be observed.

1489 *ALI\_ID\_IDC#010 Authenticate Original Credential*

1490 Prior to issuing any derived credential the original credential on which the identity-  
1491 proofing relies must be proven to be in the possession and under the control of the  
1492 Applicant.

1493 **Guidance:** This is the equivalent of recording the details of identity-proofing documents  
1494 provided during (e.g.) face-face id-proofing. It is not required that the original credential  
1495 be issued by a Kantara-Approved CSP.

#### 1496 **5.1.2.8 Secondary Identity Verification**

1497 In each of the above cases, an enterprise or specified service must:

1498 *ALI\_ID\_SCV#010 Secondary checks*

1499 Have in place additional measures (e.g., require additional documentary evidence, delay  
1500 completion while out-of-band checks are undertaken) to deal with:

1501 a) any reasonably anomalous circumstances that can be reasonably anticipated (e.g.,  
1502 a legitimate and recent change of address that has yet to be established as the  
1503 address of record);

1504 b) any use of processes and/or technologies which may not fully meet the preceding  
1505 applicable requirements but which are deemed to be comparable and thus able to  
1506 support AL1.

#### 1507 **5.1.2.9 Identity-proofing Records**

1508 *ALI\_ID\_VRC#010 No stipulation*

1509 *ALI\_ID\_VRC#020 No stipulation*

1510 *ALI\_ID\_VRC#025 Provide Subject Identity Records*

1511 If required, provide to qualifying parties a unique identity for each Subscriber and their  
1512 associated tokens and credentials to the extent permitted by applicable legislation and/or  
1513 agreed by the Subscriber.

1514 **Guidance:** the qualifier 'if required' is intended to account for circumstances where  
1515 conditions such as whether a contract or a federation policy permits or is required or  
1516 jurisdiction / legal injunction demand such provision. A qualifying party is any party to  
1517 which provision of such info can be justified according to circumstance: by contract/policy;  
1518 with Subject's agreement; with due authority (Court Order, e.g.). The CSP needs to make  
1519 the case, according to their service's characteristics and operating environment.

1520 *ALI\_ID\_VRC#030 No stipulation*

1521 *ALI\_CM\_IDP#010 Revision to Subject Information*

1522 Provide a means for Subjects to amend their stored information after registration.

1523 **Guidance:** The necessity for re-issuance will be determined by, *inter alia*, policy, the  
1524 technology and practices in use, the nature of change (e.g. registration data not bound into  
1525 the credential) and the nature of the proofing processes.

1526 *ALI\_CM\_IDP#020 Authenticate Subject Information Changes*  
1527 Permit only changes which are supported by appropriate and sufficient authentication of  
1528 the legitimacy of change according, to its type.

1529 **Guidance:** The requirement to authenticate the legitimacy of a change will depend upon  
1530 what is retained by the CSP and what is being changed: whereas a change of address may  
1531 require less demanding authentication than may a change of name, a change of date-of-  
1532 birth would be very unlikely and therefore would require substantial supporting  
1533 authentication.

#### 1534 **5.1.2.10 Credential Creation**

1535 These criteria address the requirements for creation of credentials that can only be used at  
1536 AL1. Any credentials/tokens that comply with the criteria stipulated for AL2 and higher  
1537 are acceptable at AL1.

1538 An enterprise and its specified service must:

1539 *ALI\_CM\_CRN#010 Authenticated Request*

1540 Only accept a request to generate a credential and bind it to an identity if the source of the  
1541 request can be authenticated as being authorized to perform identity proofing at AL1 or  
1542 higher.

1543 *ALI\_CM\_CRN#020 No stipulation*

1544 *ALI\_CM\_CRN#030 Credential uniqueness*

1545 Allow the Subject to select a credential (e.g., UserID) that is verified to be unique within  
1546 the specified service's community and assigned uniquely to a single identity Subject.

1547 *ALI\_CM\_CRN#035 Convey credential*

1548 Be capable of conveying the unique identity information associated with a credential to  
1549 Verifiers and Relying Parties.

1550 *ALI\_CM\_CRN#040 Token strength*

1551 Ensure that the single-factor token associated with the credential has one of the following  
1552 set of characteristics:

1553 c) For a memorized secret, apply a rule-set such that there shall be a minimum of 14  
1554 bits of entropy in the pin or pass-phrase;

1555 d) For a knowledge-based question, apply a rule-set such that there shall be:

1556 i) a minimum of 14 bits of entropy in the pin or pass-phrase OR;

1557 ii) a set of knowledge-based questions created by the user OR;

1558           iii) a set of knowledge-based questions selected by the user from a service-  
1559           generated list of at least five questions.

1560

1561           Note – null or empty answers in any case above shall not be permitted.

1562           Only allow password tokens that have a resistance to online guessing attack against a  
1563           selected user/password of at least 1 in  $2^{14}$  (16,384), accounting for state-of-the-art attack  
1564           strategies, and at least 10 bits of min-entropy Error! Bookmark not defined..

1565   **5.1.2.11 No stipulation**

1566   **5.1.2.12 No stipulation**

1567   **5.1.3 Part C - Credential Renewal and Re-issuing**

1568   These criteria apply to the renewal and re-issuing of credentials. They address  
1569   requirements levied by the use of various technologies to achieve the appropriate  
1570   Assurance Level 1.

1571   **5.1.3.1 Renewal/Re-issuance Procedures**

1572   These criteria address general renewal and re-issuance functions, to be exercised as  
1573   specific controls in these circumstances while continuing to observe the general  
1574   requirements established for initial credential issuance.

1575   An enterprise and its specified service must:

1576   *ALI\_CM\_RNR#010 Changeable PIN/Password*

1577   Permit Subjects to change their PINs/passwords.

1578   **5.1.4 Part D - Credential Revocation**

1579   These criteria deal with credential revocation and the determination of the legitimacy of a  
1580   revocation request.

1581   An enterprise and its specified service must:

1582 **5.1.4.1 No stipulation**

1583 **5.1.4.2 No stipulation**

1584 **5.1.4.3 No stipulation**

1585 **5.1.4.4 Secure Revocation Request**

1586 This criterion applies when revocation requests between remote components of a service  
1587 are made over a secured communication.

1588 An enterprise and its specified service must:

1589 *ALI\_CM\_SRR#010 Submit Request*

1590 Submit a request for revocation to the Credential Issuer service (function), using a  
1591 secured network communication, if necessary.

1592

1593 **5.1.5 Part E - Credential Status Management**

1594 These criteria deal with credential status management, such as the receipt of requests for  
1595 new status information arising from a new credential being issued or a revocation or other  
1596 change to the credential that requires notification. They also deal with the provision of  
1597 status information to requesting parties (Verifiers, Relying Parties, courts and others  
1598 having regulatory authority, etc.) having the right to access such information.

1599 **5.1.5.1 Status Maintenance**

1600 An enterprise and its specified service must:

1601 *ALI\_CM\_CSM#010 Maintain Status Record*

1602 Maintain a record of the status of all credentials issued.

1603 *ALI\_CM\_CSM#020 No stipulation*

1604 *ALI\_CM\_CSM#030 No stipulation*

1605 *ALI\_CM\_CSM#040 Status Information Availability*

1606 Provide, with 95% availability, a secure automated mechanism to allow relying parties to  
1607 determine credential status and authenticate the Claimant's identity.

1608 **5.1.6 Part F - Credential Verification/Authentication**

1609 These criteria apply to credential validation and identity authentication.



1610 **5.1.6.1 Assertion Security**

1611 An enterprise and its specified service must:

1612 *ALI\_CM\_ASS#010 Validation and Assertion Security*

1613 Provide validation of credentials to a Relying Party using a protocol that:

- 1614 a) requires authentication of the specified service or of the validation source;
- 1615 b) ensures the integrity of the authentication assertion;
- 1616 c) protects assertions against manufacture, modification and substitution, and
- 1617 secondary authenticators from manufacture;

1618 and which, specifically:

- 1619 d) creates assertions which are specific to a single transaction;
- 1620 e) where assertion references are used, generates a new reference whenever a new
- 1621 assertion is created;
- 1622 f) when an assertion is provided indirectly, either signs the assertion or sends it via a
- 1623 protected channel, using a strong binding mechanism between the secondary
- 1624 authenticator and the referenced assertion;
- 1625 g) requires the secondary authenticator to:
  - 1626 i) be signed when provided directly to Relying Party, or;
  - 1627 ii) have a minimum of 64 bits of entropy when provision is indirect (i.e.
  - 1628 through the credential user).

1629 *ALI\_CM\_ASS#015 No stipulation*

1630 *ALI\_CM\_ASS#018 No stipulation*

1631 *ALI\_CM\_ASS#020 No Post Authentication*

1632 Not authenticate credentials that have been revoked.

1633 *ALI\_CM\_ASS#030 Proof of Possession*

1634 Use an authentication protocol that requires the claimant to prove possession and control

1635 of the authentication token.

1636 *ALI\_CM\_ASS#035 Limit authentication attempts*

1637 Limit the number of failed authentication attempts to no more than 100 in any 30-day

1638 period.

1639 *ALI\_CM\_ASS#040 Assertion Lifetime*

1640 Set assertions to expire such that:

- 1641 a) those used outside of the internet domain of the Verifier become invalid 5 minutes
- 1642 after their creation; or
- 1643 b) those used within a single internet domain become invalid 12 hours after their
- 1644 creation (including assertions contained in or referenced by cookies).

1645 **5.1.6.2 Authenticator-generated challenges**

1646 No stipulation.

1647 **5.1.6.3 Multi-factor authentication**

1648 No stipulation.

1649 **5.1.6.4 Verifier's assertion schema**

1650 Note: Since assertions and related schema can be complex and may be modeled directly  
1651 on the needs and preferences of the participants, the details of such schema fall outside  
1652 the scope of the SAC's herein, which are expressed observing, insofar as is feasible, a  
1653 technology-agnostic policy. The following criteria, therefore, are perhaps more open to  
1654 variable conformity through their final implementation than are others in this document.

1655 These criteria are derived directly from NIST SP 800-63-2 and have been expressed in as  
1656 generic a manner as they can be.

1657 An enterprise and its specified service must:

1658 *ALI\_CM\_VAS#010 No stipulation*

1659 No stipulation.

1660 *ALI\_CM\_VAS#020 No stipulation*

1661 No stipulation.

1662 *ALI\_CM\_VAS#030 Assertion assurance level*

1663 Create assertions which, either explicitly or implicitly (using a mutually-agreed  
1664 mechanism), indicate the assurance level at which the initial authentication of the Subject  
1665 was made.

1666 *ALI\_CM\_VAS#040 No stipulation*

1667 No stipulation.

1668 *ALI\_CM\_VAS#050 No stipulation*

1669 No stipulation.

1670 *ALI\_CM\_VAS#060 No assertion manufacture/modification*

1671 Ensure that it is impractical to manufacture an assertion or assertion reference by using at  
1672 least one of the following techniques:

1673 a) Signing the assertion;

1674 b) Encrypting the assertion using a secret key shared with the RP;

1675 c) Creating an assertion reference which has a minimum of 64 bits of entropy;

- 1676 d) Sending the assertion over a protected channel during a mutually-authenticated  
1677 session.
- 1678 *ALI\_CM\_VAS#070 No stipulation*  
1679 No stipulation.
- 1680 *ALI\_CM\_VAS#080 Single-use assertions*  
1681 Limit to a single transaction the use of assertions which do not support proof of  
1682 ownership.
- 1683 *ALI\_CM\_VAS#090 Single-use assertion references*  
1684 Limit to a single transaction the use of assertion references.
- 1685 *ALI\_CM\_VAS#100 Bind reference to assertion*  
1686 Provide a strong binding between the assertion reference and the corresponding assertion,  
1687 based on integrity-protected (or signed) communications over which the Verifier has been  
1688 authenticated.
- 1689

## 1690 5.2 Assurance Level 2

### 1691 5.2.1 Part A - Credential Operating Environment

1692 These criteria describe requirements for the overall operational environment in which  
1693 credential lifecycle management is conducted. The Common Organizational criteria  
1694 describe broad requirements. The criteria in this Part describe operational  
1695 implementation specifics.

1696 These criteria apply to passwords, as well as acceptable SAML assertions.

1697 The following three criteria are **MANDATORY** for all Services, Full or Component, and  
1698 are individually marked as such:

1699 AL2\_CM\_CPP#010, AL2\_CM\_CPP#030, AL2\_CM\_CTR#030.

#### 1700 5.2.1.1 Credential Policy and Practices

1701 These criteria apply to the policy and practices under which credentials are managed.

1702 An enterprise and its specified service must:

1703 *AL2\_CM\_CPP#010 Credential Policy and Practice Statement*

1704 **MANDATORY.**

1705 **Include in its Service Definition a description of the policy against which it issues**  
1706 **credentials and the corresponding practices it applies in their management. At a**  
1707 **minimum, the Credential Policy and Practice Statement must specify:**

- 1708 a) **if applicable, any OIDs related to the Practice and Policy Statement;**
- 1709 b) **how users may subscribe to the service/apply for credentials and how users'**  
1710 **credentials will be delivered to them;**
- 1711 c) **how Subjects acknowledge receipt of tokens and credentials and what**  
1712 **obligations they accept in so doing (including whether they consent to**  
1713 **publication of their details in credential status directories);**
- 1714 d) **how credentials may be renewed, modified, revoked, and suspended,**  
1715 **including how requestors are authenticated or their identity re-proven;**
- 1716 e) **what actions a Subject must take to terminate a subscription;**
- 1717 f) **how records are retained and archived.**

1718 *AL2\_CM\_CPP#020 No stipulation*

1719 *AL2\_CM\_CPP#030 Management Authority*

1720 **MANDATORY.**

1721 **Have a nominated management body with authority and responsibility for**  
1722 **approving the Credential Policy and Practice Statement and for its implementation.**

1723 **5.2.1.2 Security Controls**

1724 An enterprise and its specified service must:

1725 *AL2\_CM\_CTR#010* **Withdrawn**

1726 *AL2\_CM\_CTR#020* *Protocol threat risk assessment and controls*

1727 Account for at least the following protocol threats **in its risk assessment** and apply  
1728 **[omitted]** controls **that reduce them to acceptable risk levels:**

- 1729 a) password guessing, such that **there are at least 24 bits of entropy to resist an on-**  
1730 **line guessing attack against a selected user/password**
- 1731 b) message replay, **showing that it is impractical;**
- 1732 c) **eavesdropping, showing that it is impractical;**
- 1733 d) **no stipulation;**
- 1734 e) **man-in-the-middle attack;**
- 1735 f) **session hijacking.**

1736 **Guidance:** Organizations should consider potential protocol threats identified in other  
1737 sources, e.g. ISO/IEC 29115:2013 “Information technology -- Security techniques –  
1738 Entity authentication assurance framework”.

1739 *AL2\_CM\_CTR#025* *Authentication protocols*

1740 **Apply only authentication protocols which, through a comparative risk assessment**  
1741 **which takes into account the target Assurance Level, are shown to have resistance to**  
1742 **attack at least as strong as that provided by commonly-recognized protocols such as:**

- 1743 a) **tunneling;**
- 1744 b) **zero knowledge-based;**
- 1745 c) **signed SAML [Omitted].**

1746 **Guidance:** Whilst many authentication protocols are well-established and may be  
1747 mandated or strongly-recommended by specific jurisdictions or sectors (e.g. standards  
1748 published by national SDOs or applicable to government-specific usage) this criterion  
1749 gives flexibility to advanced and innovative authentication protocols for which adequate  
1750 strength can be shown to be provided by the protocol applied with the specific service.

1751 *AL2\_CM\_CTR#028* *One-time passwords*

1752 **Use only one-time passwords which:**

- 1753 a) **are generated using an approved block-cipher or hash function to combine a**  
1754 **symmetric key, stored on the device, with a nonce; or**
- 1755 b) **derive the nonce from a date and time, or a counter, which is generated on**  
1756 **the device; or**
- 1757 c) **have a limited lifetime, in the order of minutes.**

1758 *AL2\_CM\_CTR#030* *System threat risk assessment and controls*

1759 **MANDATORY.**

1760 Account for the following system threats **in its risk assessment** and apply **[omitted]**  
1761 controls **that reduce them to acceptable risk levels:**

- 1762 a) the introduction of malicious code;
- 1763 b) compromised authentication arising from insider action;
- 1764 c) out-of-band attacks by both users and system operators (e.g., the ubiquitous  
1765 shoulder-surfing);
- 1766 d) spoofing of system elements/applications;
- 1767 e) malfeasance on the part of Subscribers and Subjects;
- 1768 f) **intrusions leading to information theft.**

1769 **Guidance:** the risk assessment should address these threats from any perspective in  
1770 which they might adversely affect the operation of the service, whether they be from  
1771 within the organization (e.g. in its development environment, the hosting environment) or  
1772 without (e.g. network attacks, hackers).

1773 *AL2\_CM\_CTR#040 Specified Service's Key Management*

1774 **Specify and observe procedures and processes for the generation, storage, and**  
1775 **destruction of its own cryptographic keys used for securing the specific service's**  
1776 **assertions and other publicized information. At a minimum, these should address:**

- 1777 a) **the physical security of the environment;**
- 1778 b) **access control procedures limiting access to the minimum number of**  
1779 **authorized personnel;**
- 1780 c) **public-key publication mechanisms;**
- 1781 d) **application of controls deemed necessary as a result of the service's risk**  
1782 **assessment;**
- 1783 e) **destruction of expired or compromised private keys in a manner that**  
1784 **prohibits their retrieval, or their archival in a manner that prohibits their**  
1785 **reuse;**
- 1786 f) **applicable cryptographic module security requirements, quoting FIPS 140-2**  
1787 **[FIPS140-2] or equivalent, as established by a recognized national technical**  
1788 **authority.**

1789 **5.2.1.3 Storage of Long-term Secrets**

1790 *AL2\_CM\_STS#010 Withdrawn*

1791 Withdrawn (AL2\_CO\_SCO#020 (a) & (b) enforce this requirement).

1792 **5.2.1.4 No stipulation**

1793 **5.2.1.5 No stipulation**

1794 *AL2\_CM\_OPN#010 Withdrawn*

1795 Withdrawn – see AL2\_CM\_RNR#010.

1796 **5.2.2 Part B - Credential Issuing**

1797 These criteria apply to the verification of the identity of the Subject of a credential and  
1798 with token strength and credential delivery mechanisms. They address requirements  
1799 levied by the use of various technologies to achieve Assurance Level 2.

1800 **5.2.2.1 Identity Proofing Policy**

1801 The specific service must show that it applies identity proofing policies and procedures  
1802 and that it retains appropriate records of identity proofing activities and evidence.

1803 The enterprise and its specified service must:

1804 *AL2\_ID\_POL#010 Unique service identity*

1805 Ensure that a unique identity is attributed to the specific service, such that credentials  
1806 issued by it can be distinguishable from those issued by other services, including services  
1807 operated by the same enterprise.

1808 *AL2\_ID\_POL#020 Unique Subject identity*

1809 Ensure that each applicant's identity is unique within the service's community of Subjects  
1810 and uniquely associable with tokens and/or credentials issued to that identity.

1811 **Guidance:** Cf. AL2\_CM\_CRN#020 which expresses a very similar requirement.

1812 Although presenting repetition for a single provider, if the identity-proofing functions and  
1813 credential management functions are provided by separate CSPs, each needs to fulfill this  
1814 requirement.

1815 *AL2\_ID\_POL#030 Published Proofing Policy*

1816 **Make available the Identity Proofing Policy under which it verifies the identity of**  
1817 **applicants<sup>1</sup> in form, language, and media accessible to the declared community of**  
1818 **Users.**

1819 *AL2\_ID\_POL#040 Adherence to Proofing Policy*

1820 **Perform all identity proofing strictly in accordance with its published Identity**  
1821 **Proofing Policy.**

1822 **5.2.2.2 Identity Verification**

1823 The enterprise or specific service:

1824 *AL2\_ID\_IDV#000 Identity Proofing classes*

---

<sup>1</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.



- 1825 a) must include in its Service Definition at least one of the following classes of  
1826 identity proofing service, and;
- 1827 b) may offer any additional classes of identity proofing service it chooses, Subject to  
1828 the nature and the entitlement of the CSP concerned;
- 1829 c) must fulfill the applicable assessment criteria according to its choice of identity  
1830 proofing service, i.e. conform to at least one of the criteria sets defined in:
- 1831 i) §0, “[In-Person Public Identity Verification](#)”;
- 1832 ii) §5.2.2.4, “[Remote Public Identity Verification](#)”;
- 1833 iii) §5.2.2.5, “[Current Relationship Identity Verification](#)”;
- 1834 iv) §5.2.2.6, “[Affiliation Identity Verification](#)”;
- 1835 **although, in any of the above cases, the criteria defined in §5.2.2.7 may be**  
1836 **substituted for identity proofing where the Applicant already possesses a**  
1837 **recognized credential at Level 3 or 4.**

1838 *AL2\_ID\_IDV#010 - Identity Verification Measures*

1839 **For each identity proofing service offered (see above [*i.e.* AL2\_ID\_IDV#000]) justify**  
1840 **the identity verification measures applied by describing how these meet or exceed**  
1841 **the requirements of applicable policies, regulations, adopted standards and other**  
1842 **relevant conditions in order to maintain a level of rigour consistent with the**  
1843 **applicable Assurance Level.**

1844 **Guidance:** Although strict requirements for identity proofing and verification can be  
1845 defined, a real-world approach must account for instances where there is not 100%  
1846 certitude. To cope with this CSPs need to have a set of prescribed (through policy – see  
1847 AL2\_ID\_POL#030) and applied measures (see AL2\_ID\_POL#040) which observe  
1848 policy, identify the measures taken according to the degree of certitude determined by  
1849 each step in the verification process and what additional measures are taken. The CSP  
1850 must present a case which shows that their solution is sufficient to ensure that the basic  
1851 requirements of the applicable AL are met or exceeded.

1852 Note that in each set of proofing service criteria below there are criteria with specific  
1853 requirements for evidence checks and an additional criterion for ‘secondary’ checks, all of  
1854 which have an interplay with these overall requirements to have a policy and practice  
1855 statement and to demonstrate processes which sustain confidence that AL2 is being  
1856 achieved.

1857 Even though a CSP may use the services of a component service for the performance of  
1858 the identity-proofing within its own service, it still needs to ensure that its policy is both  
1859 justified and upheld. Where another service provider is used appropriate stipulations in  
1860 contracts should be established, but any internal adherence to (e.g.) ‘POL#040 should be  
1861 determined by the fact that the component service is already Kantara Approved.

1862 **5.2.2.3 In-Person Public Identity Proofing**

1863 If the specific service offers in-person identity proofing to applicants with whom it has no  
1864 previous relationship, then it must comply with the criteria in this section.

