



# Identity Assurance Framework: Service Assessment Criteria

**Version:** 3.1*bis* (Aligned to SP800-63-2)

This document is provided for 45-day public review, ending 2014-01-30.  
**The PDF version of this document shall be the reference version for any comments.**  
A MS Word version is provided as a convenience.  
Comments should be submitted using the *pro forma* comment form available [here](#).

**Date:** 2013-12-16  
**Editor:** Richard G. Wilsher  
Zygya LLC

## Contributors

The full list of contributors can be referenced here:

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

## 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 is comprised of a set of documents that includes an Overview publication, the *IAF Glossary*, a summary *Assurance Levels* document, and an *Assurance Assessment Scheme (AAS)*, which encompasses the associated assessment and certification program, as well as several subordinate documents, among them the *Service Assessment Criteria (SAC)*, which establishes baseline criteria for general organizational conformity, identity proofing services, credential strength, and credential management services against which all CSPs will be evaluated. The present document describes the Service Assessment Criteria component of the IAF, including setting out the Assurance Levels.

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

**Filename:** Kantara IAF-1400 SAC v4-0 (pending)

32

## Notice

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

39

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

51 Copyright: The content of this document is copyright of Kantara Initiative.  
52 © 2013 Kantara Initiative.

53

54

55		<b>Contents</b>	
56			
57	<b>1</b>	<b>INTRODUCTION.....</b>	<b>5</b>
58	1.1	Changes in this revision.....	5
59	<b>2</b>	<b>ASSURANCE LEVELS.....</b>	<b>7</b>
60	<b>3</b>	<b>SERVICE ASSESSMENT CRITERIA - GENERAL .....</b>	<b>8</b>
61	3.1	Context and Scope .....	8
62	3.2	Criteria Applicability .....	8
63	3.3	Status and Readership.....	9
64	3.4	Criteria Descriptions .....	9
65	3.5	Terminology.....	11
66	<b>4</b>	<b>COMMON ORGANIZATIONAL SERVICE ASSESSMENT CRITERIA .....</b>	<b>12</b>
67	4.1	Assurance Level 1.....	12
68	4.1.1	Enterprise and Service Maturity .....	12
69	4.1.2	Notices and User information .....	13
70	4.1.3	No stipulation.....	14
71	4.1.4	No stipulation.....	14
72	4.1.5	No stipulation.....	14
73	4.1.6	No stipulation.....	14
74	4.1.7	Secure Communications .....	14
75	4.2	Assurance Level 2.....	15
76	4.2.1	Enterprise and Service Maturity .....	15
77	4.2.2	Notices and User Information/Agreements .....	16
78	4.2.3	Information Security Management .....	18
79	4.2.4	Security-relevant Event (Audit) Records.....	19
80	4.2.5	Operational infrastructure .....	20
81	4.2.6	External Services and Components .....	21
82	4.2.7	Secure Communications .....	21
83	4.3	Assurance Level 3.....	24
84	4.3.1	Enterprise and Service Maturity .....	24
85	4.3.2	Notices and User Information.....	25
86	4.3.3	Information Security Management .....	27
87	4.3.4	Security-Relevant Event (Audit) Records .....	29
88	4.3.5	Operational Infrastructure.....	30
89	4.3.6	External Services and Components .....	31
90	4.3.7	Secure Communications .....	31
91	4.4	Assurance Level 4.....	33
92	4.4.1	Enterprise and Service Maturity .....	33
93	4.4.2	Notices and Subscriber Information/Agreements.....	34
94	4.4.3	Information Security Management .....	36
95	4.4.4	Security-Related (Audit) Records.....	38
96	4.4.5	Operational Infrastructure.....	38
97	4.4.6	External Services and Components .....	40

98	4.4.7	Secure Communications .....	40
99	4.5	Compliance Tables .....	42
100	<b>5</b>	<b>OPERATIONAL SERVICE ASSESSMENT CRITERIA.....</b>	<b>49</b>
101	5.1	Assurance Level 1 .....	49
102	5.1.1	Part A - Credential Operating Environment .....	49
103	5.1.2	Part B - Credential Issuing.....	51
104	5.1.3	Part C - Credential Renewal and Re-issuing.....	54
105	5.1.4	Part D - Credential Revocation .....	55
106	5.1.5	Part E - Credential Status Management .....	55
107	5.1.6	Part F - Credential Verification/Authentication.....	56
108	5.2	Assurance Level 2.....	59
109	5.2.1	Part A - Credential Operating Environment .....	59
110	5.2.2	Part B - Credential Issuing.....	61
111	5.2.3	Part C - Credential Renewal and Re-issuing.....	72
112	5.2.4	Part D - Credential Revocation .....	73
113	5.2.5	Part E - Credential Status Management .....	76
114	5.2.6	Part F - Credential Verification/Authentication.....	77
115	5.3	Assurance Level 3.....	81
116	5.3.1	Part A - Credential Operating Environment .....	81
117	5.3.2	Part B - Credential Issuing.....	84
118	5.3.3	Part C - Credential Renewal and Re-issuing.....	95
119	5.3.4	Part D - Credential Revocation .....	96
120	5.3.5	Part E - Credential Status Management .....	99
121	5.3.6	Part F - Credential Verification/Authentication.....	100
122	5.4	Assurance Level 4.....	104
123	5.4.1	Part A - Credential Operating Environment .....	104
124	5.4.2	Part B - Credential Issuing.....	107
125	5.4.3	Part C - Credential Renewal and Re-issuing.....	117
126	5.4.4	Part D - Credential Revocation .....	118
127	5.4.5	Part E - Credential Status Management .....	121
128	5.4.6	Part F - Credential Verification/Authentication.....	122
129	5.5	Compliance Tables .....	126
130	<b>6</b>	<b>REFERENCES.....</b>	<b>141</b>
131			
132			