1865 The enterprise or specified service must:

1866 *AL2\_ID\_IPV#010 Required evidence*

1867 **Ensure that the applicant is in possession of a primary Government Picture ID**  
1868 **document that bears a photographic image of the holder.**

1869 *AL2\_ID\_IPV#020 Evidence checks*

1870 **Have in place and apply processes which ensure that the presented document:**

- 1871 a) **appears to be a genuine document properly issued by the claimed issuing**  
1872 **authority and valid at the time of application;**  
1873 b) **bears a photographic image of the holder that matches that of the applicant;**  
1874 c) **provides all reasonable certainty that the identity exists and that it uniquely**  
1875 **identifies the applicant.**

1876 **5.2.2.4 Remote Public Identity Proofing**

1877 If the specific service offers remote identity proofing to applicants with whom it has no  
1878 previous relationship, then it must comply with the criteria in this section.

1879 An enterprise or specified service must:

1880 *AL2\_ID\_RPV#010 Required evidence*

1881 **Ensure that the applicant submits the references of and attests to current possession**  
1882 **of a primary Government [omitted] ID document, and one of:**

- 1883 a) **a second Government ID;**  
1884 b) **an employee or student ID number;**  
1885 c) **a financial account number (e.g., checking account, savings account, loan or**  
1886 **credit card) or;**  
1887 d) **a utility service account number (e.g., electricity, gas, or water) for an address**  
1888 **matching that in the primary document;**  
1889 e) **a telephone service account.**

1890 **Ensure that the applicant provides additional verifiable personal information that at**  
1891 **a minimum must include:**

- 1892 f) **a name that matches the referenced photo-ID;**  
1893 g) **date of birth and;**  
1894 h) **current address [omitted];**  
1895 i) **for a telephone service account, the demonstrable ability to send or receive**  
1896 **messages at the phone number.**

1897 **Additional information may be requested so as to ensure a unique identity, and**  
1898 **alternative information may be sought where the enterprise can show that it leads to**  
1899 **at least the same degree of certitude when verified.**

1900 *AL2\_ID\_RPV#020 Evidence checks*

1901 **Perform inspection and analysis of records against the provided identity references**  
1902 **with the specified issuing authorities/institutions or through similar databases,**  
1903 **according to the inspection rules set by the issuing authorities:**

- 1904 a) **the existence of such records with matching name and reference numbers;**  
1905 b) **corroboration of date of birth, current contact information of record, and**  
1906 **other personal information sufficient to ensure a unique identity;**  
1907 c) **dynamic verification of personal information previously provided by or**  
1908 **likely to be known only by the applicant;**  
1909 d) **for a telephone service account, confirmation that the phone number is**  
1910 **associated in Records with the Applicant's name and address of record and**  
1911 **by having the applicant demonstrate that they are able to send or receive**  
1912 **messages at the phone number.**

1913 **Confirm contact information of record by at least one of the following means,**  
1914 **ensuring that any secret sent over an unprotected channel shall be reset upon first**  
1915 **use and shall be valid for a maximum lifetime of seven days:**

- 1916 e) **RA sends notice to an address of record confirmed in the records check and**  
1917 **receives a mailed or telephonic reply from applicant;**  
1918 f) **RA issues credentials in a manner that confirms the address of record**  
1919 **supplied by the applicant, for example by requiring applicant to enter on-line**  
1920 **some information from a notice sent to the applicant;**  
1921 g) **RA issues credentials in a manner that confirms ability of the applicant to**  
1922 **receive telephone communications at telephone number or email at email**  
1923 **address associated with the applicant in records.**  
1924 h) **[Omitted]**

1925 **Additional checks may be performed so as to establish the uniqueness of the claimed**  
1926 **identity (see AL2\_ID\_SCV#010).**

1927 **Alternative checks may be performed where the enterprise can show that they lead**  
1928 **to a comparable degree of certitude (see AL2\_ID\_SCV#010).**

### 1929 **5.2.2.5 Current Relationship Identity Proofing**

1930 If the specific service offers identity proofing to applicants with whom it has a current  
1931 relationship, then it must comply with the criteria in this section.

1932 The enterprise or specified service must:

1933 *AL2\_ID\_CRV#010 Required evidence*

1934 **Ensure that it has previously exchanged with the applicant a shared secret (e.g., a**  
1935 **PIN or password) that meets AL2 (or higher) entropy requirements<sup>2</sup>.**

1936 *AL2\_ID\_CRV#020 Evidence checks*

1937 **Ensure that it has:**

- 1938 a) **only issued the shared secret after originally establishing the applicant's**  
1939 **identity:**
- 1940 i) **with a degree of rigor equivalent to that required under either the AL2**  
1941 **(or higher) requirements for in-person or remote public verification;**  
1942 **or**
  - 1943 ii) **by complying with regulatory requirements effective within the**  
1944 **applicable jurisdiction which set forth explicit proofing requirements**  
1945 **which include a prior in-person appearance by the applicant and are**  
1946 **defined as meeting AL2 (or higher) requirements;**
- 1947 b) **an ongoing business relationship sufficient to satisfy the enterprise of the**  
1948 **applicant's continued personal possession of the shared secret.**

#### 1949 **5.2.2.6 Affiliation Identity Proofing**

1950 If the specific service offers identity proofing to applicants on the basis of some form of  
1951 affiliation, then it must comply with the criteria in this section for the purposes of  
1952 establishing that affiliation, in addition to the previously stated requirements for the  
1953 verification of the individual's identity.

1954 The enterprise or specified service must:

1955 *AL2\_ID\_AJV#000 Meet preceding criteria*

1956 **Meet all the criteria set out above, under §5.2.2.5, "[Current Relationship](#)**  
1957 **[Verification](#)".**

1958 *AL2\_ID\_AJV#010 Required evidence*

1959 **Ensure that the applicant possesses:**

- 1960 a) **identification from the organization with which it is claiming affiliation;**
- 1961 b) **agreement from the organization that the applicant may be issued a**  
1962 **credential indicating that an affiliation exists.**

1963 *AL2\_ID\_AJV#020 Evidence checks*

1964 **Have in place and apply processes which ensure that the presented documents:**

- 1965 a) **each appear to be a genuine document properly issued by the claimed issuing**  
1966 **authorities and valid at the time of application;**
- 1967 b) **refer to an existing organization with a contact address;**

---

<sup>2</sup> Refer to NIST SP 800-63 "Appendix A: Estimating Entropy and Strength" or similar recognized sources of such information.

- 1968 c) **indicate that the applicant has some form of recognizable affiliation with the**  
1969 **organization;**  
1970 d) **appear to grant the applicant an entitlement to obtain a credential indicating**  
1971 **its affiliation with the organization.**

#### 1972 **5.2.2.7 Identity-proofing based on Recognized Credentials**

1973 Where the Applicant already possesses recognized original credentials the CSP may  
1974 choose to accept the verified identity of the Applicant as a substitute for identity proofing,  
1975 subject to the following specific provisions. All other requirements of **Assurance Level**  
1976 **2** identity proofing must also be observed.

##### 1977 *AL2\_ID\_IDC#010 Authenticate Original Credential*

1978 Prior to issuing any derived credential the original credential on which the identity-  
1979 proofing relies must be:

- 1980 a) **authenticated by a source trusted by the CSP as being valid and un-revoked;**  
1981 b) **issued at Assurance Level 3 or 4;**  
1982 c) **issued in the same name as that which the Applicant is claiming;**  
1983 d) **proven to be in the possession and under the control of the Applicant.**

1984 **Guidance:** This is the equivalent of recording the details of id documents provided  
1985 during (e.g.) face-face id-proofing. It is not required that the original credential be issued  
1986 by a Kantara-Approved CSP.

##### 1987 *AL2\_ID\_IDC#020 Record Original Credential*

1988 **Record the details of the original credential.**

##### 1989 *AL2\_ID\_IDC#030 Issue Derived Credential*

1990 **Before issuing the derived credential ensure that:**

- 1991 a) **for in-person issuance, the claimant is the Applicant;**  
1992 b) **for remote issuance, token activation requires proof of possession of both the**  
1993 **derived token and the original Level 3 or Level 4 token.**

#### 1994 **5.2.2.8 Secondary Identity-proofing**

1995 In each of the above cases, the enterprise or specified service must:

##### 1996 *AL2\_ID\_SCV#010 Secondary checks*

1997 Have in place additional measures (e.g., require additional documentary evidence, delay  
1998 completion while out-of-band checks are undertaken) to deal with:

- 1999 a) any **reasonably** anomalous circumstances that can be reasonably anticipated (e.g.,  
2000 a legitimate and recent change of address that has yet to be established as the  
2001 address of record);

2002 b) any use of processes and/or technologies which may not fully meet the preceding  
2003 applicable requirements but which are deemed to be comparable and thus able to  
2004 support AL2.

### 2005 5.2.2.9 Identity-proofing Records

2006 The specific service must retain s of the identity proofing (verification) that it undertakes  
2007 and provide them to qualifying parties when so required.

2008 An enterprise or specified service must:

2009 *AL2\_ID\_VRC#010 Verification Records for Personal Applicants*

2010 **Log, taking account of all applicable legislative and policy obligations, a record of**  
2011 **the facts of the verification process, including a reference relating to the verification**  
2012 **processes, the date and time of verification and the identity of the registrar (person,**  
2013 **or entity if remote or automatic) performing the proofing functions.**

2014 **Guidance:** The facts of the verification process should include the specific record  
2015 information (source, unique reference, value/content) used in establishing the applicant's  
2016 identity, and will be determined by the specific processes used and documents accepted  
2017 by the CSP. The CSP need not retain these records itself if it uses a third-party service  
2018 which retains such records securely and to which the CSP has access when required, in  
2019 which case it must retain a record of the identity of the third-party service providing the  
2020 verification service or the location at which the (in-house) verification was performed.

2021 *AL2\_ID\_VRC#020 Verification Records for Affiliated Applicants*

2022 **In addition to the foregoing, log, taking account of all applicable legislative and**  
2023 **policy obligations, a record of the additional facts of the verification process**  
2024 **[omitted].**

2025 **Guidance:** Although there is no specific stipulation as to what should be recorded the  
2026 list below suggests facts which would typically be captured:

- 2027 a) the Subject's full name;  
2028 b) the Subject's current telephone or email address of record;  
2029 c) the Subscriber's acknowledgement for issuing the Subject with a credential;  
2030 d) type, issuing authority, and reference number(s) of all documents checked in the  
2031 identity proofing process.

2032 *AL2\_ID\_VRC#025 Provide Subject identity records*

2033 If required, provide to qualifying parties **records of identity proofing** to the extent  
2034 permitted by applicable legislation and/or agreed by the Subscriber.

2035 **Guidance:** the qualifier 'if required' is intended to account for circumstances where  
2036 conditions such as whether a contract or a federation policy permits or is required or  
2037 jurisdiction / legal injunction demand such provision. A qualifying party is any party to  
2038 which provision of such info can justified according to circumstance: by contract/policy;



2039 with Subject's agreement; with due authority (Court Order, e.g.). The CSP needs to make  
2040 the case, according to their service's characteristics and operating environment.

2041 *AL2\_ID\_VRC#030 Record Retention*

2042 **Either retain, securely, the record of the verification process for the duration of the**  
2043 **Subject account plus a further period sufficient to allow fulfillment of any period**  
2044 **required legally, contractually or by any other form of binding agreement or**  
2045 **obligation, or submit same record to a client CSP that has undertaken to retain the**  
2046 **record for the requisite period or longer.**

2047 *AL2\_CM\_IDP#010 Revision to Subject information*

2048 Provide a means for Subjects to **securely** amend their stored information after  
2049 registration, **either by re-proving their identity, as in the initial registration process,**  
2050 **or by using their credentials to authenticate their revision. Successful revision must**  
2051 **instigate the re-issuance of the credential when the data being revised are bound into**  
2052 **the credential.**

2053 **Guidance:** The necessity for re-issuance will be determined by, *inter alia*, policy, the  
2054 technology and practices in use, the nature of change (e.g. registration data not bound into  
2055 the credential) and the nature of the proofing processes.

2056 *AL2\_CM\_IDP#020 Authenticate Subject Information Changes*

2057 Permit only changes which are supported by appropriate and sufficient authentication of  
2058 the legitimacy of change according, to its type.

2059 **Guidance:** The requirement to authenticate the legitimacy of a change will depend upon  
2060 what is retained by the CSP and what is being changed: whereas a change of address may  
2061 require less demanding authentication than may a change of name, a change of date-of-  
2062 birth would be very unlikely and therefore would require substantial supporting  
2063 authentication.

#### 2064 **5.2.2.10 Credential Creation**

2065 These criteria define the requirements for creation of credentials whose highest use is at  
2066 AL2. Credentials/tokens that comply with the criteria stipulated at AL3 and higher are  
2067 also acceptable at AL2 and below.

2068 Note, however, that a token and credential required by a higher AL but created according  
2069 to these criteria may not necessarily provide that higher level of assurance for the claimed  
2070 identity of the Subject. Authentication can only be provided at the assurance level at  
2071 which the identity is proven.

2072 An enterprise and its specified service must:

2073 *AL2\_CM\_CRN#010 Authenticated Request*

2074 Only accept a request to generate a credential and bind it to an identity if the source of the  
2075 request can be authenticated, **i.e., Registration Authority, as being authorized to**  
2076 **perform identity proofing at AL2 or higher.**

2077 *AL2\_CM\_CRN#020 Unique identity*

2078 **Ensure that the identity which relates to a specific applicant is unique within the**  
2079 **specified service, including identities previously used and that are now cancelled,**  
2080 **other than its re-assignment to the same applicant.**

2081 **Guidance:** This requirement is intended to prevent identities that may exist in a Relying  
2082 Party's access control list from possibly representing a different physical person.  
2083 Cf. AL2\_CM\_POL#020 which expresses a very similar requirement. Although  
2084 presenting repetition for a single provider, if the identity-proofing functions and  
2085 credential management functions are provided by separate CSPs, each needs to fulfill this  
2086 requirement.

2087 *AL2\_CM\_CRN#030 Credential uniqueness*

2088 Allow the Subject to select a credential (e.g., UserID) that is verified to be unique within  
2089 the specified service's community and assigned uniquely to a single identity Subject.

2090 *AL2\_CM\_CRN#035 Convey credential*

2091 Be capable of conveying the unique identity information associated with a credential to  
2092 Verifiers and Relying Parties.

2093 *AL2\_CM\_CRN#040 Token strength*

2094 Ensure that the single-factor token associated with the credential has one of the following  
2095 set of characteristics:

2096 a) For a memorized secret, apply a rule-set such that there shall be a minimum of **24**  
2097 bits of entropy in the pin or pass-phrase;

2098 b) For a knowledge-based question, apply a rule-set such that there shall be:

2099 i) a minimum of **20** bits of entropy in the pin or pass-phrase OR;

2100 ii) a set of knowledge-based questions created by the user OR;

2101 iii) a set of knowledge-based questions selected by the user from a service-generated  
2102 list of at least **seven** questions.

2103

2104 Note – null or empty answers in either case above shall not be permitted.

2105 c) For a look-up token, apply a rule-set such that there shall be a minimum of **20**  
2106 bits of entropy in the secret phrase(s);

2107 d) For an out-of-band token, ensure that the token is uniquely addressable and  
2108 supports communication over a channel that is separate from the primary  
2109 channel for e-authentication;

2110 e) For a one-time-password device, generate one-time passwords using an  
2111 approved block cipher or hash function to combine a nonce and a symmetric  
2112 key;



2113 f) Use a cryptographic device validated at FIPS 140-2 Level 1 or higher or  
2114 equivalent, as established by a recognized national technical authority.

2115

2116 [Omitted]

2117 *AL2\_CM\_CRN#050 One-time password strength*

2118 Only allow password tokens that have a resistance to online guessing attack against  
2119 a selected user/password of at least 1 in  $2^{14}$  (16,384), accounting for state-of-the-art  
2120 attack strategies, and at least 10 bits of min-entropy.

2121 *AL2\_CM\_CRN#055 One-time password lifetime*

2122 Set the minimum valid lifetime for the one-time password to a value commensurate  
2123 with service usage and in no case greater than fifteen minutes.

2124 *AL2\_CM\_CRN#060 Software cryptographic token strength*

2125 Ensure that software cryptographic keys stored on general-purpose devices are  
2126 protected by a key and cryptographic protocol that are evaluated against FIPS 140-2  
2127 [FIPS140-2] Level 1, or equivalent, as established by a recognized national technical  
2128 authority.

2129 [Omitted]

2130 *AL2\_CM\_CRN#070 Hardware token strength*

2131 Ensure that hardware tokens used to store cryptographic keys employ a  
2132 cryptographic module that is evaluated against FIPS 140-2 [FIPS140-2] Level 1 or  
2133 higher, or equivalent, as established by a recognized national technical authority.

2134 [Omitted]

2135 *AL2\_CM\_CRN#075 No stipulation*

2136 *AL2\_CM\_CRN#080 No stipulation*

2137 *AL2\_CM\_CRN#090 Nature of Subject*

2138 Record the nature of the Subject of the credential (which must correspond to the  
2139 manner of identity proofing performed), i.e., physical person, a named person acting  
2140 on behalf of a corporation or other legal entity, corporation or legal entity, or  
2141 corporate machine entity, in a manner that can be unequivocally associated with the  
2142 credential and the identity that it asserts. [Omitted]

2143 *AL2\_CM\_CRN#095 Pseudonym's Real Identity*

2144 If the credential is based upon a pseudonym this must be indicated in the credential  
2145 and a record of the real identity retained.

#### 2146 5.2.2.11 Subject Key Pair Generation

2147 No stipulation.

2148 **5.2.2.12 Credential Delivery**

2149 An enterprise and its specified service must:

2150 *AL2\_CM\_CRD#010 Notify Subject of Credential Issuance*

2151 **Notify the Subject of the credential's issuance and, if necessary, confirm the**  
2152 **Subject's contact information by:**

- 2153 a) **sending notice to the address of record confirmed during identity proofing**  
2154 **or;**  
2155 b) **issuing the credential(s) in a manner that confirms the address of record**  
2156 **supplied by the applicant during identity proofing or;**  
2157 c) **issuing the credential(s) in a manner that confirms the ability of the applicant**  
2158 **to receive telephone communications at a fixed-line telephone number or**  
2159 **postal address supplied by the applicant during identity proofing.**

2160 **Guidance:** The nature of issuance could mean that the Subject is fully aware and  
2161 therefore no notification is necessary. If any other such circumstances prevailed, the CSP  
2162 should identify them.

2163 *AL2\_CM\_CRD#015 Confirm Applicant's identity (in person)*

2164 **Prior to delivering the credential, require the Applicant to identify themselves in**  
2165 **person in any new transaction (beyond the first transaction or encounter) by either:**

- 2166 (a) **using a temporary secret which was established during a prior**  
2167 **transaction or encounter, or sent to the Applicant's phone number, email**  
2168 **address, or physical address of record, or;**  
2169 (b) **matching a biometric sample against a reference sample that was**  
2170 **recorded during a prior encounter.**

2171 *AL2\_CM\_CRD#016 Confirm Applicant's identity (remotely)*

2172 **Prior to delivering the credential, require the Applicant to identify themselves in any**  
2173 **new electronic transaction (beyond the first transaction or encounter) by presenting**  
2174 **a temporary secret which was established during a prior transaction or encounter,**  
2175 **or sent to the Applicant's phone number, email address, or physical address of**  
2176 **record.**

2177 **5.2.3 Part C - Credential Renewal and Re-issuing**

2178 These criteria apply to the renewal and re-issuing of credentials. They address  
2179 requirements levied by the use of various technologies to achieve Assurance Level 2.

### 2180 5.2.3.1 Renewal/Re-issuance Procedures

2181 These criteria address general renewal and re-issuance functions, to be exercised as  
2182 specific controls in these circumstances while continuing to observe the general  
2183 requirements established for initial credential issuance.

2184 An enterprise and its specified service must:

2185 *AL2\_CM\_RNR#010 Changeable PIN/Password*

2186 Permit Subjects to change their [omitted] passwords, **but employ reasonable practices**  
2187 **with respect to password resets and repeated password failures.**

2188 *AL2\_CM\_RNR#020 Proof-of-possession on Renewal/Re-issuance*

2189 **Subjects wishing to change their passwords must demonstrate that they are in**  
2190 **possession of the unexpired current token prior to the CSP proceeding to renew or**  
2191 **re-issue it.**

2192 *AL2\_CM\_RNR#030 Renewal/Re-issuance limitations*

2193 a) **not renew but may re-issue Passwords;**

2194 b) **neither renew nor re-issue expired tokens;**

2195 c) **neither set to default nor re-use any token secrets;**

2196 d) **conduct all renewal / re-issuance interactions with the Subject over a**  
2197 **protected channel such as SSL/TLS.**

2198 **Guidance:** Renewal is considered as an extension of usability, whereas re-issuance  
2199 requires a change.

2200 *AL2\_CM\_RNR#040 No stipulation*

2201 **No stipulation.**

2202 *AL2\_CM\_RNR#050 Record Retention*

2203 **Retain, securely, the record of any renewal/re-issuance process for the duration of**  
2204 **the Subscriber's account plus a further period sufficient to allow fulfillment of any**  
2205 **period required legally, contractually or by any other form of binding agreement or**  
2206 **obligation, or submit same record to a client CSP that has undertaken to retain the**  
2207 **record for the requisite period or longer.**

### 2208 5.2.4 Part D - Credential Revocation

2209 These criteria deal with credential revocation and the determination of the legitimacy of a  
2210 revocation request.

#### 2211 5.2.4.1 Revocation Procedures

2212 These criteria address general revocation functions, such as the processes involved and  
2213 the basic requirements for publication.

- 2214 An enterprise and its specified service must:
- 2215 *AL2\_CM\_RVP#010 Revocation procedures*
- 2216 a) **State the conditions under which revocation of an issued credential may**  
2217 **occur;**
- 2218 b) **State the processes by which a revocation request may be submitted;**
- 2219 c) **State the persons and organizations from which a revocation request will be**  
2220 **accepted;**
- 2221 d) **State the validation steps that will be applied to ensure the validity (identity)**  
2222 **of the Revocant, and;**
- 2223 e) **State the response time between a revocation request being accepted and the**  
2224 **publication of revised certificate status.**
- 2225 *AL2\_CM\_RVP#020 Secure status notification*
- 2226 **Ensure that published credential status notification information can be relied upon**  
2227 **in terms of the enterprise of its origin (i.e., its authenticity) and its correctness (i.e.,**  
2228 **its integrity).**
- 2229 *AL2\_CM\_RVP#030 Revocation publication*
- 2230 **Unless the credential will expire automatically within 72 hours:**
- 2231 **Ensure that published credential status notification is revised within 72 hours of the**  
2232 **receipt of a valid revocation request, such that any subsequent attempts to use that**  
2233 **credential in an authentication shall be unsuccessful.**
- 2234 *AL2\_CM\_RVP#040 Verify revocation identity*
- 2235 **Establish that the identity for which a revocation request is received is one that was**  
2236 **issued by the specified service.**
- 2237 *AL2\_CM\_RVP#045 Notification of Revoked Credential*
- 2238 **When a verification / authentication request results in notification of a revoked**  
2239 **credential one of the following measures shall be taken:**
- 2240 a) **the confirmation message shall be time-stamped, or;**
- 2241 b) **the session keys shall expire with an expiration time no longer than that of**  
2242 **the applicable revocation list, or;**
- 2243 c) **the time-stamped message, binding, and credential shall all be signed by the**  
2244 **service.**
- 2245 *AL2\_CM\_RVP#050 Revocation Records*
- 2246 **Retain a record of any revocation of a credential that is related to a specific identity**  
2247 **previously verified, solely in connection to the stated credential. At a minimum,**  
2248 **records of revocation must include:**
- 2249 a) **the Revocant's full name;**

- 2250 b) **the Revocant’s authority to revoke (e.g., Subscriber, the Subject themselves,**  
2251 **someone acting with the Subscriber’s or the Subject’s power of attorney, the**  
2252 **credential issuer, law enforcement, or other legal due process);**  
2253 c) **the Credential Issuer’s identity (if not directly responsible for the identity**  
2254 **proofing service);**  
2255 d) **the identity associated with the credential (whether the Subject’s name or a**  
2256 **pseudonym);**  
2257 e) **the reason for revocation.**

2258 *AL2\_CM\_RVP#060 Record Retention*

2259 **Retain securely, the record of the revocation process for a period which is the**  
2260 **maximum of:**

- 2261 a) **the records retention policy required by AL2\_CM\_CPP#010; and**  
2262 b) **applicable legislation, regulation, contract or standards.**

#### 2263 **5.2.4.2 Verify Revocant’s Identity**

2264 Revocation of a credential requires that the requestor and the nature of the request be  
2265 verified as rigorously as the original identity proofing. The enterprise should not act on a  
2266 request for revocation without first establishing the validity of the request (if it does not,  
2267 itself, determine the need for revocation).

2268 In order to do so, the enterprise and its specified service must:

2269 *AL2\_CM\_RVR#010 Verify revocation identity*

2270 **Establish that the credential for which a revocation request is received was one that**  
2271 **was issued by the specified service, applying the same process and criteria as would**  
2272 **be applied to an original identity proofing.**

2273 *AL2\_CM\_RVR#020 Revocation reason*

2274 **Establish the reason for the revocation request as being sound and well founded, in**  
2275 **combination with verification of the Revocant, according to AL2\_ID\_RVR#030,**  
2276 **AL2\_ID\_RVR#040, or AL2\_ID\_RVR#050.**

2277 *AL2\_CM\_RVR#030 Verify Subscriber as Revocant*

2278 **When the Subscriber or Subject seeks revocation of the Subject’s credential, the**  
2279 **enterprise must:**

- 2280 a) **if in person, require presentation of a primary Government Picture ID**  
2281 **document that shall be electronically verified by a record check against the**  
2282 **provided identity with the specified issuing authority’s records;**  
2283 b) **if remote:**  
2284 i. **electronically verify a signature against records (if available),**  
2285 **confirmed with a call to a telephone number of record, or;**  
2286 ii. **authenticate an electronic request as being from the same Subscriber or**  
2287 **Subject, supported by a credential at Assurance Level 2 or higher.**

2288 *AL2\_CM\_RVR#040 CSP as Revocant*

2289 **Where a CSP seeks revocation of a Subject's credential, the enterprise must**  
2290 **establish that the request is either:**

- 2291 a) **from the specified service itself, with authorization as determined by**
- 2292 **established procedures, or;**
- 2293 b) **from the client Credential Issuer, by authentication of a formalized request**
- 2294 **over the established secure communications network.**

2295 *AL2\_CM\_RVR#050 Verify Legal Representative as Revocant*

2296 **Where the request for revocation is made by a law enforcement officer or**  
2297 **presentation of a legal document, the enterprise must:**

- 2298 a) **if in-person, verify the identity of the person presenting the request;**
- 2299 b) **if remote:**
  - 2300 i. **in paper/facsimile form, verify the origin of the legal document by a**
  - 2301 **database check or by telephone with the issuing authority, or;**
  - 2302 ii. **as an electronic request, authenticate it as being from a recognized**
  - 2303 **legal office, supported by a credential at Assurance Level 2 or higher.**

#### 2304 **5.2.4.3 No stipulation**

#### 2305 **5.2.4.4 Secure Revocation Request**

2306 This criterion applies when revocation requests must be communicated between remote  
2307 components of the service organization.

2308 An enterprise and its specified service must:

2309 *AL2\_CM\_SRR#010 Submit Request*

2310 Submit a request for the revocation to the Credential Issuer service (function), using a  
2311 secured network communication.

### 2312 **5.2.5 Part E - Credential Status Management**

2313 These criteria deal with credential status management, such as the receipt of requests for  
2314 new status information arising from a new credential being issued or a revocation or other  
2315 change to the credential that requires notification. They also deal with the provision of  
2316 status information to requesting parties (Verifiers, Relying Parties, courts and others  
2317 having regulatory authority, etc.) having the right to access such information.

#### 2318 **5.2.5.1 Status Maintenance**

2319 An enterprise and its specified service must:

2320 *AL2\_CM\_CSM#010 Maintain Status Record*

2321 Maintain a record of the status of all credentials issued.

2322 *AL2\_CM\_CSM#020 Validation of Status Change Requests*

2323 **Authenticate all requestors seeking to have a change of status recorded and**  
2324 **published and validate the requested change before considering processing the**  
2325 **request. Such validation should include:**

2326 a) **the requesting source as one from which the specified service expects to**  
2327 **receive such requests;**

2328 b) **if the request is not for a new status, the credential or identity as being one**  
2329 **for which a status is already held.**

2330 *AL2\_CM\_CSM#030 Revision to Published Status*

2331 **Process authenticated requests for revised status information and have the revised**  
2332 **information available for access within a period of 72 hours.**

2333 *AL2\_CM\_CSM#040 Status Information Availability*

2334 Provide, with 95% availability, a secure automated mechanism to allow relying parties to  
2335 determine credential status and authenticate the Claimant's identity.

2336 *AL2\_CM\_CSM#050 Inactive Credentials*

2337 **Disable any credential that has not been successfully used for authentication during**  
2338 **a period of 18 months.**

## 2339 **5.2.6 Part F - Credential Verification/Authentication**

2340 These criteria apply to credential validation and identity authentication.

### 2341 **5.2.6.1 Assertion Security**

2342 An enterprise and its specified service must:

2343 *AL2\_CM\_ASS#010 Validation and Assertion Security*

2344 Provide validation of credentials to a Relying Party using a protocol that:

2345 a) requires authentication of the specified service, itself, or of the validation source;

2346 b) ensures the integrity of the authentication assertion;

2347 c) protects assertions against manufacture, modification, **substitution and**  
2348 **disclosure**, and secondary authenticators from manufacture, **capture and replay**;

2349 **d) uses approved cryptography techniques;**

2350 and which, specifically:

2351 e) creates assertions which are specific to a single transaction;

2352 f) where assertion references are used, generates a new reference whenever a new  
2353 assertion is created;



- 2354 g) when an assertion is provided indirectly, either signs the assertion or sends it via a  
2355 protected channel, using a strong binding mechanism between the secondary  
2356 authenticator and the referenced assertion;
- 2357 **h) send assertions either via a channel mutually-authenticated with the Relying**  
2358 **Party, or signed and encrypted for the Relying Party;**
- 2359 i) requires the secondary authenticator to:
- 2360 i) be signed when provided directly to Relying Party, or;
- 2361 ii) have a minimum of 64 bits of entropy when provision is indirect (i.e.  
2362 through the credential user);
- 2363 **iii) be transmitted to the Subject through a protected channel which is**  
2364 **linked to the primary authentication process in such a way that**  
2365 **session hijacking attacks are resisted;**
- 2366 **iv) not be subsequently transmitted over an unprotected channel or to an**  
2367 **unauthenticated party while it remains valid.**

2368 *AL2\_CM\_ASS#013 No Stipulation*

2369 *AL2\_CM\_ASS#015 No False Authentication*

2370 **Employ techniques which ensure that system failures do not result in ‘false positive**  
2371 **authentication’ errors.**

2372 *AL2\_CM\_ASS#018 No stipulation*

2373 *AL2\_CM\_ASS#020 No Post Authentication*

2374 **Not** authenticate credentials that have been revoked **unless the time of the transaction**  
2375 **for which verification is sought precedes the time of revocation of the credential.**

2376 **Guidance:** The purpose in this criterion is that, if a verification is intended to refer to the  
2377 status of a credential at a specific historical point in time, e.g. to determine whether the  
2378 Claimant was entitled to act as a signatory in a specific capacity at the time of the  
2379 transaction, this may be done. It is implicit in this thinking that both the request and the  
2380 response indicate the historical nature of the query and response; otherwise the default  
2381 time is ‘now’. If no such service is offered then this criterion may simply be  
2382 ‘Inapplicable’, for that reason.

2383 *AL2\_CM\_ASS#030 Proof of Possession*

2384 Use an authentication protocol that requires the claimant to prove possession and control  
2385 of the authentication token.

2386 *AL2\_CM\_ASS#035 Limit authentication attempts*

2387 **Unless the token authenticator has at least 64 bits of entropy,** limit the number of  
2388 failed authentication attempts to no more than 100 in any 30-day period.

2389 *AL2\_CM\_ASS#040 Assertion Lifetime*

2390 **Set assertions to expire such that:**



- 2391 a) those used outside of the internet domain of the Verifier become invalid 5 minutes  
2392 after their creation; or  
2393 b) those used within a single internet domain become invalid 12 hours after their  
2394 creation (including assertions contained in or referenced by cookies).

#### 2395 **5.2.6.2 Authenticator-generated challenges**

2396 An enterprise and its specified service must:

2397 *AL2\_CM\_AGC#010 Entropy level*

2398 **Create authentication secrets to be used during the authentication exchange (i.e.**  
2399 **with out-of-band or cryptographic device tokens) with a degree of entropy**  
2400 **appropriate to the token type in question.**

#### 2401 **5.2.6.3 Multi-factor authentication**

2402 An enterprise and its specified service must:

2403 *AL2\_CM\_MFA#010 Permitted multi-factor tokens*

2404 **Require two tokens which, when used in combination within a single authentication**  
2405 **exchange, are acknowledged as providing an equivalence of AL2, as determined by a**  
2406 **recognized national technical authority.**

#### 2407 **5.2.6.4 Verifier's assertion schema**

2408 Note: Since assertions and related schema can be complex and may be modeled directly  
2409 on the needs and preferences of the participants, the details of such schema fall outside  
2410 the scope of the SAC's herein, which are expressed observing, insofar as is feasible, a  
2411 technology-agnostic policy. The following criteria, therefore, are perhaps more open to  
2412 variable conformity through their final implementation than are others in this document.

2413 These criteria are derived directly from NIST SP 800-63-2 and have been expressed in as  
2414 generic a manner as they can be.

2415 *Editor's note: I have avoided reference to the RP here – I am concerned as to what the*  
2416 *SAC requires services to do, not who might be using their products. SAC do not refer to*  
2417 *RPs.*

2418 An enterprise and its specified service must:

2419 *AL2\_CM\_VAS#010 Approved cryptography*

2420 **Apply assertion protocols which use cryptographic techniques approved by a**  
2421 **national authority or other generally-recognized authoritative body.**

2422 *AL2\_CM\_VAS#020 No stipulation*

2423 No stipulation.

- 2424 *AL2\_CM\_VAS#030 Assertion assurance level*  
2425 Create assertions which, either explicitly or implicitly (using a mutually-agreed  
2426 mechanism), indicate the assurance level at which the initial authentication of the Subject  
2427 was made.
- 2428 *AL2\_CM\_VAS#040 Notify pseudonyms*  
2429 **Create assertions which indicate whether the Subscriber name in the credential**  
2430 **subject to verification is a pseudonym.**
- 2431 *AL2\_CM\_VAS#050 Specify recipient*  
2432 **Create assertions which identify the intended recipient of the verification such that**  
2433 **the recipient may validate that it is intended for them.**
- 2434 *AL2\_CM\_VAS#060 No assertion manufacture/modification*  
2435 Ensure that it is impractical to manufacture an assertion or assertion reference by using at  
2436 least one of the following techniques:
- 2437 a) Signing the assertion;  
2438 b) Encrypting the assertion using a secret key shared with the RP;  
2439 c) Creating an assertion reference which has a minimum of 64 bits of entropy;  
2440 d) Sending the assertion over a protected channel during a mutually-authenticated  
2441 session.
- 2442 *AL2\_CM\_VAS#070 Assertion protections*  
2443 **Provide protection of assertion-related data such that:**
- 2444 a) **both assertions and assertion references are protected against capture and**  
2445 **re-use;**  
2446 b) **assertions are also protected against redirection;**  
2447 [US / EZP800-63-2: §9.3.2.2.2]  
2448 c) **assertions, assertion references and session cookies used for authentication**  
2449 **purposes, including any which are re-directed, are protected against session**  
2450 **hijacking, for at least the duration of their validity (see AL2\_CM\_VAS#110).**
- 2451 *AL2\_CM\_VAS#080 Single-use assertions*  
2452 Limit to a single transaction the use of assertions which do not support proof of  
2453 ownership.
- 2454 *AL2\_CM\_VAS#090 Single-use assertion references*  
2455 Limit to a single transaction the use of assertion references.
- 2456 *AL2\_CM\_VAS#100 Bind reference to assertion*  
2457 Provide a strong binding between the assertion reference and the corresponding assertion,  
2458 based on integrity-protected (or signed) communications over which the Verifier has been  
2459 authenticated.
- 2460

## 2461 5.3 Assurance Level 3

### 2462 5.3.1 Part A - Credential Operating Environment

2463 These criteria describe requirements for the overall operational environment in which  
2464 credential lifecycle management is conducted. The Common Organizational criteria  
2465 describe broad requirements. The criteria in this Part describe operational  
2466 implementation specifics.

2467 These criteria apply to one-time password devices and soft crypto applications protected  
2468 by passwords or biometric controls, as well as cryptographically-signed SAML  
2469 assertions.

2470 The following four criteria are **MANDATORY** for all Services, Full or Component, and  
2471 are individually marked as such:

2472 AL3\_CM\_CPP#010, AL3\_CM\_CPP#030, AL3\_CM\_CTR#030, AL3\_CM\_SER#010.

2473

#### 2474 5.3.1.1 Credential Policy and Practices

2475 These criteria apply to the policy and practices under which credentials are managed.

2476 An enterprise and its specified service must:

2477 *AL3\_CM\_CPP#010 Credential Policy and Practice Statement*

2478 **MANDATORY.**

2479 Include in its Service Definition a full description of the policy against which it issues  
2480 credentials and the corresponding practices it applies in their issuance. At a minimum,  
2481 the Credential Policy and Practice Statement must specify:

- 2482 a) if applicable, any OIDs related to the Credential Policy and Practice Statement;
- 2483 b) how users may subscribe to the service/apply for credentials and how the users'  
2484 credentials will be delivered to them;
- 2485 c) how Subscribers and/or Subjects acknowledge receipt of tokens and credentials  
2486 and what obligations they accept in so doing (including whether they consent to  
2487 publication of their details in credential status directories);
- 2488 d) how credentials may be renewed, modified, revoked, and suspended, including  
2489 how requestors are authenticated or their identity proven;
- 2490 e) what actions a Subscriber or Subject must take to terminate a subscription;
- 2491 f) how records are retained and archived.

2492 *AL3\_CM\_CPP#020 No stipulation*

2493 *AL3\_CM\_CPP#030 Management Authority*

2494 **MANDATORY.**

2495 Have a nominated or appointed high-level management body with authority and  
2496 responsibility for approving the Certificate Policy and Certification Practice Statement,  
2497 including ultimate responsibility for their proper implementation.

2498

### 2499 **5.3.1.2 Security Controls**

2500 *AL3\_CM\_CTR#010* **Withdrawn**

2501 *AL3\_CM\_CTR#020* *Protocol threat risk assessment and controls*

2502 Account for at least the following protocol threats in its risk assessment and apply  
2503 controls that reduce them to acceptable risk levels:

- 2504 a) password guessing, such that the resistance to an on-line guessing attack against a  
2505 selected user/password is at least 1 in  $2^{14}$  (16,384);
- 2506 b) message replay, showing that it is impractical;
- 2507 c) eavesdropping, showing that it is impractical;
- 2508 **d) relying party (verifier) impersonation, showing that it is impractical;**
- 2509 e) man-in-the-middle attack;
- 2510 **f) session hijacking, showing that it is impractical.**

2511 **The above list shall not be considered to be a complete list of threats to be addressed**  
2512 **by the risk assessment.**

2513 **Guidance:** Organizations should consider potential protocol threats identified in other  
2514 sources, e.g. ISO/IEC 29115:2013 “Information technology -- Security techniques –  
2515 Entity authentication assurance framework”.

2516 *AL3\_CM\_CTR#025* *Permitted authentication protocols*

2517 **For non-PKI credentials,** apply only authentication protocols which, through a  
2518 comparative risk assessment which takes into account the target Assurance Level, are  
2519 shown to have resistance to attack at least as strong as that provided by commonly-  
2520 recognized protocols such as:

- 2521 d) tunneling;
- 2522 e) zero knowledge-based;
- 2523 f) signed SAML [Omitted].

2524 *AL3\_CM\_CTR#028* **No Stipulation**

2525 *AL3\_CM\_CTR#030* *System threat risk assessment and controls*

2526 **MANDATORY.**

2527 Account for the following system threats in its risk assessment and apply controls that  
2528 reduce them to acceptable risk levels:

- 2529 a) the introduction of malicious code;
- 2530 b) compromised authentication arising from insider action;
- 2531 c) out-of-band attacks by both users and system operators (e.g., shoulder-surfing);
- 2532 d) spoofing of system elements/applications;
- 2533 e) malfeasance on the part of Subscribers and Subjects;
- 2534 f) intrusions leading to information theft.

2535 The above list shall not be considered to be a complete list of threats to be addressed by  
2536 the risk assessment.

2537 **Guidance:** the risk assessment should address these threats from any perspective in  
2538 which they might adversely affect the operation of the service, whether they be from  
2539 within the organization (e.g. in its development environment, the hosting environment) or  
2540 without (e.g. network attacks, hackers).

2541 *AL3\_CM\_CTR#040 Specified Service's Key Management*

2542 Specify and observe procedures and processes for the generation, storage, and destruction  
2543 of its own cryptographic keys used for securing the specific service's assertions and other  
2544 publicized information. At a minimum, these should address:

- 2545 a) the physical security of the environment;
- 2546 b) access control procedures limiting access to the minimum number of authorized  
2547 personnel;
- 2548 c) public-key publication mechanisms;
- 2549 d) application of controls deemed necessary as a result of the service's risk  
2550 assessment;
- 2551 e) destruction of expired or compromised private keys in a manner that prohibits  
2552 their retrieval or their archival in a manner that prohibits their reuse;
- 2553 f) applicable cryptographic module security requirements, quoting FIPS 140-2  
2554 [FIPS140-2] or equivalent, as established by a recognized national technical  
2555 authority.

### 2556 **5.3.1.3 Storage of Long-term Secrets**

2557 An enterprise and its specified service must:

2558 *AL3\_CM\_STS#010 Withdrawn*

2559 Withdrawn (AL3\_CO\_SCO#020 (a) & (b) enforce this requirement).

2560 *AL3\_CM\_STS#020 Stored Secret Encryption*

2561 **Encrypt such shared secret files so that:**

- 2562 a) **the encryption key for the shared secret file is encrypted under a key held in**  
2563 **a FIPS 140-2 [FIPS140-2] Level 2 or higher validated hardware or software**  
2564 **cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module,**  
2565 **or equivalent, as established by a recognized national technical authority;**

- 2566 b) the shared secret file is decrypted only as immediately required for an  
2567 authentication operation;  
2568 c) shared secrets are protected as a key within the boundary of a FIPS 140-2  
2569 Level 2 or higher validated hardware cryptographic module or any FIPS  
2570 140-2 Level 3 or 4 cryptographic module and are not exported from the  
2571 module in plain text, or equivalent, as established by a recognized national  
2572 technical authority;  
2573 d) shared secrets are split by an "n from m" cryptographic secret sharing  
2574 method.

#### 2575 5.3.1.4 Security-relevant Event (Audit) Records

2576 These criteria describe the need to provide an auditable log of all events that are pertinent  
2577 to the correct and secure operation of the service. The common organizational criteria  
2578 applying to provision of an auditable log of all security-related events pertinent to the  
2579 correct and secure operation of the service must also be considered carefully. These  
2580 criteria carry implications for credential management operations.

2581 In the specific context of a certificate management service, an enterprise and its specified  
2582 service must:

2583 *AL3\_CM\_SER#010 Security event logs*

2584 **MANDATORY, to the extent that the sub-items relate to the scope of service.**

2585 **Ensure that such audit records include:**

- 2586 a) the identity of the point of registration (irrespective of whether internal or  
2587 outsourced);  
2588 b) generation of the Subject's keys or the evidence that the Subject was in  
2589 possession of both parts of their own key-pair;  
2590 c) generation of the Subject's certificate;  
2591 d) dissemination of the Subject's certificate;  
2592 e) any revocation or suspension associated with the Subject's certificate.

#### 2593 5.3.1.5 Subject options

2594 *AL3\_CM\_OPN#010 Changeable PIN/Password*

2595 Withdrawn – see AL3\_CM\_RNR#010.

#### 2596 5.3.2 Part B - Credential Issuing

2597 These criteria apply to the verification of the identity of the Subject of a credential and  
2598 with token strength and credential delivery mechanisms. They address requirements  
2599 levied by the use of various technologies to achieve Assurance Level 3.

### 2600 **5.3.2.1 Identity Proofing Policy**

2601 The specific service must show that it applies identity proofing policies and procedures  
2602 and that it retains appropriate records of identity proofing activities and evidence.

2603 The enterprise and its specified service must:

2604 *AL3\_ID\_POL#010 Unique service identity*

2605 Ensure that a unique identity is attributed to the specific service, such that credentials  
2606 issued by it can be distinguishable from those issued by other services, including services  
2607 operated by the same enterprise.

2608 *AL3\_ID\_POL#020 Unique Subject identity*

2609 Ensure that each applicant's identity is unique within the service's community of Subjects  
2610 and uniquely associable with tokens and/or credentials issued to that identity.