## 133 1 INTRODUCTION

---

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

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

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

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

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

### 166 1.1 Changes in this revision

167 The principal reason for changes in this revision is to capture results of a mapping  
168 between version 3.0 of the SAC and NIST SP 800-63-2. Historically, AL1 and AL2 were  
169 aligned against SP 800-63-1 but no formalized mapping had been conducted at ALs 3  
170 & 4.

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

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

175 Additionally, the mapping between v2.0 and v3.0 found in §8 of v3.0 has been removed –  
176 at the time of formal publication of the revisions in the present version of the document  
177 SAC v3.0 had been published for over twelve months, and thereby all ongoing and new  
178 Approvals should be granted against at least v3.0.

179 A table listing all resolved Change Request ‘tickets’ is provided at the end of the  
180 document.

## 181 **2 ASSURANCE LEVELS**

---

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

## 187 **3 SERVICE ASSESSMENT CRITERIA - GENERAL**

---

### 188 **3.1 Context and Scope**

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

195

196 **1) Organizational Criteria:**

197 These criteria address the general business and organizational conformity of  
198 services and their providers. They are generally referred-to as the ‘CO-SAC’;

199 **2) Operational Criteria:**

200 These criteria address operational conformity of credential management services  
201 and the necessary functions which they embrace. They are generally referred-to  
202 as the ‘OP-SAC’.

### 203 **3.2 Criteria Applicability**

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

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

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

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

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



### 219 3.3 Status and Readership

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

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

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

### 233 3.4 Criteria Descriptions

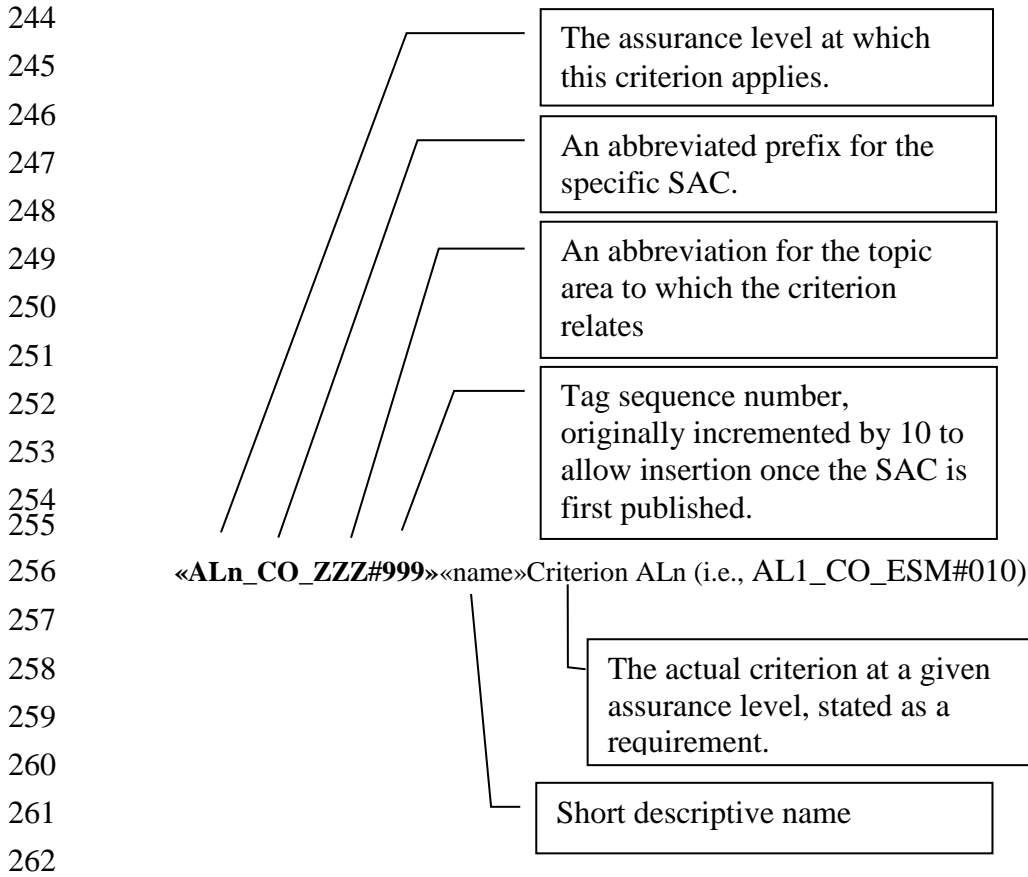
234 The Service Assessment Criteria are organized by AL. Subsections within each level  
235 describe the criteria that apply to specific functions. The subsections are parallel.  
236 Subsections describing the requirements for the same function at different levels of  
237 assurance have the same title.