2611 **Guidance:** Cf. AL3\_CM\_CRN#020 which expresses a very similar requirement.

2612 Although presenting repetition for a single provider, if the identity-proofing functions and  
2613 credential management functions are provided by separate CSPs, each needs to fulfill this  
2614 requirement.

2615 *AL3\_ID\_POL#030 Published Proofing Policy*

2616 Make available the Identity Proofing Policy under which it verifies the identity of  
2617 applicants<sup>3</sup> in form, language, and media accessible to the declared community of Users.

2618 *AL3\_ID\_POL#040 Adherence to Proofing Policy*

2619 Perform all identity proofing strictly in accordance with its published Identity Proofing  
2620 Policy, **through application of the procedures and processes set out in its Identity  
2621 Proofing Practice Statement (IdPPS).**

### 2622 **5.3.2.2 Identity Proofing**

2623 The enterprise or specific service:

2624 *AL3\_ID\_IDV#000 Identity Proofing classes*

2625 a) must include in its Service Definition at least one of the following classes of  
2626 identity proofing services, and;

2627 b) may offer any additional classes of identity proofing service it chooses, Subject to  
2628 the nature and the entitlement of the CSP concerned;

---

<sup>3</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.



- 2629 c) must fulfill the applicable assessment criteria according to its choice of identity  
2630 proofing service, i.e. conform to at least one of the criteria sets defined in:
- 2631 i) §0, “[In-Person Public Identity Verification](#)”;
  - 2632 ii) §5.3.2.4, “[Remote Public Identity Verification](#)”;
  - 2633 iii) §5.2.2.5, “[Current Relationship Identity Verification](#)”;
  - 2634 iv) §5.3.2.6, “[Affiliation Identity Verification](#)”.
- 2635 although, in any of the above cases, the criteria defined in §5.3.2.7 may be  
2636 substituted for identity proofing where the Applicant already possesses a  
2637 recognized credential at **Level 4**

#### 2638 *AL3\_ID\_IDV#010 - Identity Verification Measures*

2639 For each identity proofing service offered (see above [*i.e.* AL3\_IDV#000]) justify the  
2640 identity verification measures **described in its IdPPS (see AL3\_ID\_POL#040)** by  
2641 describing how these meet or exceed the requirements of applicable policies, regulations,  
2642 adopted standards and other relevant conditions in order to maintain a level of rigour  
2643 consistent with the AL3.

2644 **Guidance:** Although strict requirements for identity proofing and verification can be  
2645 defined, a real-world approach must account for instances where there is not 100%  
2646 certitude. To cope with this CSPs need to have a set of prescribed (through policy – see  
2647 AL3\_ID\_POL#030) and applied measures (see AL3\_ID\_POL#040) which observe  
2648 policy, identify the measures taken according to the degree of certitude determined by  
2649 each step in the verification process and what additional measures are taken. The CSP  
2650 must present a case which shows that their solution is sufficient to ensure that the basic  
2651 requirements of the applicable AL are met or exceeded.

2652 Note that in each set of proofing service criteria below there are criteria with specific  
2653 requirements for evidence checks and an additional criterion for ‘secondary’ checks, all of  
2654 which have an interplay with these overall requirements to have a policy and practice  
2655 statement and to demonstrate processes which sustain confidence that AL3 is being  
2656 achieved.

2657 Even though a CSP may use the services of a component service for the performance of  
2658 the identity-proofing within its own service, it still needs to ensure that its policy is both  
2659 justified and upheld. Where another service provider is used appropriate stipulations in  
2660 contracts should be established, but any internal adherence to (e.g.) ‘POL#040 should be  
2661 determined by the fact that the component service is already Kantara Approved.

#### 2662 **5.3.2.3 In-Person Public Identity Proofing**

2663 A specific service that offers identity proofing to applicants with whom it has no previous  
2664 relationship must comply with the criteria in this section.



2665 The enterprise or specified service must:

2666 *AL3\_ID\_IPV#010 Required evidence*

2667 Ensure that the applicant is in possession of a primary Government Picture ID document  
2668 that bears a photographic image of the holder.

2669 *AL3\_ID\_IPV#020 Evidence checks*

2670 **Have in place and apply processes which ensure** that the presented document:

- 2671 a) appears to be a genuine document properly issued by the claimed issuing  
2672 authority and valid at the time of application;
- 2673 b) bears a photographic image of the holder that matches that of the applicant;
- 2674 c) **is electronically verified by a record check with the specified issuing**  
2675 **authority or through similar databases that:**
- 2676 i) **establishes the existence of such records with matching name and**  
2677 **reference numbers;**
- 2678 ii) **corroborates date of birth, current address of record, and other**  
2679 **personal information sufficient to ensure a unique identity;**
- 2680 d) provides all reasonable certainty that the identity exists and that it uniquely  
2681 identifies the applicant.

#### 2682 **5.3.2.4 Remote Public Identity Proofing**

2683 A specific service that offers remote identity proofing to applicants with whom it has no  
2684 previous relationship must comply with the criteria in this section.

2685 The enterprise or specified service must:

2686 *AL3\_ID\_RPV#010 Required evidence*

2687 Ensure that the applicant submits the references of and attests to current possession of a  
2688 primary Government [omitted] ID document, and one of:

- 2689 a) a second Government ID;
- 2690 b) an employee or student ID number;
- 2691 c) a financial account number (e.g., checking account, savings account, loan, or  
2692 credit card), or;
- 2693 d) a utility service account number (e.g., electricity, gas, or water) for an address  
2694 matching that in the primary document.

2695 Ensure that the applicant provides additional verifiable personal information that at a  
2696 minimum must include:

- 2697 e) a name that matches the referenced photo-ID;
- 2698 f) date of birth;
- 2699 g) current address [omitted].

2700 Additional information may be requested so as to ensure a unique identity, and alternative  
2701 information may be sought where the enterprise can show that it leads to at least the same  
2702 degree of certitude when verified.

2703 *AL3\_ID\_RPV#020 Evidence checks*

2704 **Electronically verify by a record check** against the provided identity references with the  
2705 specified issuing authorities/institutions or through similar databases, according to the  
2706 inspection rules set by the issuing authorities:

- 2707 a) the existence of such records with matching name and reference numbers;
- 2708 b) corroboration of date of birth, contact information of record [omitted], and other  
2709 personal information sufficient to ensure a unique identity;
- 2710 c) dynamic verification of personal information previously provided by or likely to  
2711 be known only by the applicant
- 2712 d) for a telephone service account, confirmation that the phone number is associated  
2713 in Records with the Applicant's name and address of record and by having the  
2714 applicant demonstrate that they are able to send or receive messages at the phone  
2715 number.

2716 Confirm contact information of record by at least one of the following means, ensuring  
2717 that any secret sent over an unprotected channel shall be reset upon first use and shall be  
2718 valid for a maximum lifetime of seven days:

- 2719 e) RA sends notice to an address of record confirmed in the records check and  
2720 receives a mailed or telephonic reply from applicant;
- 2721 f) RA issues credentials in a manner that confirms the address of record supplied by  
2722 the applicant, for example by requiring applicant to enter on-line some  
2723 information from a notice sent to the applicant;
- 2724 g) RA issues credentials in a manner that confirms ability of the applicant to receive  
2725 telephone communications at telephone number or email at email address  
2726 associated with the applicant in records.
- 2727 h) [Omitted]

2728 Additional checks may be performed so as to establish the uniqueness of the claimed  
2729 identity (see AL3\_ID\_SCV#010).

2730 Alternative checks may be performed where the enterprise can show that they lead to a  
2731 comparable degree of certitude (see AL3\_ID\_SCV#010).

### 2732 **5.3.2.5 Current Relationship Identity Proofing**

2733 If the specific service offers identity proofing to applicants with whom it has a current  
2734 relationship, then it must comply with the criteria in this section.

2735 The enterprise or specified service must:

2736 *AL3\_ID\_CRV#010 Required evidence*

2737 Ensure that it has previously exchanged with the applicant a shared secret (e.g., a PIN or  
2738 password) that meets AL3 (or higher) entropy requirements<sup>4</sup>.

2739 *AL3\_ID\_CRV#020 Evidence checks*

2740 Ensure that it has:

- 2741 a) only issued the shared secret after originally establishing the applicant's identity:
  - 2742 iii) with a degree of rigor equivalent to that required under either the AL3 (or  
2743 higher) requirements for in-person or remote public verification; or
  - 2744 iv) by complying with regulatory requirements effective within the applicable  
2745 jurisdiction which set forth explicit proofing requirements which include a  
2746 prior in-person appearance by the applicant and are defined as meeting AL3  
2747 (or higher) requirements;
- 2748 b) an ongoing business relationship sufficient to satisfy the enterprise of the  
2749 applicant's continued personal possession of the shared secret.

### 2750 5.3.2.6 Affiliation Identity Proofing

2751 A specific service that offers identity proofing to applicants on the basis of some form of  
2752 affiliation must comply with the criteria in this section to establish that affiliation and  
2753 with the previously stated requirements to verify the individual's identity.

2754 The enterprise or specified service must:

2755 *AL3\_ID\_AJV#000 Meet preceding criteria*

2756 Meet all the criteria set out above, under §5.3.2.4, "[Remote Public Identity](#)  
2757 [Verification](#)".

2758 *AL3\_ID\_AJV#010 Required evidence*

2759 Ensure that the applicant possesses:

- 2760 a) identification from the organization with which it is claiming affiliation;
- 2761 b) agreement from the organization that the applicant may be issued a credential  
2762 indicating that an affiliation exists.

2763 *AL3\_ID\_AJV#020 Evidence checks*

2764 Have in place and apply processes which ensure that the presented documents:

- 2765 a) each appear to be a genuine document properly issued by the claimed issuing  
2766 authorities and valid at the time of application;
- 2767 b) refer to an existing organization with a contact address;
- 2768 c) indicate that the applicant has some form of recognizable affiliation with the  
2769 organization;
- 2770 d) appear to grant the applicant an entitlement to obtain a credential indicating an  
2771 affiliation with the organization.

---

<sup>4</sup> Refer to NIST SP 800-63 "Appendix A: Estimating Entropy and Strength" or similar recognized sources of such information.

2772 **5.3.2.7 Identity-proofing based on Recognized Credentials**

2773 Where the Applicant already possesses recognized original credentials the CSP may  
2774 choose to accept the verified identity of the Applicant as a substitute for identity proofing,  
2775 subject to the following specific provisions. All other requirements of Assurance Level 3  
2776 identity proofing must also be observed.

2777 *AL3\_ID\_IDC#010 Authenticate Original Credential*

2778 Prior to issuing any derived credential the original credential on which the identity-  
2779 proofing relies must be:

- 2780 a) authenticated by a source trusted by the CSP as being valid and un-revoked;
- 2781 b) issued at **Assurance Level 4**;
- 2782 c) issued in the same name as that which the Applicant is claiming;
- 2783 d) proven to be in the possession and under the control of the Applicant.

2784 **Guidance:** This is the equivalent of recording the details of id documents provided  
2785 during (e.g.) face-face id-proofing. It is not required that the original credential be issued  
2786 by a Kantara-Approved CSP.

2787 *AL3\_ID\_IDC#020 Record Original Credential*

2788 Record the details of the original credential.

2789 *AL3\_ID\_IDC#030 Issue Derived Credential*

2790 Before issuing the derived credential ensure that:

- 2791 a) for in-person issuance, the claimant is the Applicant;
- 2792 b) for remote issuance, token activation requires proof of possession of both the  
2793 derived token and the original **Level 4** token.

2794 **5.3.2.8 Secondary Identity-proofing**

2795 In each of the above cases, the enterprise or specified service must also meet the  
2796 following criteria:

2797 *AL3\_ID\_SCV#010 Secondary checks*

2798 Have in place additional measures (e.g., require additional documentary evidence, delay  
2799 completion while out-of-band checks are undertaken) to deal with:

- 2800 a) any reasonably anomalous circumstance that can reasonably be anticipated (e.g.,  
2801 a legitimate and recent change of address that has yet to be established as the  
2802 address of record);
- 2803 b) any use of processes and/or technologies which may not fully meet the preceding  
2804 applicable requirements but which are deemed to be comparable and thus able to  
2805 support **AL3**.

2806 **5.3.2.9 Identity-proofing Records**

2807 The specific service must retain records of the identity proofing (verification) that it  
2808 undertakes and provide them to qualifying parties when so required.

2809 The enterprise or specified service must:

2810 *AL3\_ID\_VRC#010 Verification Records for Personal Applicants*

2811 Log, taking account of all applicable legislative and policy obligations, a record of the  
2812 facts of the verification process **and the identity of the registrar**, including a reference  
2813 relating to the verification processes, the date and time of verification and the identity of  
2814 the registrar (person, or entity if remote or automatic) performing the proofing functions.

2815 **Guidance:** The facts of the verification process should include the specific record  
2816 information (source, unique reference, value/content) used in establishing the applicant's  
2817 identity, and will be determined by the specific processes used and documents accepted  
2818 by the CSP. The CSP need not retain these records itself if it uses a third-party service  
2819 which retains such records securely and to which the CSP has access when required, in  
2820 which case it must retain a record of the identity of the third-party service providing the  
2821 verification service or the location at which the (in-house) verification was performed.

2822 *AL3\_ID\_VRC#020 Verification Records for Affiliated Applicants*

2823 In addition to the foregoing, log, taking account of all applicable legislative and policy  
2824 obligations, a record of the additional facts of the verification process [omitted].

2825 **Guidance:** Although there is no specific stipulation as to what should be recorded the  
2826 list below suggests facts which would typically be captured:

- 2827 a) the Subject's full name;  
2828 b) the Subject's current telephone or email address of record;  
2829 c) the Subject's acknowledgement of issuing the Subject with a credential;  
2830 d) type, issuing authority, and reference number(s) of all documents checked in the  
2831 identity proofing process;  
2832 e) where required, a telephone or email address for related contact and/or delivery of  
2833 credentials/notifications.

2834 *AL3\_ID\_VRC#025 Provide Subject Identity Records*

2835 If required, provide to qualifying parties records of identity proofing to the extent  
2836 permitted by applicable legislation and/or agreed by the Subscriber.

2837 **Guidance:** the qualifier 'if required' is intended to account for circumstances where  
2838 conditions such as whether a contract or a federation policy permits or is required or  
2839 jurisdiction / legal injunction demand such provision. A qualifying party is any party to  
2840 which provision of such info can justified according to circumstance: by contract/policy;  
2841 with Subject's agreement; with due authority (Court Order, e.g.). The CSP needs to make  
2842 the case, according to their service's characteristics and operating environment.

2843 *AL3\_ID\_VRC#030 Record Retention*

2844 Either retain, securely, the record of the verification/revocation process for the duration of  
2845 the Subject account plus a further period sufficient to allow fulfillment of any period  
2846 required legally, contractually or by any other form of binding agreement or obligation ,  
2847 or submit the same record to a client CSP that has undertaken to retain the record for the  
2848 requisite period or longer.

2849 *AL3\_CM\_IDP#010 Revision to Subject information*

2850 Provide a means for Subjects to securely amend their stored information after  
2851 registration, either by re-proving their identity as in the initial registration process or by  
2852 using their credentials to authenticate their revision. Successful revision must instigate  
2853 the re-issuance of the credential when the data being revised are bound into the  
2854 credential.

2855 **Guidance:** The necessity for re-issuance will be determined by, *inter alia*, policy, the  
2856 technology and practices in use, the nature of change (e.g. registration data not bound into  
2857 the credential) and the nature of the proofing processes.

2858 *AL3\_CM\_IDP#020 Authenticate Subject Information Changes*

2859 Permit only changes which are supported by appropriate and sufficient authentication of  
2860 the legitimacy of change according, to its type.

2861 **Guidance:** The requirement to authenticate the legitimacy of a change will depend upon  
2862 what is retained by the CSP and what is being changed: whereas a change of address may  
2863 require less demanding authentication than may a change of name, a change of date-of-  
2864 birth would be very unlikely and therefore would require substantial supporting  
2865 authentication.

#### 2866 **5.3.2.10 Credential Creation**

2867 These criteria define the requirements for creation of credentials whose highest use is  
2868 AL3. Any credentials/tokens that comply with the criteria stipulated at AL4 are also  
2869 acceptable at AL3 and below.

2870 Note, however, that a token and credential type required by a higher AL but created  
2871 according to these criteria may not necessarily provide that higher level of assurance for  
2872 the claimed identity of the Subject. Authentication can only be provided at the assurance  
2873 level at which the identity is proven.

2874 An enterprise and its specified service must:

2875 *AL3\_CM\_CRN#010 Authenticated Request*

2876 Only accept a request to generate a credential and bind it to an identity if the source of the  
2877 request, i.e., Registration Authority, can be authenticated as being authorized to perform  
2878 identity proofing at AL3 or higher.

2879 *AL3\_CM\_CRN#020 Unique identity*



2880 Ensure that the identity which relates to a specific applicant is unique within the specified  
2881 service, including identities previously used and that are now cancelled other than its re-  
2882 assignment to the same applicant.

2883 **Guidance:** This requirement is intended to prevent identities that may exist in a Relying  
2884 Party's access control lists from possibly representing a different physical person.

2885 Cf. AL3\_CM\_POL#020 which expresses a very similar requirement. Although  
2886 presenting repetition for a single provider, if the identity-proofing functions and  
2887 credential management functions are provided by separate CSPs, each needs to fulfill this  
2888 requirement.

2889 *AL3\_CM\_CRN#030 Credential uniqueness*

2890 Allow the Subject to select a credential (e.g., UserID) that is verified to be unique within  
2891 the specified service's community and assigned uniquely to a single identity Subject.

2892 *AL3\_CM\_CRN#035 Convey credential*

2893 Be capable of conveying the unique identity information associated with a credential to  
2894 Verifiers and Relying Parties.

2895 *AL3\_CM\_CRN#040 Token strength*

2896 **Not use PIN/password tokens.**

2897 *AL3\_CM\_CRN#050 One-time password strength*

2898 Only allow one-time password tokens that:

- 2899 a) **depend on a symmetric key stored on a personal hardware device evaluated**  
2900 **against FIPS 140-2 [FIPS140-2] Level 1 or higher, or equivalent, as**  
2901 **established by a recognized national technical authority;**  
2902 b) **permit at least 10<sup>6</sup> possible password values;**  
2903 c) **require password or biometric activation by the Subject.**

2904 *AL3\_CM\_CRN#055 No stipulation*

2905 *AL3\_CM\_CRN#060 Software cryptographic token strength*

2906 Ensure that software cryptographic keys stored on general-purpose devices:

- 2907 a) are protected by a key and cryptographic protocol that are evaluated against  
2908 FIPS 14-2 [FIPS140-2] Level 1, or equivalent, as established by a recognized  
2909 national technical authority;  
2910 b) **require password or biometric activation by the Subject or employ a**  
2911 **password protocol when being used for authentication;**  
2912 c) **erase any unencrypted copy of the authentication key after each**  
2913 **authentication.**

2914 *AL3\_CM\_CRN#070 Hardware token strength*

2915 Ensure that hardware tokens used to store cryptographic keys:

- 2916 a) employ a cryptographic module that is evaluated against FIPS 140-2 [FIPS140-2]  
2917 Level 1 or higher, or equivalent, as established by a recognized national technical  
2918 authority;
- 2919 **b) require password or biometric activation by the Subject or also employ a**  
2920 **password when being used for authentication;**
- 2921 **c) erase any unencrypted copy of the authentication key after each**  
2922 **authentication.**

2923 *AL3\_CM\_CRN#075 No stipulation*

2924 *AL3\_CM\_CRN#080 Binding of key*

2925 **If the specified service generates the Subject's key pair, that the key generation**  
2926 **process securely and uniquely binds that process to the certificate generation and**  
2927 **maintains at all times the secrecy of the private key, until it is accepted by the**  
2928 **Subject.**

2929 *AL3\_CM\_CRN#090 Nature of Subject*

2930 Record the nature of the Subject of the credential (which must correspond to the manner  
2931 of identity proofing performed), i.e., private person, a named person acting on behalf of a  
2932 corporation or other legal entity, corporation or legal entity, or corporate machine entity,  
2933 in a manner that can be unequivocally associated with the credential and the identity that  
2934 it asserts.

2935 *AL3\_CM\_CRN#095 No stipulation*

2936 No stipulation

### 2937 **5.3.2.11 Subject Key Pair Generation**

2938 An enterprise and its specified service must:

2939 *AL3\_CM\_SKP#010 Key generation by Specified Service*

2940 **If the specified service generates the Subject's keys:**

- 2941 a) use a FIPS 140-2 [FIPS140-2] compliant algorithm, or equivalent, as  
2942 established by a recognized national technical authority, that is recognized as  
2943 being fit for the purposes of the service;
- 2944 b) only create keys of a key length and for use with a FIPS 140-2 [FIPS140-2]  
2945 compliant public key algorithm, or equivalent, as established by a recognized  
2946 national technical authority, recognized as being fit for the purposes of the  
2947 service;
- 2948 c) generate and store the keys securely until delivery to and acceptance by the  
2949 Subject;
- 2950 d) deliver the Subject's private key in a manner that ensures that the privacy of  
2951 the key is not compromised and only the Subject has access to the private  
2952 key.

2953 *AL3\_CM\_SKP#020 Key generation by Subject*



2954 **If the Subject generates and presents its own keys, obtain the Subject's written**  
2955 **confirmation that it has:**

- 2956 a) **used a FIPS 140-2 [FIPS140-2] compliant algorithm, or equivalent, as**  
2957 **established by a recognized national technical authority, that is recognized as**  
2958 **being fit for the purposes of the service;**  
2959 b) **created keys of a key length and for use with a FIPS 140-2 [FIPS140-2]**  
2960 **compliant public key algorithm, or equivalent, as established by a recognized**  
2961 **national technical authority, recognized as being fit for the purposes of the**  
2962 **service.**

### 2963 **5.3.2.12 Credential Delivery**

2964 An enterprise and its specified service must:

2965 *AL3\_CM\_CRD#010, Notify Subject of Credential Issuance*

2966 Notify the Subject of the credential's issuance and, if necessary, confirm Subject's contact  
2967 information by:

- 2968 a) sending notice to the address of record confirmed during identity proofing, **and**  
2969 **either:**  
2970 i) **issuing the credential(s) in a manner that confirms the address of**  
2971 **record supplied by the applicant during identity proofing, or;**  
2972 ii) **issuing the credential(s) in a manner that confirms the ability of the**  
2973 **applicant to receive telephone communications at a phone number**  
2974 **supplied by the applicant during identity proofing, while recording**  
2975 **the applicant's voice.**

2976 **Guidance:** The nature of issuance could mean that the Subject is fully aware and  
2977 therefore no notification is necessary. If any other such circumstances prevailed, the CSP  
2978 should identify them.

2979 *AL3\_CM\_CRD#015 Confirm Applicant's identity (in person)*

2980 Prior to delivering the credential, require the Applicant to identify themselves in person in  
2981 any new transaction (beyond the first transaction or encounter) by either:

- 2982 (a) using a temporary secret which was established during **the** prior transaction or  
2983 encounter (**whilst ensuring that such temporary secrets are used only**  
2984 **once**), or sent to the Applicant's phone number, email address, or physical  
2985 address of record, or;  
2986 (b) matching a biometric sample against a reference sample that was recorded  
2987 during a prior encounter.

2988 *AL3\_CM\_CRD#016 Confirm Applicant's identity (remotely)*

2989 Prior to delivering the credential, require the Applicant to identify themselves in any new  
2990 electronic transaction (beyond the first transaction or encounter) by presenting a

2991 temporary secret which was established during a prior transaction or encounter, or sent to  
2992 the Applicant's phone number, email address, or physical address of record.

2993 *AL3\_CM\_CRD#017 Protected Issuance of Permanent Secrets (in person)*  
2994 **Only issue permanent secrets if the CSP has loaded the secret itself onto the physical**  
2995 **device, which was either:**

2996 **a) issued in-person to the Applicant, or;**

2997 **b) delivered in a manner that confirms the address of record.**

2998 *AL3\_CM\_CRD#018 Protected Issuance of Permanent Secrets (remotely)*

2999 **Only issue permanent secrets within a protected session.**

3000 *AL3\_CM\_CRD#020 Subject's acknowledgement*

3001 **Receive acknowledgement of receipt of the credential before it is activated and its**  
3002 **directory status record is published (and thereby the subscription becomes active or**  
3003 **re-activated, depending upon the circumstances of issue).**

3004

### 3005 **5.3.3 Part C - Credential Renewal and Re-issuing**

3006 These criteria apply to the renewal and re-issuing of credentials. They address  
3007 requirements levied by the use of various technologies to achieve Assurance Level 3.

#### 3008 **5.3.3.1 Renewal/Re-issuance Procedures**

3009 These criteria address general renewal and re-issuance functions, to be exercised as  
3010 specific controls in these circumstances while continuing to observe the general  
3011 requirements established for initial credential issuance.

3012 An enterprise and its specified service must:

3013 *AL3\_CM\_RNR#010 Changeable PIN/Password*

3014 Permit Subjects to change **the passwords used to activate their credentials.**

3015 *AL3\_CM\_RNR#020 Proof-of-possession on Renewal/Re-issuance*

3016 Subjects wishing to change their passwords must demonstrate that they are in possession  
3017 of the unexpired current token prior to the CSP proceeding to renew or re-issue it.

3018 *AL3\_CM\_RNR#030 Renewal/Re-issuance limitations*

3019 a) **No stipulation;**

3020 b) **No stipulation;**

3021 c) **No stipulation;**

3022 d) **conduct all renewal / re-issuance interactions with the Subject over a protected**  
3023 **channel such as SSL/TLS.**

3024 **Guidance:** Renewal is considered as an extension of usability, whereas re-issuance  
3025 requires a change.

3026 *AL3\_CM\_RNR#040 No stipulation*  
3027 No stipulation.

3028 *AL3\_CM\_RNR#050 Record Retention*  
3029 Retain, securely, the record of any renewal/re-issuance process for the duration of the  
3030 Subscriber's account plus a further period sufficient to allow fulfillment of any period  
3031 required legally, contractually or by any other form of binding agreement or obligation, or  
3032 submit same record to a client CSP that has undertaken to retain the record for the  
3033 requisite period or longer.

### 3034 **5.3.4 Part D - Credential Revocation**

3035 These criteria deal with credential revocation and the determination of the legitimacy of a  
3036 revocation request.

#### 3037 **5.3.4.1 Revocation Procedures**

3038 These criteria address general revocation functions, such as the processes involved and  
3039 the basic requirements for publication.

3040 An enterprise and its specified service must:

3041 *AL3\_CM\_RVP#010 Revocation procedures*

- 3042 a) State the conditions under which revocation of an issued credential may occur;
- 3043 b) State the processes by which a revocation request may be submitted;
- 3044 c) State the persons and organizations from which a revocation request will be  
3045 accepted;
- 3046 d) State the validation steps that will be applied to ensure the validity (identity) of  
3047 the Revocant, and;
- 3048 e) State the response time between a revocation request being accepted and the  
3049 publication of revised certificate status.

3050 *AL3\_CM\_RVP#020 Secure status notification*

3051 Ensure that published credential status notification information can be relied upon in  
3052 terms of the enterprise being its origin (i.e., its authenticity) and its correctness (i.e., its  
3053 integrity).

3054 *AL3\_CM\_RVP#030 Revocation publication*

3055 **[Omitted]** Ensure that published credential status notification is revised within **24** hours  
3056 of the receipt of a valid revocation request, such that any subsequent attempts to use that  
3057 credential in an authentication shall be unsuccessful. **The nature of the revocation**  
3058 **mechanism shall be in accord with the technologies supported by the service.**

3059 *AL3\_CM\_RVP#040 Verify Revocation Identity*

3060 Establish that the identity for which a revocation request is received is one that was  
3061 issued by the specified service.

3062 *AL3\_CM\_RVP#050 Revocation Records*

3063 Retain a record of any revocation of a credential that is related to a specific identity  
3064 previously verified, solely in connection to the stated credential. At a minimum, records  
3065 of revocation must include:

- 3066 a) the Revocant's full name;
- 3067 b) the Revocant's authority to revoke (e.g., Subscriber or the Subject themselves,  
3068 someone acting with the Subscriber's or the Subject's power of attorney, the  
3069 credential issuer, law enforcement, or other legal due process);
- 3070 c) the Credential Issuer's identity (if not directly responsible for the identity  
3071 proofing service); [Omitted]
- 3072 d) the reason for revocation.

3073 *AL3\_CM\_RVP#060 Record Retention*

3074 Retain, securely, the record of the revocation process for a period which is the maximum  
3075 of:

- 3076 a) the records retention policy required by AL3\_CM\_CPP#010;
- 3077 b) applicable legislation, regulation, contract or standards.

3078 **5.3.4.2 Verify Revocant's Identity**

3079 Revocation of a credential requires that the requestor and the nature of the request be  
3080 verified as rigorously as the original identity proofing. The enterprise should not act on a  
3081 request for revocation without first establishing the validity of the request (if it does not,  
3082 itself, determine the need for revocation).

3083 In order to do so, the enterprise and its specified service must:

3084 *AL3\_CM\_RVR#010 Verify revocation identity*

3085 Establish that the credential for which a revocation request is received is one that was  
3086 initially issued by the specified service, applying the same process and criteria as would  
3087 be applied to an original identity proofing ensuring that the Subject of the credential is  
3088 uniquely identified.

3089 *AL3\_CM\_RVR#020 Revocation reason*

3090 Establish the reason for the revocation request as being sound and well founded, in  
3091 combination with verification of the Revocant, according to AL3\_ID\_RVR#030,  
3092 AL3\_ID\_RVR#040, or AL3\_ID\_RVR#050.

3093 *AL3\_CM\_RVR#030 Verify Subscriber as Revocant*

3094 When the Subscriber or Subject seeks revocation of the Subject's credential:

- 3095 a) if in-person, require presentation of a primary Government Picture ID document  
3096 that shall be electronically verified by a record check against the provided identity  
3097 with the specified issuing authority's records;  
3098 b) if remote:  
3099 i. electronically verify a signature against records (if available), confirmed  
3100 with a call to a telephone number of record, or;  
3101 ii. as an electronic request, authenticate it as being from the same Subscriber  
3102 or Subject, supported by a credential at Assurance Level **3** or higher.

3103 *AL3\_CM\_RVR#040 Verify CSP as Revocant*

3104 Where a CSP seeks revocation of a Subject's credential, establish that the request is  
3105 either:

- 3106 a) from the specified service itself, with authorization as determined by established  
3107 procedures, or;  
3108 b) from the client Credential Issuer, by authentication of a formalized request over  
3109 the established secure communications network.

3110 *AL3\_CM\_RVR#050 Verify Legal Representative as Revocant*

3111 Where the request for revocation is made by a law enforcement officer or presentation of  
3112 a legal document:

- 3113 a) if in person, verify the identity of the person presenting the request, or;  
3114 b) if remote:  
3115 i. in paper/facsimile form, verify the origin of the legal document by a  
3116 database check or by telephone with the issuing authority, or;  
3117 ii. as an electronic request, authenticate it as being from a recognized legal  
3118 office, supported by a credential at Assurance Level **3** or higher.

3119 **5.3.4.3 No stipulation**

3120 **5.3.4.4 Secure Revocation Request**

3121 This criterion applies when revocation requests must be communicated between remote  
3122 components of the service organization.

3123 An enterprise and its specified service must:

3124 *AL3\_CM\_SRR#010 Submit Request*

3125 Submit a request for the revocation to the Credential Issuer service (function), using a  
3126 secured network communication.

3127 **5.3.5 Part E - Credential Status Management**

3128 These criteria deal with credential status management, such as the receipt of requests for  
3129 new status information arising from a new credential being issued or a revocation or other

3130 change to the credential that requires notification. They also deal with the provision of  
3131 status information to requesting parties (Verifiers, Relying Parties, courts and others  
3132 having regulatory authority, etc.) having the right to access such information.

### 3133 **5.3.5.1 Status Maintenance**

3134 An enterprise and its specified service must:

3135 *AL3\_CM\_CSM#010 Maintain Status Record*

3136 Maintain a record of the status of all credentials issued.

3137 *AL3\_CM\_CSM#020 Validation of Status Change Requests*

3138 Authenticate all requestors seeking to have a change of status recorded and published and  
3139 validate the requested change before considering processing the request. Such validation  
3140 should include:

- 3141 a) the requesting source as one from which the specified service expects to receive  
3142 such requests;
- 3143 b) if the request is not for a new status, the credential or identity as being one for  
3144 which a status is already held.

3145 *AL3\_CM\_CSM#030 Revision to Published Status*

3146 Process authenticated requests for revised status information and have the revised  
3147 information available for access within a period of 72 hours.

3148 *AL3\_CM\_CSM#040 Status Information Availability*

3149 Provide, with **99%** availability, a secure automated mechanism to allow relying parties to  
3150 determine credential status and authenticate the Claimant's identity.

3151 *AL3\_CM\_CSM#050 Inactive Credentials*

3152 Disable any credential that has not been successfully used for authentication during a  
3153 period of 18 months.

### 3154 **5.3.6 Part F - Credential Verification/Authentication**

3155 These criteria apply to credential validation and identity authentication.

#### 3156 **5.3.6.1 Assertion Security**

3157 An enterprise and its specified service must:

3158 *AL3\_CM\_ASS#010 Validation and Assertion Security*

3159 Provide validation of credentials to a Relying Party using a protocol that:

- 3160 a) requires authentication of the specified service, itself, or of the validation source;
- 3161 b) ensures the integrity of the authentication assertion;

- 3162 c) protects assertions against manufacture, modification, substitution and disclosure,  
3163 and secondary authenticators from manufacture, capture and replay;  
3164 d) uses approved cryptography techniques;
- 3165 and which, specifically:
- 3166 e) creates assertions which are specific to a single transaction;  
3167 f) where assertion references are used, generates a new reference whenever a new  
3168 assertion is created;  
3169 g) when an assertion is provided indirectly, either signs the assertion or sends it via a  
3170 protected channel, using a strong binding mechanism between the secondary  
3171 authenticator and the referenced assertion;  
3172 h) send assertions either via a channel mutually-authenticated with the Relying  
3173 Party, or signed and encrypted for the Relying Party;  
3174 i) requires the secondary authenticator to:
- 3175 i) be signed when provided directly to Relying Party, or;
  - 3176 ii) have a minimum of 64 bits of entropy when provision is indirect (i.e.  
3177 through the credential user);
  - 3178 iii) be transmitted to the Subject through a protected channel which is linked  
3179 to the primary authentication process in such a way that session hijacking  
3180 attacks are resisted;
  - 3181 iv) not be subsequently transmitted over an unprotected channel or to an  
3182 unauthenticated party while it remains valid.

3183 *AL3\_CM\_ASS#015 No False Authentication*  
3184 Employ techniques which ensure that system failures do not result in ‘false positive  
3185 authentication’ errors.

3186 *AL3\_CM\_ASS#018 Ensure token validity*  
3187 **Ensure that tokens are either still valid or have been issued within the last 24 hours.**

3188 **Guidance:** The 24-hour period allows for the fact that if a freshly-issued credential is  
3189 then revoked, notice of the revocation may take 24 hours to be publicised (per  
3190 *AL3\_CM\_RVP#030*).

3191 *AL3\_CM\_ASS#020 Post Authentication*  
3192 *Not* authenticate credentials that have been revoked unless the time of the transaction for  
3193 which verification is sought precedes the time of revocation of the credential.

3194 **Guidance:** The purpose in this criterion is that, if a verification is intended to refer to the  
3195 status of a credential at a specific historical point in time, e.g. to determine whether the  
3196 Claimant was entitled to act as a signatory in a specific capacity at the time of the  
3197 transaction, this may be done. It is implicit in this thinking that both the request and the  
3198 response indicate the historical nature of the query and response; otherwise the default  
3199 time is ‘now’. If no such service is offered then this criterion may simply be  
3200 ‘Inapplicable’, for that reason.

3201 *AL3\_CM\_ASS#030 Proof of Possession*



3202 Use an authentication protocol that requires the claimant to prove possession and control  
3203 of the authentication token.

3204 *AL3\_CM\_ASS#035 Limit authentication attempts*

3205 Unless the token authenticator has at least 64 bits of entropy, limit the number of failed  
3206 authentication attempts to no more than 100 in any 30-day period.

3207 *AL3\_CM\_ASS#040 Assertion Lifetime*

3208 **For non-cryptographic credentials**, generate assertions so as to indicate and effect their  
3209 expiration 12 hours after their creation; **otherwise, notify the relying party of how often**  
3210 **the revocation status sources are updated.**

### 3211 **5.3.6.2 Authenticator-generated challenges**

3212 An enterprise and its specified service must:

3213 *AL3\_CM\_AGC#010 Entropy level*

3214 Create authentication secrets to be used during the authentication exchange (i.e. with out-  
3215 of-band or cryptographic device tokens) with a degree of entropy appropriate to the token  
3216 type in question.

### 3217 **5.3.6.3 Multi-factor authentication**

3218 An enterprise and its specified service must:

3219 *AL3\_CM\_MFA#010 Permitted multi-factor tokens*

3220 Require two tokens which, when used in combination within a single authentication  
3221 exchange, are acknowledged as providing an equivalence of AL3, as determined by a  
3222 recognized national technical authority.

### 3223 **5.3.6.4 Verifier's assertion schema**

3224 Note: Since assertions and related schema can be complex and may be modeled directly  
3225 on the needs and preferences of the participants, the details of such schema fall outside  
3226 the scope of the SAC's herein, which are expressed observing, insofar as is feasible, a  
3227 technology-agnostic policy. The following criteria, therefore, are perhaps more open to  
3228 variable conformity through their final implementation than are others in this document.

3229 These criteria are derived directly from NIST SP 800-63-2 and have been expressed in as  
3230 generic a manner as they can be.

3231 *Editor's note: I have avoided reference to the RP here – I am concerned as to what the*  
3232 *SAC requires services to do, not who might be using their products. SAC do not refer to*  
3233 *RPs.*

3234 An enterprise and its specified service must:

- 3235 *AL3\_CM\_VAS#010 Approved cryptography*  
3236 Apply assertion protocols which use cryptographic techniques approved by a national  
3237 authority or other generally-recognized authoritative body.
- 3238 *AL3\_CM\_VAS#020 No stipulation*  
3239 No stipulation.
- 3240 *AL3\_CM\_VAS#030 Assertion assurance level*  
3241 Create assertions which, either explicitly or implicitly (using a mutually-agreed  
3242 mechanism), indicate the assurance level at which the initial authentication of the Subject  
3243 was made.
- 3244 *AL3\_CM\_VAS#040 No pseudonyms*  
3245 Create assertions which indicate **only verified Subscriber names** in the credential  
3246 subject to verification.
- 3247 *AL3\_CM\_VAS#050 Specify recipient*  
3248 Create assertions which identify the intended recipient of the verification such that the  
3249 recipient may validate that it is intended for them.
- 3250 *AL3\_CM\_VAS#060 No assertion manufacture/modification*  
3251 Ensure that it is impractical to manufacture an assertion or assertion reference by **Signing**  
3252 **the assertion and** using at least one of the following techniques:
- 3253 a) **Signing the assertion;**  
3254 b) **Encrypting the assertion using a secret key shared with the RP;**  
3255 c) **Creating an assertion reference which has a minimum of 64 bits of entropy;**  
3256 d) **Sending the assertion over a protected channel during a mutually-authenticated**  
3257 **session.**
- 3258 *AL3\_CM\_VAS#070 Assertion protections*  
3259 Provide protection of assertion-related data such that:
- 3260 a) **both assertions and assertion references are protected against capture and re-use;**  
3261 b) **assertions are also protected against redirection;**  
3262 c) **assertions, assertion references and session cookies used for authentication**  
3263 **purposes, including any which are re-directed, are protected against session**  
3264 **hijacking, for at least the duration of their validity (see AL3\_CM\_VAS#110).**
- 3265 *AL3\_CM\_VAS#080 Single-use assertions*  
3266 Limit to a single transaction the use of assertions which do not support proof of  
3267 ownership.
- 3268 *AL3\_CM\_VAS#090 Single-use assertion references*  
3269 Limit to a single transaction the use of assertion references.

3270 *AL3\_CM\_VAS#100 Bind reference to assertion*  
3271 Provide a strong binding between the assertion reference and the corresponding assertion,  
3272 based on integrity-protected (or signed) communications over which the Verifier has been  
3273 authenticated.

3274 *AL3\_CM\_VAS#110 SSO provisions*

3275 **If SSO is supported, provide a re-authentication of the Subject so long as:**

- 3276 **a) the Subject has been successfully authenticated within the last 12 hours;**  
3277 **b) the Subject continues to be able to demonstrate that they were the party that**  
3278 **was previously authenticated;**  
3279 **c) it can be ensured that the Subscriber has not been inactive for more than 30**  
3280 **minutes.**

3281 **Guidance:** The conditional nature of this criterion is dictated by the phrasing used in  
3282 NIST SP 800-63 which states 'may'.

3283

## 3284 5.4 Assurance Level 4

### 3285 5.4.1 Part A - Credential Operating Environment

3286 These criteria describe requirements for the overall operational environment in which  
3287 credential lifecycle management is conducted. The Common Organizational criteria  
3288 describe broad requirements. The criteria in this Part describe operational  
3289 implementation specifics.

3290 These criteria apply exclusively to cryptographic technology deployed through a Public  
3291 Key Infrastructure. This technology requires hardware tokens protected by password or  
3292 biometric controls. No other forms of credential are permitted at AL4.

3293 The following four criteria are **MANDATORY** for all Services, Full or Component, and  
3294 are individually marked as such:

3295 AL4\_CM\_CPP#020, AL4\_CM\_CPP#030, AL4\_CM\_CTR#030, AL4\_CM\_SER#010.

#### 3296 5.4.1.1 Certification Policy and Practices

3297 These criteria apply to the policy and practices under which certificates are managed.

3298 An enterprise and its specified service must:

3299 *AL4\_CM\_CPP#010 No stipulation*

3300 *AL4\_CM\_CPP#020 Certificate Policy/Certification Practice Statement*

3301 **MANDATORY.**

3302 **Include in its Service Definition its full Certificate Policy and the corresponding**  
3303 **Certification and Practice Statement. The Certificate Policy and Certification**  
3304 **Practice Statement must conform to IETF RFC 3647 (2003-11) [RFC 3647] in their**  
3305 **content and scope or be demonstrably consistent with the content or scope of that**  
3306 **RFC. At a minimum, the Certificate Policy must specify:**

- 3307 a) **applicable OIDs for each certificate type issued;**
- 3308 b) **how users may subscribe to the service/apply for certificates, and how**  
3309 **certificates will be issued to them;**
- 3310 c) **if users present their own keys, how they will be required to demonstrate**  
3311 **possession of the private key;**
- 3312 d) **if users' keys are generated for them, how the private keys will be delivered**  
3313 **to them;**
- 3314 e) **how Subjects acknowledge receipt of tokens and credentials and what**  
3315 **obligations they accept in so doing (including whether they consent to**  
3316 **publication of their details in certificate status directories);**

- 3317 f) **how certificates may be renewed, re-keyed, modified, revoked, and**  
3318 **suspended, including how requestors are authenticated or their identity**  
3319 **proven;**  
3320 g) **what actions a Subject must take to terminate their subscription.**

3321 *ALA\_CM\_CPP#030 Management Authority*  
3322 **MANDATORY.**

3323 Have a nominated or appointed high-level management body with authority and  
3324 responsibility for approving the Certificate Policy and Certification Practice Statement,  
3325 including ultimate responsibility for their proper implementation.

3326 *ALA\_CM\_CPP#040 Discretionary Access Control*  
3327 **Apply discretionary access controls that limit access to trusted administrators and to**  
3328 **those applications that require access.**

3329 **Guidance:** This requirement was previously AL3\_CM\_STS#010 b) (part a) having been  
3330 withdrawn, which left part b) somewhat out of context.

#### 3331 **5.4.1.2 Security Controls**

3332 An enterprise and its specified service must:

3333 *ALA\_CM\_CTR#010 Withdrawn*

3334 *ALA\_CM\_CTR#020 Protocol threat risk assessment and controls*

3335 Account for at least the following protocol threats in its risk assessment and apply  
3336 controls that reduce them to acceptable risk levels:

- 3337 a) password guessing, **showing that there is sufficient entropy;**  
3338 b) message replay, showing that it is impractical;  
3339 c) eavesdropping, showing that it is impractical;  
3340 d) relying party (verifier) impersonation, showing that it is impractical;  
3341 e) man-in-the-middle attack, **showing that it is impractical;**  
3342  
3343 f) **session hijacking, showing that it is impractical.**

3344 The above list shall not be considered to be a complete list of threats to be addressed by  
3345 the risk assessment.

3346 **Guidance:** Organizations should consider potential protocol threats identified in other  
3347 sources, e.g. ISO/IEC 29115:2013 “Information technology -- Security techniques –  
3348 Entity authentication assurance framework”. *ALA\_CM\_CTR#025 No stipulation*

3349 *ALA\_CM\_CTR#028 No Stipulation*

3350 *ALA\_CM\_CTR#030 System threat risk assessment and controls*  
3351 **MANDATORY.**

3352 Account for the following system threats in its risk assessment and apply controls that  
3353 reduce them to acceptable risk levels:

- 3354 a) the introduction of malicious code;
- 3355 b) compromised authentication arising from insider action;
- 3356 c) out-of-band attacks by both users and system operators (e.g., shoulder-surfing);
- 3357 d) spoofing of system elements/applications;
- 3358 e) malfeasance on the part of Subscribers and Subjects;
- 3359 f) intrusions leading to information theft.

3360 The above list shall not be considered to be a complete list of threats to be addressed by  
3361 the risk assessment.

3362 **Guidance:** the risk assessment should address these threats from any perspective in  
3363 which they might adversely affect the operation of the service, whether they be from  
3364 within the organization (e.g. in its development environment, the hosting environment) or  
3365 without (e.g. network attacks, hackers).

3366 *AL4\_CM\_CTR#040 Specified Service's Key Management*

3367 Specify and observe procedures and processes for the generation, storage, and destruction  
3368 of its own cryptographic keys used for securing the specific service's assertions and other  
3369 publicized information. At a minimum, these should address:

- 3370 a) the physical security of the environment;
- 3371 b) access control procedures limiting access to the minimum number of authorized  
3372 personnel;
- 3373 c) public-key publication mechanisms;
- 3374 d) application of controls deemed necessary as a result of the service's risk  
3375 assessment;
- 3376 e) destruction of expired or compromised private keys in a manner that prohibits  
3377 their retrieval, or their archival in a manner which prohibits their reuse;
- 3378 f) applicable cryptographic module security requirements, quoting FIPS 140-2  
3379 [FIPS140-2] or equivalent, as established by a recognized national technical  
3380 authority.

### 3381 **5.4.1.3 Storage of Long-term Secrets**

3382 The enterprise and its specified service must meet the following criteria:

3383 *AL4\_CM\_STS#010* **Withdrawn**

3384 Withdrawn (AL4\_CO\_SCO#020 (a) & (b) enforce this requirement **part a)** and  
3385 **AL4\_CM\_CPP#040** now enforces **part b)**)

3386 *AL4\_CM\_STS#020 Stored Secret Encryption*

3387 Encrypt such **[omitted]** secret files so that:

- 3388 a) the encryption key for the [omitted] secret file is encrypted under a key held in a  
3389 FIPS 140-2 [FIPS140-2] Level 2 or higher validated hardware cryptographic  
3390 module or any FIPS 140-2 Level 3 or 4 cryptographic module, or equivalent, as  
3391 established by a recognized national technical authority;
- 3392 b) the [omitted] secret file is decrypted only as immediately required for a key  
3393 recovery operation;
- 3394 c) [omitted] secrets are protected as a key within the boundary of a FIPS 140-2  
3395 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2  
3396 Level 3 or 4 cryptographic module and are not exported from the module in  
3397 plaintext, or equivalent, as established by a recognized national technical  
3398 authority;
- 3399 d) escrowed secrets are split by an "n from m" cryptographic secret **storing** method.

#### 3400 5.4.1.4 Security-relevant Event (Audit) Records

3401 These criteria describe the need to provide an auditable log of all events that are pertinent  
3402 to the correct and secure operation of the service. The common organizational criteria  
3403 relating to the recording of all security-related events must also be considered carefully.  
3404 These criteria carry implications for credential management operations.

3405 In the specific context of a certificate management service, an enterprise and its specified  
3406 service must:

3407 *ALA\_CM\_SER#010 Security event logs*

3408 **MANDATORY**, to the extent that the sub-items relate to the scope of service.

3409 Ensure that such audit records include:

- 3410 a) the identity of the point of registration (irrespective of whether internal or  
3411 outsourced);
- 3412 b) generation of the Subject's keys or evidence that the Subject was in possession of  
3413 both parts of the key-pair;
- 3414 c) generation of the Subject's certificate;
- 3415 d) dissemination of the Subject's certificate;
- 3416 e) any revocation or suspension associated with the Subject's credential.

#### 3417 5.4.1.5 Subject Options

3418 *ALA\_CM\_OPN#010 Changeable PIN/Password*

3419 Withdrawn – see AL4\_CM\_RNR#010.



## 3420 5.4.2 Part B - Credential Issuing

3421 These criteria apply to the verification of the identity of the Subject of a credential and  
3422 with token strength and credential delivery mechanisms. They address requirements  
3423 levied by the use of various technologies to achieve Assurance Level 4.

### 3424 5.4.2.1 Identity Proofing Policy

3425 Identity proofing at Assurance Level 4 requires the physical presence of the applicant in  
3426 front of the registration officer with photo ID or other readily verifiable biometric identity  
3427 information, as well as the requirements set out by the following criteria.

3428 The specific service must show that it applies identity proofing policies and procedures  
3429 and that it retains appropriate records of identity proofing activities and evidence.

3430 An enterprise and its specified service must:

3431 *ALA\_ID\_POL#010 Unique service identity*

3432 Ensure that a unique identity is attributed to the specific service, such that credentials  
3433 issued by it can be distinguishable from those issued by other services, including services  
3434 operated by the same enterprise.

3435 *ALA\_ID\_POL#020 Unique Subject identity*

3436 Ensure that each applicant's identity is unique within the service's community of Subjects  
3437 and uniquely associable with tokens and/or credentials issued to that identity.

3438 **Guidance:** Cf. AL4\_CM\_CRN#020 which expresses a very similar requirement.  
3439 Although presenting repetition for a single provider, if the identity-proofing functions and  
3440 credential management functions are provided by separate CSPs, each needs to fulfill this  
3441 requirement.

3442 *ALA\_ID\_POL#030 Published Proofing Policy*

3443 Make available the Identity Proofing Policy under which it verifies the identity of  
3444 applicants<sup>5</sup> in form, language, and media accessible to the declared community of users.

3445 *ALA\_ID\_POL#040 Adherence to Proofing Policy*

3446 Perform all identity proofing strictly in accordance with its published Identity Proofing  
3447 Policy, through application of the procedures and processes set out in its Identity Proofing  
3448 Practice Statement (IdPPS).

---

<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.

#### 3449 **5.4.2.2 Identity Verification**

3450 The enterprise or specific service may:

3451 *AL4\_ID\_IDV#000 Identity Proofing classes*

3452 **[Omitted] offer only face-to-face identity proofing service. Remote verification is not**  
3453 **allowed at this assurance level;**

3454 *AL4\_ID\_IDV#010 - Identity Verification Measures*

3455 **[Omitted]** Justify the identity verification measures described in its IdPPS (see  
3456 *AL4\_ID\_POL#040*) by describing how these meet or exceed the requirements of  
3457 applicable policies, regulations, adopted standards and other relevant conditions in order  
3458 to maintain a level of rigour consistent with the **AL4**.

3459 **Guidance:** Although strict requirements for identity proofing and verification can be  
3460 defined, a real-world approach must account for instances where there is not 100%  
3461 certitude. To cope with this CSPs need to have a set of prescribed (through policy – see  
3462 *AL4\_ID\_POL#030*) and applied measures (see *AL4\_ID\_POL#040*) which observe  
3463 policy, identify the measures taken according to the degree of certitude determined by  
3464 each step in the verification process and what additional measures are taken. The CSP  
3465 must present a case which shows that their solution is sufficient to ensure that the basic  
3466 requirements of the applicable AL are met or exceeded.

3467 Note that in each set of proofing service criteria below there are criteria with specific  
3468 requirements for evidence checks and an additional criterion for ‘secondary’ checks, all of  
3469 which have an interplay with these overall requirements to have a policy and practice  
3470 statement and to demonstrate processes which sustain confidence that AL3 is being  
3471 achieved.

3472 Even though a CSP may use the services of a component service for the performance of  
3473 the identity-proofing within its own service, it still needs to ensure that its policy is both  
3474 justified and upheld. Where another service provider is used appropriate stipulations in  
3475 contracts should be established, but any internal adherence to (e.g.) ‘POL#040 should be  
3476 determined by the fact that the component service is already Kantara Approved.

#### 3477 **5.4.2.3 In-Person Public Identity Proofing**

3478 A specific service that offers identity proofing to applicants with whom it has no previous  
3479 relationship must comply with the criteria in this section.

3480 The enterprise or specified service must:

3481 *AL4\_ID\_IPV#010 Required evidence*

3482 Ensure that the applicant is in possession of:

3483 a) a primary Government Picture ID document that bears a photographic image of  
3484 the **holder and either:**

- 3485 i) secondary Government Picture ID or an account number issued by a  
3486 regulated financial institution or;  
3487 ii) two items confirming name, and address or telephone number, such  
3488 as: utility bill, professional license or membership, or other evidence  
3489 of equivalent standing.

3490 *ALA\_ID\_IPV#020 No stipulation*

3491 *ALA\_ID\_IPV#030 Evidence checks – primary ID*

3492 **Ensure that the presented document:**

- 3493 a) appears to be a genuine document properly issued by the claimed issuing  
3494 authority and valid at the time of application;  
3495 b) bears a photographic image of the holder which matches that of the  
3496 applicant;  
3497 c) is electronically verified by a record check with the specified issuing  
3498 authority or through similar databases that:  
3499 i) establishes the existence of such records with matching name and  
3500 reference numbers;  
3501 ii) corroborates date of birth, current address of record, and other  
3502 personal information sufficient to ensure a unique identity;  
3503 d) provides all reasonable certainty, at AL4, that the identity exists and that it  
3504 uniquely identifies the applicant.

3505 *ALA\_ID\_IPV#040 Evidence checks – secondary ID*

3506 **Ensure that the presented document meets the following conditions:**

- 3507 a) **If it is secondary Government Picture ID:**  
3508 i) appears to be a genuine document properly issued by the claimed  
3509 issuing authority and valid at the time of application;  
3510 ii) bears a photographic image of the holder which matches that of the  
3511 applicant;  
3512 iii) states an address at which the applicant can be contacted.  
3513 b) **If it is a financial institution account number, is verified by a record check**  
3514 **with the specified issuing authority or through similar databases that:**  
3515 i) establishes the existence of such records with matching name and  
3516 reference numbers;  
3517 ii) corroborates date of birth, current address of record, and other  
3518 personal information sufficient to ensure a unique identity.  
3519 c) **If it is two utility bills or equivalent documents:**  
3520 i) each appears to be a genuine document properly issued by the  
3521 claimed issuing authority;  
3522 ii) corroborates current address of record or telephone number sufficient to  
3523 ensure a unique identity.

3524 *ALA\_ID\_IPV#050 Applicant knowledge checks*

3525 **Where the applicant is unable to satisfy any of the above requirements, that the**  
3526 **applicant can provide a unique identifier, such as a Social Security Number (SSN),**  
3527 **that matches the claimed identity.**

3528 **5.4.2.4 Remote Public Identity Proofing**

3529 **Not permitted.**

3530 **5.4.2.5 Current Relationship Identity Proofing**

3531 **Not permitted**

3532 **5.4.2.6 Affiliation Identity Proofing**

3533 A specific service that offers identity proofing to applicants on the basis of some form of  
3534 affiliation must comply with the criteria in this section to establish that affiliation, in  
3535 addition to complying with the previously stated requirements for verifying the  
3536 individual's identity.

3537 The enterprise or specified service must:

3538 *ALA\_ID\_AFV#000 Meet preceding criteria*

3539 Meet all the criteria set out above, under §5.4.2.3, “[In-Person Public Identity](#)  
3540 [Verification](#)”.

3541 *ALA\_ID\_AFV#010 Required evidence*

3542 Ensure that the applicant possesses:

- 3543 a) identification from the organization with which it is claiming affiliation;  
3544 b) agreement from the organization that the applicant may be issued a credential  
3545 indicating that an affiliation exists.

3546 *ALA\_ID\_AFV#020 Evidence checks*

3547 Have in place and apply processes which ensure that the presented documents:

- 3548 a) each appear to be a genuine document properly issued by the claimed issuing  
3549 authorities and valid at the time of application;  
3550 b) refer to an existing organization with a contact address;  
3551 c) indicate that the applicant has some form of recognizable affiliation with the  
3552 organization;  
3553 d) appear to grant the applicant an entitlement to obtain a credential indicating an  
3554 affiliation with the organization.

3555 **5.4.2.7 Issuing Derived Credentials**

3556 Where the Applicant already possesses recognized original credentials the CSP may  
3557 choose to accept the verified identity of the Applicant as a substitute for identity proofing,  
3558 subject to the following specific provisions. All other identity proofing requirements  
3559 must also be observed.

3560 *ALA\_ID\_IDC#010 Authenticate Original Credential*

3561 Prior to issuing any derived credential the original credential on which the identity-  
3562 proofing relies must be:

- 3563 a) authenticated by a source trusted by the CSP as being valid and un-revoked;  
3564 b) issued at Assurance Level 4;  
3565 c) issued in the same name as that which the Applicant is claiming;  
3566 d) proven to be in the possession and under the control of the Applicant, **who shall**  
3567 **be physically present.**

3568 **Guidance:** This is the equivalent of recording the details of id documents provided  
3569 during (e.g.) face-face id-proofing. It is not required that the original credential be issued  
3570 by a Kantara-Approved CSP.

3571 *ALA\_ID\_IDC#020 Record Original Credential*

3572 Record the details of the original credential, **the biometric sample related to the**  
3573 **original credential and the biometric sample captured when authenticating the**  
3574 **Applicant.**

3575 *ALA\_ID\_IDC#030 Issue Derived Credential*

3576 **Only issue the derived credential in-person after performing biometric**  
3577 **authentication of the Applicant .**

3578 **5.4.2.8 Secondary Identity Verification**

3579 In each of the above cases, the enterprise or specified service must also meet the  
3580 following criteria:

3581 *ALA\_ID\_SCV#010 Secondary checks*

3582 Have in place additional measures (e.g., require additional documentary evidence, delay  
3583 completion while out-of-band checks are undertaken) to deal with any anomalous  
3584 circumstances that can reasonably be anticipated (e.g., a legitimate and recent change of  
3585 address that has yet to be established as the address of record).

3586

3587 **5.4.2.9 Identity-proofing Records**

3588 The specific service must retain records of the identity proofing (verification) that it  
3589 undertakes and provide them to qualifying parties when so required.

3590 The enterprise or specified service must:

3591 *ALA\_ID\_VRC#010 Verification Records for Personal Applicants*

3592 Log, taking account of all applicable legislative and policy obligations, a record of the  
3593 facts of the verification process and the identity of the registrar (person, or entity if  
3594 remote or automatic) performing the proofing functions, including a reference relating to  
3595 the verification processes and the date and time of verification **issued by a trusted time-**  
3596 **source**.

3597 **Guidance:** The facts of the verification process should include the specific record  
3598 information (source, unique reference, value/content) used in establishing the applicant's  
3599 identity, and will be determined by the specific processes used and documents accepted  
3600 by the CSP. The CSP need not retain these records itself if it uses a third-party service  
3601 which retains such records securely and to which the CSP has access when required, in  
3602 which case it must retain a record of the identity of the third-party service providing the  
3603 verification service or the location at which the (in-house) verification was performed.

3604 *ALA\_ID\_VRC#020 Verification Records for Affiliated Applicants*

3605 In addition to the foregoing, log, taking account of all applicable legislative and policy  
3606 obligations, a record of the additional facts of the verification process [omitted].

3607 **Guidance:** Although there is no specific stipulation as to what should be recorded the  
3608 list below suggests facts which would typically be captured at this level:

- 3609 a) the Subject's full name;
- 3610 b) the Subject's current address of record;
- 3611 c) the Subject's current telephone or email address of record;
- 3612 d) the Subscriber's authorization for issuing the Subject a credential;
- 3613 e) type, issuing authority, and reference number(s) of all documents checked in the  
3614 identity proofing process;
- 3615 f) a biometric record of each required representative of the affiliating organization  
3616 (e.g., a photograph, fingerprint, voice recording), as determined by that  
3617 organization's governance rules/charter.

3618 *ALA\_ID\_VRC#025 Provide Subject identity records*

3619 If required, provide to qualifying parties records of identity proofing to the extent  
3620 permitted by applicable legislation and/or agreed by the Subscriber.

3621 **Guidance:** the qualifier 'if required' is intended to account for circumstances where  
3622 conditions such as whether a contract or a federation policy permits or is required or  
3623 jurisdiction / legal injunction demand such provision. A qualifying party is any party to  
3624 which provision of such info can justified according to circumstance: by contract/policy;

3625 with Subject's agreement; with due authority (Court Order, e.g.). The CSP needs to make  
3626 the case, according to their service's characteristics and operating environment.

3627 *AL4\_ID\_VRC#030 Record Retention*

3628 Either retain, securely, the record of the verification/revocation process for the duration of  
3629 the Subject account plus a further period sufficient to allow fulfillment of any period  
3630 required legally, contractually or by any other form of binding agreement or obligation, or  
3631 submit the record to a client CSP that has undertaken to retain the record for the requisite  
3632 period or longer.

3633 *AL4\_CM\_IDP#010 Revision to Subscriber information*

3634 Provide a means for Subscribers and Subjects to securely amend their stored information  
3635 after registration, either by re-proving their identity as in the initial registration process or  
3636 by using their credentials to authenticate their revision. Successful revision must, where  
3637 necessary, instigate the re-issuance of the credential.

3638 *AL4\_CM\_IDP#020 No stipulation*

#### 3639 **5.4.2.10 Credential Creation**

3640 These criteria define the requirements for creation of credentials whose highest use is  
3641 AL4.

3642 Note, however, that a token and credential created according to these criteria may not  
3643 necessarily provide that level of assurance for the claimed identity of the Subject.  
3644 Authentication can only be provided at the assurance level at which the identity is proven.

3645 An enterprise and its specified service must:

3646 *AL4\_CM\_CRN#010 Authenticated Request*

3647 Only accept a request to generate a credential and bind it to an identity if the source of the  
3648 request, i.e., Registration Authority, can be authenticated as being authorized to perform  
3649 identity proofing at AL4.

3650 *AL4\_CM\_CRN#020 Unique identity*

3651 Ensure that the identity which relates to a specific applicant is unique within the specified  
3652 service, including identities previously used and that are now cancelled, other than its re-  
3653 assignment to the same applicant.

3654 **Guidance:** This requirement is intended to prevent identities that may exist in a Relying  
3655 Party's access control lists from possibly representing a different physical person.

3656 Cf. AL4\_CM\_POL#020 which expresses a very similar requirement. Although  
3657 presenting repetition for a single provider, if the identity-proofing functions and  
3658 credential management functions are provided by separate CSPs, each needs to fulfill this  
3659 requirement.

3660 *AL4\_CM\_CRN#030 Credential uniqueness*



3661 Allow the Subject to select a credential (e.g., UserID) that is verified to be unique within  
3662 the specified service's community and assigned uniquely to a single identity Subject.

3663 *ALA\_CM\_CRN#035 Convey credential*

3664 Be capable of conveying the unique identity information associated with a credential to  
3665 Verifiers and Relying Parties.

3666 *ALA\_CM\_CRN#040 Token strength*

3667 **Not use PIN/password tokens.**

3668 *ALA\_CM\_CRN#050 One-time password strength*

3669 **Not use one-time password tokens.**

3670 *ALA\_CM\_CRN#055 No stipulation*

3671 *ALA\_CM\_CRN#060 Software cryptographic token strength*

3672 **Not use software cryptographic tokens.**

3673 *ALA\_CM\_CRN#070 One-time password hardware token strength*

3674 Ensure that hardware tokens used to store cryptographic keys:

3675 a) employ a cryptographic module that is validated against FIPS 140-2 [FIPS140-2]  
3676 Level 2 or higher, or equivalent, as determined by a recognized national technical  
3677 authority;

3678 b) require password or biometric activation by the Subject [omitted];

3679 c) **Generate a one-time password using an algorithm recognized by a national**  
3680 **technical authority.**

3681 *ALA\_CM\_CRN#075 Multi-factor hardware cryptographic token strength*

3682 **Ensure that hardware tokens used to store cryptographic keys:**

3683 a) **employ a cryptographic module that is validated against FIPS 140-2**  
3684 **[FIPS140-2] Level 2 or higher, or equivalent, as determined by a recognized**  
3685 **national technical authority;**

3686 b) **are evaluated against FIPS 140-2 Level 3 or higher, or equivalent, as**  
3687 **determined by a recognized national technical authority, for their physical**  
3688 **security;**

3689 c) **require password, PIN or biometric activation by the Subject when being**  
3690 **used for authentication;**

3691 d) **does not permit the export of authentication keys.**

3692 *ALA\_CM\_CRN#080 Binding of key*

3693 If the specified service generates the Subject's key pair, that the key generation process  
3694 securely and uniquely binds that process to the certificate generation and maintains at all  
3695 times the secrecy of the private key, until it is accepted by the Subject.

3696 *ALA\_CM\_CRN#090 Nature of Subject*

3697 Record the nature of the Subject of the credential **[omitted]**, i.e., private person, a named  
3698 person acting on behalf of a corporation or other legal entity, corporation or legal entity,  
3699 or corporate machine entity, in a manner that can be unequivocally associated with the  
3700 credential and the identity that it asserts.

3701 *ALA\_CM\_CRN#095 No stipulation*  
3702 No stipulation

#### 3703 **5.4.2.11 Subject Key Pair Generation**

3704 An enterprise and its specified service must:

3705 *ALA\_CM\_SKP#010 Key generation by Specified Service*

3706 If the specified service generates the Subject's keys:

- 3707 a) use a FIPS 140-2 [[FIPS140-2](#)] compliant algorithm, or equivalent, as established  
3708 by a recognized national technical authority, that is recognized as being fit for the  
3709 purposes of the service;
- 3710 b) only create keys of a key length and for use with a FIPS 140-2 [[FIPS140-2](#)]  
3711 compliant public key algorithm, or equivalent, as established by a recognized  
3712 national technical authority, recognized as being fit for the purposes of the  
3713 service;
- 3714 c) generate and store the keys securely until delivery to and acceptance by the  
3715 Subject;
- 3716 d) deliver the Subject's private key in a manner that ensures that the privacy of the  
3717 key is not compromised and only the Subject has access to the private key.

3718 *ALA\_CM\_SKP#020 Key generation by Subject*

3719 If the Subject generates and presents its own keys, obtain the Subject's written  
3720 confirmation that it has:

- 3721 a) used a FIPS 140-2 [[FIPS140-2](#)] compliant algorithm, or equivalent, as established  
3722 by a recognized national technical authority, that is recognized as being fit for the  
3723 purposes of the service;
- 3724 b) created keys of a key length and for use with a FIPS 140-2 [[FIPS140-2](#)] compliant  
3725 public key algorithm, or equivalent, as established by a recognized national  
3726 technical authority, recognized as being fit for the purposes of the service.

#### 3727 **5.4.2.12 Credential Delivery**

3728 An enterprise and its specified service must:

3729 *ALA\_CM\_CRD#010 Notify Subject of Credential Issuance*

3730 Notify the Subject of the credential's issuance and, if necessary, confirm Subject's contact  
3731 information by:

- 3732 a) sending notice to the address of record confirmed during identity proofing;

- 3733 b) unless the Subject presented with a private key, issuing the hardware token  
3734 to the Subject in a manner that confirms the address of record supplied by  
3735 the applicant during identity proofing;  
3736 c) issuing the certificate to the Subject over a separate channel in a manner that  
3737 confirms either the address of record or the email address supplied by the  
3738 applicant during identity proofing.

3739 **Guidance:** The nature of issuance could mean that the Subject is fully aware and  
3740 therefore no notification is necessary. If any other such circumstances prevailed, the CSP  
3741 should identify them.

3742 *ALA\_CM\_CRD#015 Confirm Applicant's identity (in person)*

3743 Prior to delivering the credential, require the Applicant to identify themselves in person in  
3744 any new transaction (beyond the first transaction or encounter) **[deleted]** through the use  
3745 of a biometric that was recorded during **the first** encounter.

3746 *ALA\_CM\_CRD#016 No stipulation*

3747 **No stipulation.**

3748 *ALA\_CM\_CRD#017 Protected Issuance of Permanent Secrets (in person)*

3749 Only issue permanent secrets if the CSP has loaded the secret itself onto the physical  
3750 device, which was either:

- 3751 a) issued in-person to the Applicant, or;  
3752 b) delivered in a manner that confirms the address of record.

3753 *ALA\_CM\_CRD#018 No stipulation*

3754 **No stipulation.**

3755 *ALA\_CM\_CRD#020 Subject's acknowledgement*

3756 Receive acknowledgement of receipt of the **hardware token** before it is activated and **the**  
3757 **corresponding certificate and** its directory status record are published (and thereby the  
3758 subscription becomes active or re-activated, depending upon the circumstances of issue).

### 3759 **5.4.3 Part C - Credential Renewal and Re-issuing**

3760 These criteria apply to the renewal and re-issuing of credentials. They address  
3761 requirements levied by the use of various technologies to achieve Assurance Level 4.

#### 3762 **5.4.3.1 Renewal/Re-issuance Procedures**

3763 These criteria address general renewal and re-issuance functions, to be exercised as  
3764 specific controls in these circumstances while continuing to observe the general  
3765 requirements established for initial credential issuance.

3766 An enterprise and its specified service must:

3767 *ALA\_CM\_RNR#010 Changeable PIN/Password*

3768 Permit Subjects to change the passwords used to activate their credentials.

3769 *ALA\_CM\_RNR#020 Proof-of-possession on Renewal/Re-issuance*

3770 Subjects wishing to change their passwords must demonstrate that they are in possession  
3771 of the unexpired current token prior to the CSP proceeding to renew or re-issue it.

3772 *ALA\_CM\_RNR#030 Renewal/Re-issuance limitations*

3773 a) No stipulation;

3774 b) No stipulation;

3775 c) No stipulation;

3776 d) **cryptographically authenticate** all **sensitive** renewal / re-issuance interactions  
3777 with the Subject **using keys bound to the authentication process.**

3778 **Guidance:** Renewal is considered as an extension of usability, whereas re-issuance  
3779 requires a change.

3780 *ALA\_CM\_RNR#040 Authentication key life*

3781 **Expire after 24 hours all temporary or short-term keys derived during the**  
3782 **authentication process.**

3783 *ALA\_CM\_RNR#050 Record Retention*

3784 Retain, securely, the record of any renewal/re-issuance process for the duration of the  
3785 Subscriber's account plus a further period sufficient to allow fulfillment of any period  
3786 required legally, contractually or by any other form of binding agreement or obligation, or  
3787 submit same record to a client CSP that has undertaken to retain the record for the  
3788 requisite period or longer.

## 3789 **5.4.4 Part D - Credential Revocation**

3790 These criteria deal with credential revocation and the determination of the legitimacy of a  
3791 revocation request.

### 3792 **5.4.4.1 Revocation Procedures**

3793 These criteria address general revocation functions, such as the processes involved and  
3794 the basic requirements for publication.

3795 An enterprise and its specified service must:

3796 *ALA\_CM\_RVP#010 Revocation procedures*

3797 a) State the conditions under which revocation of an issued certificate may occur;

3798 b) State the processes by which a revocation request may be submitted;

3799 c) State the persons and organizations from which a revocation request will be  
3800 accepted;

3801 d) State the validation steps that will be applied to ensure the validity (identity) of  
3802 the Revocant, and;

3803 e) State the response time between a revocation request being accepted and the  
3804 publication of revised certificate status.

3805 *ALA\_CM\_RVP#020 Secure status notification*

3806 Ensure that published credential status notification information can be relied upon in  
3807 terms of the enterprise of its origin (i.e., its authenticity) and its correctness (i.e., its  
3808 integrity).

3809 *ALA\_CM\_RVP#030 Revocation publication*

3810 Ensure that published credential status notification is revised within **18** hours of the  
3811 receipt of a valid revocation request, such that any subsequent attempts to use that  
3812 credential in an authentication shall be unsuccessful. The nature of the revocation  
3813 mechanism shall be in accordance with the technologies supported by the service.

3814 *ALA\_CM\_RVP#040 Verify Revocation Identity*

3815 Establish that the identity for which a revocation request is received is one that was  
3816 issued by the specified service.

3817 *ALA\_CM\_RVP#050 Revocation Records*

3818 Retain a record of any revocation of a credential that is related to a specific identity  
3819 previously verified, solely in connection to the stated credential. At a minimum, records  
3820 of revocation must include:

3821 a) the Revocant's full name;

3822 b) the Revocant's authority to revoke (e.g., Subscriber or Subject themselves,  
3823 someone acting with the Subscriber's or Subject's power of attorney, the  
3824 credential issuer, law enforcement, or other legal due process);

3825 c) the Credential Issuer's identity (if not directly responsible for the identity  
3826 proofing service); [Omitted]

3827 d) the reason for revocation.

3828 *ALA\_CM\_RVP#060 Record Retention*

3829 Retain, securely, the record of the revocation process for a period which is the maximum  
3830 of:

3831 a) the records retention policy required by **AL4\_CM\_CPP#020**;

3832 b) applicable legislation, regulation, contract or standards.

#### 3833 **5.4.4.2 Verify Revocant's Identity**

3834 Revocation of a credential requires that the requestor and the nature of the request be  
3835 verified as rigorously as the original identity proofing. The enterprise should not act on a  
3836 request for revocation without first establishing the validity of the request (if it does not,  
3837 itself, determine the need for revocation).

3838 In order to do so, the enterprise and its specified service must:

3839 *AL4\_CM\_RVR#010 Verify revocation identity*

3840 Establish that the credential for which a revocation request is received is one that was  
3841 initially issued by the specified service, applying the same process and criteria as would  
3842 apply to an original identity proofing.

3843 *AL4\_CM\_RVR#020 Revocation reason*

3844 Establish the reason for the revocation request as being sound and well founded, in  
3845 combination with verification of the Revocant, according to AL4\_CM\_RVR#030,  
3846 AL4\_CM\_RVR#040, or AL4\_CM\_RVR#050.

3847 *AL4\_CM\_RVR#030 Verify Subscriber as Revocant*

3848 Where the Subscriber or Subject seeks revocation of the Subject's credential:

- 3849 a) if in person, require presentation of a primary Government Picture ID document  
3850 that shall be **[Omitted]** verified by a record check against the provided identity  
3851 with the specified issuing authority's records;  
3852 b) if remote:  
3853 i. verify a signature against records (if available), confirmed with a call to a  
3854 telephone number of record, or;  
3855 ii. as an electronic request, authenticate it as being from the same Subscriber  
3856 or Subject, supported by a **different** credential at **Assurance Level 4**.

3857 *AL4\_CM\_RVR#040 Verify CSP as Revocant*

3858 Where a CSP seeks revocation of a Subject's credential, establish that the request is  
3859 either:

- 3860 a) from the specified service itself, with authorization as determined by established  
3861 procedures, or;  
3862 b) from the client Credential Issuer, by authentication of a formalized request over  
3863 the established secure communications network.

3864 *AL4\_CM\_RVR#050 Verify Legal Representative as Revocant*

3865 Where the request for revocation is made by a law enforcement officer or presentation of  
3866 a legal document:

- 3867 a) if in-person, verify the identity of the person presenting the request, or;  
3868 b) if remote:  
3869 i. in paper/facsimile form, verify the origin of the legal document by a  
3870 database check or by telephone with the issuing authority;  
3871 ii. as an electronic request, authenticate it as being from a recognized legal  
3872 office, supported by a different credential at **Assurance Level 4**.

#### 3873 **5.4.4.3 Re-keying a credential**

3874 Re-keying of a credential requires that the requestor be verified as the Subject with as  
3875 much rigor as was applied to the original identity proofing. The enterprise should not act

3876 on a request for re-key without first establishing that the requestor is identical to the  
3877 Subject.

3878 In order to do so, the enterprise and its specified service must:

3879 *ALA\_CM\_RKY#010 Verify Requestor as Subscriber*

3880 **Where the Subject seeks a re-key for the Subject's own credential:**

- 3881 a) **if in-person, require presentation of a primary Government Picture ID**  
3882 **document that shall be verified by a record check against the provided**  
3883 **identity with the specified issuing authority's records;**  
3884 b) **if remote:**  
3885 i. **verify a signature against records (if available), confirmed with a call**  
3886 **to a telephone number of record, or;**  
3887 ii. **authenticate an electronic request as being from the same Subject,**  
3888 **supported by a different credential at Assurance Level 4.**

3889 *ALA\_CM\_RKY#020 Re-key requests other than Subject*

3890 **Re-key requests from any parties other than the Subject must not be accepted.**

#### 3891 **5.4.4.4 Secure Revocation/Re-key Request**

3892 This criterion applies when revocation **or re-key** requests must be communicated  
3893 between remote components of the service organization.

3894 The enterprise and its specified service must:

3895 *ALA\_CM\_SRR#010 Submit Request*

3896 Submit a request for the revocation to the Credential Issuer service (function), using a  
3897 secured network communication.

#### 3898 **5.4.5 Part E - Credential Status Management**

3899 These criteria deal with credential status management, such as the receipt of requests for  
3900 new status information arising from a new credential being issued or a revocation or other  
3901 change to the credential that requires notification. They also deal with the provision of  
3902 status information to requesting parties (Verifiers, Relying Parties, courts and others  
3903 having regulatory authority, etc.) having the right to access such information.

##### 3904 **5.4.5.1 Status Maintenance**

3905 An enterprise and its specified service must:

3906 *ALA\_CM\_CSM#010 Maintain Status Record*

3907 Maintain a record of the status of all credentials issued.

3908 *ALA\_CM\_CSM#020 Validation of Status Change Requests*



3909 Authenticate all requestors seeking to have a change of status recorded and published and  
3910 validate the requested change before considering processing the request. Such validation  
3911 should include:

- 3912 a) the requesting source as one from which the specified service expects to receive  
3913 such requests;
- 3914 b) if the request is not for a new status, the credential or identity as being one for  
3915 which a status is already held.

3916 *ALA\_CM\_CSM#030 Revision to Published Status*

3917 Process authenticated requests for revised status information and have the revised  
3918 information available for access within a period of 72 hours.

3919 *ALA\_CM\_CSM#040 Status Information Availability*

3920 Provide, with 99% availability, a secure automated mechanism to allow relying parties to  
3921 determine credential status and authenticate the Claimant's identity.

3922 *ALA\_CM\_CSM#050 Inactive Credentials*

3923 Disable any credential that has not been successfully used for authentication during a  
3924 period of 18 months.

3925

## 3926 **5.4.6 Part F - Credential Verification/Authentication**

3927 These criteria apply to credential validation and identity authentication.

### 3928 **5.4.6.1 Assertion Security**

3929 An enterprise and its specified service must:

3930 *ALA\_CM\_ASS#010 Validation and Assertion Security*

3931 Provide validation of credentials to a Relying Party using a protocol that:

- 3932 a) requires authentication of the specified service, itself, or of the validation source;
- 3933 b) ensures the integrity of the authentication assertion;
- 3934 c) protects assertions against manufacture, modification, substitution and disclosure,  
3935 and secondary authenticators from manufacture, capture and replay;
- 3936 d) uses approved **strong** cryptography techniques;

3937 and which, specifically:

- 3938 e) creates assertions which are specific to a single transaction;
- 3939 f) where assertion references are used, generates a new reference whenever a new  
3940 assertion is created;
- 3941 g) when an assertion is provided indirectly, either signs the assertion or sends it via a  
3942 protected channel, using a strong binding mechanism between the secondary  
3943 authenticator and the referenced assertion;

- 3944 h) send assertions either via a channel mutually-authenticated with the Relying  
3945 Party, or signed and encrypted for the Relying Party;  
3946 i) requires the secondary authenticator to:  
3947 i) be signed when provided directly to Relying Party, or;  
3948 ii) have a minimum of 64 bits of entropy when provision is indirect (i.e.  
3949 through the credential user);  
3950 iii) be transmitted to the Subject through a protected channel which is linked  
3951 to the primary authentication process in such a way that session hijacking  
3952 attacks are resisted;  
3953 iv) not be subsequently transmitted over an unprotected channel or to an  
3954 unauthenticated party while it remains valid.

3955 *ALA\_CM\_ASS#015 No False Authentication*

3956 Employ techniques which ensure that system failures do not result in 'false positive  
3957 authentication' errors.

3958 *ALA\_CM\_ASS#018 Ensure token validity*

3959 Ensure that tokens are either still valid or have been issued within the last 24 hours.

3960 **Guidance:** The 24-hour period allows for the fact that if a freshly-issued credential is  
3961 then revoked, notice of the revocation may take 24 hours to be publicised (per  
3962 AL3\_CM\_RVP#030)..

3963 *ALA\_CM\_ASS#020 Post Authentication*

3964 *Not* authenticate credentials that have been revoked unless the time of the transaction for  
3965 which verification is sought precedes the time of revocation of the credential.

3966 **Guidance:** The purpose in this criterion is that, if a verification is intended to refer to the  
3967 status of a credential at a specific historical point in time, e.g. to determine whether the  
3968 Claimant was entitled to act as a signatory in a specific capacity at the time of the  
3969 transaction, this may be done. It is implicit in this thinking that both the request and the  
3970 response indicate the historical nature of the query and response; otherwise the default  
3971 time is 'now'. If no such service is offered then this criterion may simply be  
3972 'Inapplicable', for that reason.

3973 *ALA\_CM\_ASS#030 Proof of Possession*

3974 Use an authentication protocol that requires the claimant to prove possession and control  
3975 of the authentication token.

3976 *ALA\_CM\_ASS#035 No stipulation*

3977 *ALA\_CM\_ASS#040 Assertion Life-time*

3978 **[Omitted]** Notify the relying party of how often the revocation status sources are  
3979 updated.

3980 **5.4.6.2 Authenticator-generated challenges**

3981 An enterprise and its specified service must:

3982 *ALA\_CM\_AGC#010 Entropy level*

3983 Create authentication secrets to be used during the authentication exchange (i.e. with out-  
3984 of-band or cryptographic device tokens) with a degree of entropy appropriate to the token  
3985 type in question.

3986 *ALA\_CM\_AGC#020 Limit password validity*

3987 **Employ one-time passwords which expire within two minutes.**

3988 **5.4.6.3 Multi-factor authentication**

3989 An enterprise and its specified service must:

3990 *ALA\_CM\_MFA#010 Permitted multi-factor tokens*

3991 Require two tokens which, when used in combination within a single authentication  
3992 exchange, are acknowledged as providing an equivalence of AL4, as determined by a  
3993 recognized national technical authority.

3994 **5.4.6.4 Verifier's assertion schema**

3995 Note: Since assertions and related schema can be complex and may be modeled directly  
3996 on the needs and preferences of the participants, the details of such schema fall outside  
3997 the scope of the SAC's herein, which are expressed observing, insofar as is feasible, a  
3998 technology-agnostic policy. The following criteria, therefore, are perhaps more open to  
3999 variable conformity through their final implementation than are others in this document.

4000 These criteria are derived directly from NIST SP 800-63-2 and have been expressed in as  
4001 generic a manner as they can be.

4002 An enterprise and its specified service must:

4003 *ALA\_CM\_VAS#010 Approved cryptography*

4004 Apply assertion protocols which use cryptographic techniques approved by a national  
4005 authority or other generally-recognized authoritative body.

4006 *ALA\_CM\_VAS#020 No browser/bearer assertions*

4007 **Not issue browser / bearer assertions.**

4008 *ALA\_CM\_VAS#030 Assertion assurance level*

4009 Create assertions which, either explicitly or implicitly (using a mutually-agreed  
4010 mechanism), indicate the assurance level at which the initial authentication of the Subject  
4011 was made.

4012 *ALA\_CM\_VAS#040 No pseudonyms*

- 4013 Create assertions which indicate only verified Subscriber names in the credential subject  
4014 to verification.
- 4015 *ALA\_CM\_VAS#050 Specify recipient*  
4016 Create assertions which identify the intended recipient of the verification such that the  
4017 recipient may validate that it is intended for them.
- 4018 *ALA\_CM\_VAS#060 No assertion manufacture/modification*  
4019 Ensure that it is impractical to manufacture an assertion or assertion reference by Signing  
4020 the assertion and using at least one of the following techniques:
- 4021 a) [Omitted];  
4022 b) Encrypting the assertion using a secret key shared with the RP;  
4023 c) Creating an assertion reference which has a minimum of 64 bits of entropy;  
4024 d) Sending the assertion over a protected channel during a mutually-authenticated  
4025 session.
- 4026 *ALA\_CM\_VAS#070 Assertion protections*  
4027 Provide protection of assertion-related data such that:
- 4028 a) both assertions and assertion references are protected against capture and re-use;  
4029 b) assertions are also protected against redirection  
4030 c) assertions, assertion references and session cookies used for authentication  
4031 purposes, including any which are re-directed, are protected against session  
4032 hijacking, for at least the duration of their validity (see AL1\_CM\_VAS#110).
- 4033 *ALA\_CM\_VAS#080 Single-use assertions*  
4034 Limit to a single transaction the use of assertions which do not support proof of  
4035 ownership.
- 4036 *ALA\_CM\_VAS#090 Single-use assertion references*  
4037 Limit to a single transaction the use of assertion references.
- 4038 *ALA\_CM\_VAS#100 Bind reference to assertion*  
4039 Provide a strong binding between the assertion reference and the corresponding assertion,  
4040 based on integrity-protected (or signed) communications over which the Verifier has been  
4041 authenticated.
- 4042 *ALA\_CM\_VAS#110 No stipulation*  
4043 No stipulation.  
4044

4045 **5.5 Compliance Tables**

4046 Use the following tables to correlate criteria for a particular Assurance Level (AL) and  
4047 the evidence offered to support compliance.

4048 Service providers preparing for an assessment can use the table appropriate to the AL at  
4049 which they are seeking approval to correlate evidence with criteria or to justify non-  
4050 applicability (e.g., "specific service types not offered").

4051 Assessors can use the tables to record the steps in their assessment and their  
4052 determination of compliance or failure.

4053 These tables also provide an overview of any revisions made to criteria in comparison to  
4054 v3.0 of this document (see §1.1).

4055 **Table 3-5. OP-SAC - AL1 Compliance**

Clause	Description	Compliance
Part A – Credential Operating Environment		
AL1_CM_CTR#010	Withdrawn	No conformity requirement
AL1_CM_CTR#020	<a href="#">Protocol threat risk assessment and controls</a>	<i>Amended; Guidance</i>
AL1_CM_CTR#025	No stipulation	No conformity requirement
AL1_CM_CTR#028	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	Withdrawn	No conformity requirement
AL1_CM_IDP#020	Withdrawn	No conformity requirement
AL1_CM_IDP#030	Withdrawn	No conformity requirement
AL1_ID_POL#010	<a href="#">Unique service identity</a>	
AL1_ID_POL#020	<a href="#">Unique Subject identity</a>	
AL1_ID_IDV#000	<a href="#">Identity Proofing classes</a>	<i>New</i>
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_IDC#010	<a href="#">Authenticate Original Credential</a>	<i>New</i>

AL1_ID_SCV#010	<a href="#">Secondary checks</a>	
AL1_ID_VRC#010	No stipulation	No conformity requirement
AL1_ID_VRC#020	No stipulation	No conformity requirement
AL1_ID_VRC#025	<a href="#">Provide Subject Identity Records</a>	<i>New</i>
AL1_ID_VRC#030	No stipulation	No conformity requirement
AL1_CM_IDP#010	<a href="#">Revision to Subscriber Information</a>	<i>Amended; Guidance ; Re-numbered – was 'IDP#040</i>
AL1_CM_IDP#020	<a href="#">Authenticate Subject Information Changes</a>	<i>New</i>
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>	
AL1_CM_CRN#035	<a href="#">Convey credential</a>	<i>New</i>
AL1_CM_CRN#040	<a href="#">Token strength</a>	<i>New</i>
<b>Part C – Credential Renewal and Re-issuing</b>		
AL1_CM_RNR#010	<a href="#">Changeable PIN/Password</a>	
<b>Part D – Credential Revocation</b>		
AL1_CM_SRR#010	<a href="#">Submit Request</a>	
<b>Part E – Credential Status Management</b>		
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>	
<b>Part F – Credential Validation / Authentication</b>		
AL1_CM_ASS#010	<a href="#">Validation and Assertion Security</a>	
AL1_CM_ASS#015	No stipulation	No conformity requirement
AL1_CM_ASS#018	No stipulation	No conformity requirement
AL1_CM_ASS#020	<a href="#">No Post Authentication</a>	<i>Editorial</i>
AL1_CM_ASS#030	<a href="#">Proof of Possession</a>	
AL1_CM_ASS#035	<a href="#">Limit authentication attempts</a>	<i>New</i>
AL1_CM_ASS#040	<a href="#">Assertion Lifetime</a>	<i>Amended</i>
AL1_CM_VAS#010	No stipulation	No conformity requirement <i>New</i>
AL1_CM_VAS#020	No stipulation	No conformity requirement <i>New</i>
AL1_CM_VAS#030	<a href="#">Assertion assurance level</a>	<i>New</i>
AL1_CM_VAS#040	No stipulation	No conformity requirement <i>New</i>
AL1_CM_VAS#050	No stipulation	No conformity requirement <i>New</i>

---

AL1_CM_VAS#060	<a href="#">No assertion manufacture/modification</a>	<i>New</i>
AL1_CM_VAS#070	No stipulation	No conformity requirement <i>New</i>
AL1_CM_VAS#080	<a href="#">Single-use assertions</a>	<i>New</i>
AL1_CM_VAS#090	<a href="#">Single-use assertion references</a>	<i>New</i>
AL1_CM_VAS#100	<a href="#">Bind reference to assertion</a>	<i>New</i>

4056

4057



4058

**Table 3-6. OP-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>	<i>Amended; Guidance</i>
AL2_CM_CTR#025	<a href="#">Authentication protocols</a>	<i>Amended; Guidance</i>
AL2_CM_CTR#028	<a href="#">One-time passwords</a>	<i>Amended</i>
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	Withdrawn	No conformity requirement
AL2_CM_IDP#020	Withdrawn	No conformity requirement
AL2_CM_IDP#030	Withdrawn	No conformity requirement
AL2_ID_POL#010	<a href="#">Unique service identity</a>	
AL2_ID_POL#020	<a href="#">Unique Subject identity</a>	<i>Guidance</i>
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>	<i>Amended</i>
AL2_ID_IDV#010	<a href="#">Identity Verification Measures</a>	<i>New</i>
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>	<i>Amended</i>
AL2_ID_RPV#020	<a href="#">Evidence checks</a>	<i>Amended</i>
AL2_ID_CRV#010	<a href="#">Required evidence</a>	
AL2_ID_CRV#020	<a href="#">Evidence checks</a>	<i>Amended</i>
AL2_ID_AJV#000	<a href="#">Meet preceding criteria</a>	
AL2_ID_AJV#010	<a href="#">Required evidence</a>	
AL2_ID_AJV#020	<a href="#">Evidence checks</a>	
AL2_ID_IDC#010	<a href="#">Authenticate Original Credential</a>	<i>New</i>

AL2_ID_IDC#020	<a href="#">Record Original Credential</a>	<i>New</i>
AL2_ID_IDC#030	<a href="#">Issue Derived Credential</a>	<i>New</i>
AL2_ID_SCV#010	<a href="#">Secondary checks</a>	<i>Amended</i>
AL2_ID_VRC#010	<a href="#">Verification Records for Personal Applicants</a>	<i>Amended</i>
AL2_ID_VRC#020	<a href="#">Verification Records for Affiliated Applicants</a>	<i>Amended</i>
AL2_ID_VRC#025	<a href="#">Provide Subject identity records</a>	<i>New</i>
AL2_ID_VRC#030	<a href="#">Record Retention</a>	
AL2_CM_IDP#010	<a href="#">Revision to Subscriber information</a>	<i>Amended; Guidance ; Re-numbered – was 'IDP#040</i>
AL2_CM_IDP#020	<a href="#">Authenticate Subject Information Changes</a>	<i>New</i>
AL2_CM_CRN#010	<a href="#">Authenticated Request</a>	
AL2_CM_CRN#020	<a href="#">Unique identity</a>	<i>Guidance</i>
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>	<i>Amended</i>
AL2_CM_CRN#050	<a href="#">One-time password strength</a>	
AL2_CM_CRN#055	<a href="#">One-time password lifetime</a>	<i>Amended</i>
AL2_CM_CRN#060	<a href="#">Software cryptographic token strength</a>	<i>Amended</i>
AL2_CM_CRN#070	<a href="#">Hardware token strength</a>	<i>Amended</i>
AL2_CM_CRN#075	No stipulation	No conformity requirement
AL2_CM_CRN#080	No stipulation	No conformity requirement
AL2_CM_CRN#090	<a href="#">Nature of Subject</a>	
AL2_CM_CRN#095	<a href="#">Pseudonym's Real Identity</a>	<i>New</i>
AL2_CM_CRD#010	<a href="#">Notify Subject of Credential Issuance</a>	<i>Guidance</i>
AL2_CM_CRD#015	<a href="#">Confirm Applicant's identity (in person)</a>	<i>Amended</i>
AL2_CM_CRD#016	<a href="#">Confirm Applicant's identity (remotely)</a>	
<b>Part C – Credential Renewal and Re-issuing</b>		
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>	<i>Amended</i>
AL2_CM_RNR#040	No stipulation	No conformity requirement
AL2_CM_RNR#050	<a href="#">Record Retention</a>	<i>New</i>
<b>Part D – Credential Revocation</b>		

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#045	<a href="#">Notification of Revoked Credential</a>	<i>New</i>
AL2_CM_RVP#050	<a href="#">Revocation Records</a>	
AL2_CM_RVP#060	<a href="#">Record Retention</a>	<i>Amended</i>
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>	
<b>Part E – Credential Status Management</b>		
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>	
<b>Part F – Credential Validation / Authentication</b>		
AL2_CM_ASS#010	<a href="#">Validation and Assertion Security</a>	
AL2_CM_ASS#013	No stipulation	
AL2_CM_ASS#015	<a href="#">No False Authentication</a>	
AL2_CM_ASS#018	No stipulation	<i>New</i>
AL2_CM_ASS#020	<a href="#">No Post Authentication</a>	<i>Editorial; Guidance</i>
AL2_CM_ASS#030	<a href="#">Proof of Possession</a>	
AL2_CM_ASS#035	<a href="#">Limit authentication attempts</a>	<i>New</i>
AL2_CM_ASS#040	<a href="#">Assertion Lifetime</a>	<i>Amended</i>
AL2_CM_AGC#010	<a href="#">Entropy level</a>	<i>New</i>
AL2_CM_MFA#010	<a href="#">Permitted multi-factor tokens</a>	<i>New</i>
AL2_CM_VAS#010	<a href="#">Approved cryptography</a>	<i>New</i>
AL2_CM_VAS#020	No stipulation	No conformity requirement <i>New</i>
AL2_CM_VAS#030	<a href="#">Assertion assurance level</a>	<i>New</i>
AL2_CM_VAS#040	<a href="#">Notify pseudonyms</a>	<i>New</i>
AL2_CM_VAS#050	<a href="#">Specify recipient</a>	<i>New</i>

---

AL2_CM_VAS#060	<a href="#">No assertion manufacture/modification</a>	<i>New</i>
AL2_CM_VAS#070	<a href="#">Assertion protections</a>	<i>New</i>
AL2_CM_VAS#080	<a href="#">Single-use assertions</a>	<i>New</i>
AL2_CM_VAS#090	<a href="#">Single-use assertion references</a>	<i>New</i>
AL2_CM_VAS#100	<a href="#">Bind reference to assertion</a>	<i>New</i>

4059

4060

4061

**Table 3-7. OP-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	Withdrawn	No conformity requirement
AL3_CM_CTR#020	<a href="#">Protocol threat risk assessment and controls</a>	<i>Amended; Guidance</i>
AL3_CM_CTR#025	<a href="#">Permitted authentication protocols</a>	<i>Amended</i>
AL3_CM_CTR#028	No stipulation	No conformity requirement
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_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_IDV#010	<a href="#">Identity Verification Measures</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>	<i>Amended</i>
AL3_ID_RPV#020	<a href="#">Evidence checks</a>	<i>Amended</i>
AL3_ID_CRV#010	<a href="#">Required evidence</a>	<i>New</i>
AL3_ID_CRV#020	<a href="#">Evidence checks</a>	<i>New</i>
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_IDC#010	<a href="#">Authenticate Original Credential</a>	<i>New</i>
AL3_ID_IDC#020	<a href="#">Record Original Credential</a>	<i>New</i>

AL3_ID_IDC#030	<a href="#">Issue Derived Credential</a>	<i>New</i>
AL3_ID_SCV#010	<a href="#">Secondary checks</a>	<i>Amended</i>
AL3_ID_VRC#010	<a href="#">Verification Records for Personal Applicants</a>	<i>Amended</i>
AL3_ID_VRC#020	<a href="#">Verification Records for Affiliated Applicants</a>	<i>Amended; Guidance</i>
AL3_ID_VRC#025	<a href="#">Provide Subject Identity Records</a>	<i>New</i>
AL3_ID_VRC#030	<a href="#">Record Retention</a>	
AL3_CM_IDP#010	<a href="#">Revision to Subscriber information</a>	<i>Amended; Guidance ; Re-numbered – was 'IDP#040</i>
AL3_CM_IDP#020	<a href="#">Authenticate Subject Information Changes</a>	<i>New</i>
AL3_CM_CRN#010	<a href="#">Authenticated Request</a>	
AL3_CM_CRN#020	<a href="#">Unique identity</a>	<i>Guidance</i>
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>	<i>Editorial</i>
AL3_CM_CRN#050	<a href="#">One-time password strength</a>	
AL3_CM_CRN#055	No stipulation	No conformity requirement
AL3_CM_CRN#060	<a href="#">Software cryptographic token strength</a>	<i>Amended</i>
AL3_CM_CRN#070	<a href="#">Hardware token strength</a>	<i>Amended</i>
AL3_CM_CRN#075	No stipulation	No conformity requirement
AL3_CM_CRN#080	<a href="#">Binding of key</a>	
AL3_CM_CRN#090	<a href="#">Nature of Subject</a>	
AL3_CM_CRN#095	No stipulation	No conformity requirement
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>	<i>Guidance</i>
AL3_CM_CRD#015	<a href="#">Confirm Applicant's identity (in person)</a>	<i>New</i>
AL3_CM_CRD#016	<a href="#">Confirm Applicant's identity (remotely)</a>	<i>New</i>
AL3_CM_CRD#017	<a href="#">Protected Issuance of Permanent Secrets (in person)</a>	<i>New</i>
AL3_CM_CRD#018	<a href="#">Protected Issuance of Permanent Secrets (remotely)</a>	<i>New</i>
AL3_CM_CRD#020	<a href="#">Subject's acknowledgement</a>	
<b>Part C – Credential Renewal and Re-issuing</b>		
AL3_CM_RNR#010	<a href="#">Changeable PIN/Password</a>	

AL3_CM_RNR#020	<a href="#">Proof-of-possession on Renewal/Re-issuance</a>	<i>New</i>
AL3_CM_RNR#030	<a href="#">Renewal/Re-issuance limitations</a>	<i>New</i>
AL3_CM_RNR#040	No stipulation	No conformity requirement
AL3_CM_RNR#050	<a href="#">Record Retention</a>	<i>New</i>
<b>Part D – Credential Revocation</b>		
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>	<i>Amended</i>
AL3_CM_RVP#060	<a href="#">Record Retention</a>	<i>Amended</i>
AL3_CM_RVR#010	<a href="#">Verify revocation identity</a>	<i>Amended</i>
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>	
<b>Part E – Credential Status Management</b>		
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>	
<b>Part F – Credential Validation / Authentication</b>		
AL3_CM_ASS#010	<a href="#">Validation and Assertion Security</a>	<i>Amended</i>
AL3_CM_ASS#015	<a href="#">No False Authentication</a>	
AL3_CM_ASS#018	<a href="#">Ensure token validity</a>	<i>New</i>
AL3_CM_ASS#020	<a href="#">Post Authentication</a>	<i>Guidance</i>
AL3_CM_ASS#030	<a href="#">Proof of Possession</a>	<i>New</i>
AL3_CM_ASS#035	<a href="#">Limit authentication attempts</a>	<i>New</i>
AL3_CM_ASS#040	<a href="#">Assertion Lifetime</a>	
AL3_CM_AGC#010	<a href="#">Entropy level</a>	<i>New</i>
AL3_CM_MFA#010	<a href="#">Permitted multi-factor tokens</a>	<i>New</i>
AL3_CM_VAS#010	<a href="#">Approved cryptography</a>	<i>New</i>
AL3_CM_VAS#020	No stipulation	No conformity requirement



---

AL3_CM_VAS#030	<a href="#">Assertion assurance level</a>	<i>New</i>
AL3_CM_VAS#040	<a href="#">Notify pseudonyms</a>	<i>New</i>
AL3_CM_VAS#050	<a href="#">Specify recipient</a>	<i>New</i>
AL3_CM_VAS#060	<a href="#">No assertion manufacture/modification</a>	<i>New</i>
AL3_CM_VAS#070	<a href="#">Assertion protections</a>	<i>New</i>
AL3_CM_VAS#080	<a href="#">Single-use assertions</a>	<i>New</i>
AL3_CM_VAS#090	<a href="#">Single-use assertion references</a>	<i>New</i>
AL3_CM_VAS#100	<a href="#">Bind reference to assertion</a>	<i>New</i>
AL3_CM_VAS#110	<a href="#">SSO provisions</a>	<i>New</i>

4062

4063

4064

**Table 3-8. OP-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_CPP#040	<a href="#">Discretionary Access Control</a>	<i>New</i>
AL4_CM_CTR#010	Withdrawn	No conformity requirement
AL4_CM_CTR#020	<a href="#">Protocol threat risk assessment and controls</a>	<i>Amended; Guidance</i>
AL4_CM_CTR#025	No stipulation	No conformity requirement
AL4_CM_CTR#028	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	Withdrawn	No conformity requirement <i>Re-numbered as AL4_CO_SCO#020 &amp; AL4_CM_CPP#040</i>
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_ID_POL#010	<a href="#">Unique service identity</a>	
AL4_ID_POL#020	<a href="#">Unique Subject identity</a>	<i>Guidance</i>
AL4_ID_POL#030	<a href="#">Published Proofing Policy</a>	
AL4_ID_POL#040	<a href="#">Adherence to Proofing Policy</a>	<i>Editorial</i>
AL4_ID_IDV#000	<a href="#">Identity Proofing classes</a>	
AL4_ID_IDV#010	<a href="#">Identity Verification Measures</a>	<i>New</i>
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_AJV#000	<a href="#">Meet preceding criteria</a>	
AL4_ID_AJV#010	<a href="#">Required evidence</a>	
AL4_ID_AJV#020	<a href="#">Evidence checks</a>	

AL4_ID_IDC#010	<a href="#">Authenticate Original Credential</a>	<i>New</i>
AL4_ID_IDC#020	<a href="#">Record Original Credential</a>	<i>New</i>
AL4_ID_IDC#030	<a href="#">Issue Derived Credential</a>	<i>New</i>
AL4_ID_SCV#010	<a href="#">Secondary checks</a>	
AL4_ID_VRC#010	<a href="#">Verification Records for Personal Applicants</a>	<i>Amended</i>
AL4_ID_VRC#020	<a href="#">Verification Records for Affiliated Applicants</a>	<i>Amended; Guidance</i>
AL4_ID_VRC#025	<a href="#">Provide Subject identity records</a>	<i>New</i>
AL4_ID_VRC#030	<a href="#">Record Retention</a>	
AL4_CM_IDP#010	<a href="#">Revision to Subscriber information</a>	<i>Amended; Guidance ; Re-numbered – was 'IDP#040</i>
AL4_CM_IDP#020	No stipulation	No conformity requirement
AL4_CM_CRN#010	<a href="#">Authenticated Request</a>	
AL4_CM_CRN#020	<a href="#">Unique identity</a>	<i>Guidance</i>
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>	<i>Editorial</i>
AL4_CM_CRN#050	<a href="#">One-time password strength</a>	
AL4_CM_CRN#055	No stipulation	No conformity requirement
AL4_CM_CRN#060	<a href="#">Software cryptographic token strength</a>	
AL4_CM_CRN#070	<a href="#">Hardware token strength</a>	<i>New</i>
AL4_CM_CRN#075	<a href="#">Multi-factor hardware cryptographic token strength</a>	<i>Amended</i>
AL4_CM_CRN#080	<a href="#">Binding of key</a>	
AL4_CM_CRN#090	<a href="#">Nature of Subject</a>	
AL4_CM_CRN#095	No stipulation	No conformity requirement
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>	<i>Guidance</i>
AL4_CM_CRD#015	<a href="#">Confirm Applicant's identity (in person)</a>	<i>New</i>
AL4_CM_CRD#016	No stipulation	No conformity requirement
AL4_CM_CRD#017	<a href="#">Protected Issuance of Permanent Secrets (in person)</a>	<i>New</i>
AL4_CM_CRD#018	No stipulation	No conformity requirement
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>	
AL4_CM_RNR#020	<a href="#">Proof-of-possession on Renewal/Re-issuance</a>	<i>New</i>
AL4_CM_RNR#030	<a href="#">Renewal/Re-issuance limitations</a>	<i>New</i>
AL4_CM_RNR#040	<a href="#">Authentication key life</a>	<i>New</i>
AL4_CM_RNR#050	<a href="#">Record Retention</a>	<i>New</i>
<b>Part D – Credential Revocation</b>		
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	<a href="#">Verify Revocation Identity</a>	<i>New</i>
AL4_CM_RVP#050	<a href="#">Revocation Records</a>	<i>Amended</i>
AL4_CM_RVP#060	<a href="#">Record Retention</a>	<i>Amended</i>
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 Subject</a>	
AL4_CM_SRR#010	<a href="#">Submit Request</a>	
<b>Part E – Credential Status Management</b>		
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>	
<b>Part F – Credential Validation / Authentication</b>		
AL4_CM_ASS#010	<a href="#">Validation and Assertion Security</a>	<i>Amended</i>
AL4_CM_ASS#015	<a href="#">No False Authentication</a>	
AL3_CM_ASS#018	<a href="#">Ensure token validity</a>	<i>New</i>
AL4_CM_ASS#020	<a href="#">Post Authentication</a>	<i>Guidance</i>
AL4_CM_ASS#030	<a href="#">Proof of Possession</a>	
AL3_CM_ASS#035	No stipulation	No conformity requirement
AL4_CM_ASS#040	<a href="#">Assertion Lifetime</a>	
AL4_CM_AGC#010	<a href="#">Entropy level</a>	<i>New</i>

AL4_CM_AGC#020	<a href="#">Limit password validity</a>	<i>New</i>
AL4_CM_MFA#010	<a href="#">Permitted multi-factor tokens</a>	<i>New</i>
AL4_CM_VAS#010	<a href="#">Approved cryptography</a>	<i>New</i>
AL4_CM_VAS#020	<a href="#">No browser/bearer assertions</a>	<i>New</i>
AL4_CM_VAS#030	<a href="#">Assertion assurance level</a>	<i>New</i>
AL4_CM_VAS#040	<a href="#">Notify pseudonyms</a>	<i>New</i>
AL4_CM_VAS#050	<a href="#">Specify recipient</a>	<i>New</i>
AL4_CM_VAS#060	<a href="#">No assertion manufacture/modification</a>	<i>New</i>
AL4_CM_VAS#070	<a href="#">Assertion protections</a>	<i>New</i>
AL4_CM_VAS#080	<a href="#">Single-use assertions</a>	<i>New</i>
AL4_CM_VAS#090	<a href="#">Single-use assertion references</a>	<i>New</i>
AL4_CM_VAS#100	<a href="#">Bind reference to assertion</a>	<i>New</i>
AL4_CM_VAS#110	No stipulation	No conformity requirement

## 4065 **6 REFERENCES**

---

4066

4067 [CAF] Louden, Chris, Spencer, Judy; Burr, Bill; Hawkins, Kevin; Temoshok, David;  
4068 Cornell, John; Wilsher, Richard G.; Timchak, Steve; Sill, Stephen; Silver, Dave; Harrison,  
4069 Von; eds., "E-Authentication Credential Assessment Framework (CAF)," E-  
4070 Authentication Initiative, Version 2.0.0 (March 16, 2005).  
4071 <http://www.cio.gov/eauthentication/documents/CAF.pdf>

4072

4073 [EAP CSAC 04011] "EAP working paper: Identity Proofing Service Assessment Criteria  
4074 (ID-SAC)," Electronic Authentication Partnership, Draft 0.1.3 (July 20, 2004)  
4075 [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)

4076

4077 [EAPTrustFramework] "Electronic Authentication Partnership Trust Framework"  
4078 Electronic Authentication Partnership, Version 1.0. (January 6, 2005)  
4079 [http://eap.projectliberty.org/docs/Trust\\_Framework\\_010605\\_final.pdf](http://eap.projectliberty.org/docs/Trust_Framework_010605_final.pdf)

4080

4081 [FIPS140-2] "Security Requirements for Cryptographic Modules" Federal Information  
4082 Processing Standards. (May 25, 2001) [http://csrc.nist.gov/publications/fips/fips140-](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)  
4083 [2/fips1402.pdf](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)

4084

4085 [IS27001] ISO/IEC 27001:2005 "Information technology - Security techniques -  
4086 Requirements for information security management systems" International Organization  
4087 for Standardization.  
4088 [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)

4089

4090 [M-04-04] Bolton, Joshua B., ed., "E-Authentication Guidance for Federal Agencies,"  
4091 Office of Management and Budget, (December 16, 2003).  
4092 <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>

4093

4094 [NIST800-63] Burr, William E.; Dodson, Donna F.; Polk, W. Timothy; eds., "Electronic  
4095 Authentication Guideline: : Recommendations of the National Institute of Standards and  
4096 Technology," Version 1.0.2, National Institute of Standards and Technology, (April,  
4097 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)

4098

4099 [RFC 3647] Chokhani, S.; Ford, W.; Sabett, R.; Merrill, C.; Wu, S.; eds., "Internet X.509  
4100 Public Key Infrastructure Certificate Policy and Certification Practices Framework," The  
4101 Internet Engineering Task Force (November, 2003). <http://www.ietf.org/rfc/rfc3647.txt>  
4102



4103

## 4104 **7 REVISION HISTORY**

---

- 4105 1. 2008-05-08 – Identity Assurance Framework Version 1.0 Initial Draft
- 4106 a. Released by Liberty Alliance
- 4107 b. Revision and scoping of Initial Draft release
- 4108 2. 2008-06-23 – Identity Assurance Framework Version 1.1 Final Draft
- 4109 a. Released by Liberty Alliance
- 4110 b. Inclusion of comments to Final Draft
- 4111 3. 2009-10-01 – Identity Assurance Framework Version 1.1 Final Draft
- 4112 a. Documents contributed to Kantara Initiative by Liberty Alliance
- 4113 4. 2010-04-dd – SAC Version 2.0
- 4114 a. Released by Kantara Initiative
- 4115 b. Significant scope build
- 4116 c. Original Identity Assurance Framework all inclusive document broken in
- 4117 to a set of documents with specific focus:
- 4118 i. Kantara IAF-1000-Overview
- 4119 ii. Kantara IAF-1100-Glossary
- 4120 iii. Kantara IAF-1200-Levels of Assurance
- 4121 iv. Kantara IAF-1300-Assurance Assessment Scheme
- 4122 v. Kantara IAF-1400-Service Assessment Criteria (this document)
- 4123 vi. Kantara IAF-1600-Assessor Qualifications and Requirements
- 4124 5. 2012-10-10 - SAC Version 3.0
- 4125 a. Revision to accommodate Full/Component Service Assessment and
- 4126 Approval.
- 4127 6. 2014-05-12 – SAC Version 4.0bis
- 4128 a. Revision to map SAC against NIST SP 800-63-2;
- 4129 b. Alignment to revised Glossary;
- 4130 c. Inclusion of reference to formal approving ballot (in *bis* release).
- 4131