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

241 The name identifies the intended scope or purpose of the criterion.

242

243 The criteria are described as follows:



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

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

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

266 also shown in bold.

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

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

269 then there has been addition and withdrawal of criteria.

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

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

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

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

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

275 being included but marked 'No stipulation'.

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

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

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

### 280 3.5 Terminology

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

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

## 286 4 COMMON ORGANIZATIONAL 287 SERVICE ASSESSMENT CRITERIA

---

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

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

### 295 4.1 Assurance Level 1

#### 296 4.1.1 Enterprise and Service Maturity

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

300 An enterprise and its specified service must:

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

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

304 *ALI\_CO\_ESM#020 Withdrawn*

305 Withdrawn

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

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

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

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

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

316 Specifically set out and demonstrate that it understands and complies with those legal and  
317 regulatory requirements incumbent upon it concerning the retention and destruction of  
318 private and identifiable information (personal and business - i.e. its secure storage and  
319 protection against loss, accidental public exposure, and/or improper destruction) and the

320 protection of Subjects' private information (against unlawful or unauthorized access,  
321 excepting that permitted by the information owner or required by due process).

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

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

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

333 **4.1.2 Notices and User information**

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

336 An enterprise and its specified service must:

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

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

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

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

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

346 a) a Privacy Policy

347

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

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

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

353 Require Subscribers and Subjects to:

354 a) indicate, prior to receiving service, that they have read and accept the terms of  
355 service as defined in the Service Definition;

- 356 b) at periodic intervals, determined by significant service provision events (e.g.  
357 issuance, re-issuance, renewal), re-affirm their understanding and observance of  
358 the terms of service;  
359 c) always provide full and correct responses to requests for information.

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

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

366 **4.1.3 No stipulation**

367 **4.1.4 No stipulation**

368 **4.1.5 No stipulation**

369 **4.1.6 No stipulation**

370 **4.1.7 Secure Communications**

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

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

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

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

375 Ensure that:

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

382

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#030 Due notification*

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

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

480 Require Subscribers and Subjects to:

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

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

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

492 *AL2\_CO\_NUI#060 Withdrawn*

493 Withdrawn.

494 *AL2\_CO\_NUI#070 Change of Subscriber Information*

495 **Require and provide the mechanisms for Subscribers and Subjects to provide in a**  
496 **timely manner full and correct amendments should any of their recorded**

497 **information change, as required under the terms of their use of the service, and only**  
498 **after the Subscriber's and/or Subject's identity has been authenticated.**

499 *AL2\_CO\_NUI#080 Withdrawn*  
500 Withdrawn.

### 501 **4.2.3 Information Security Management**

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

507 An enterprise and its specified service must:

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

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

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

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

524 *AL2\_CO\_ISM#050 Configuration Management*  
525 **Demonstrate that there is in place a configuration management system that at least**  
526 **includes:**

- 527 a) **version control for software system components;**
- 528 b) **timely identification and installation of all organizationally-approved patches**  
529 **for any software used in the provisioning of the specified service.**

530 *AL2\_CO\_ISM#060 Quality Management*  
531 **Demonstrate that there is in place a quality management system that is appropriate**  
532 **for the specified service.**

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

534 **Apply controls during system development, procurement installation, and operation**  
535 **that protect the security and integrity of the system environment, hardware,**  
536 **software, and communications.**

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

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

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

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

553 *AL2\_CO\_ISM#090 Withdrawn*

554 **Withdrawn.**

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

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

562 *AL2\_CO\_ISM#110 Withdrawn*

563 **Withdrawn.**

564

#### 565 **4.2.4 Security-relevant Event (Audit) Records**

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

568 An enterprise and its specified service must:

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

570 **Maintain a log of all relevant security events concerning the operation of the service,**  
571 **together with an accurate record of the time at which the event occurred (time-**

572 **stamp), and retain such records with appropriate protection and controls to ensure**  
573 **successful retrieval, accounting for service definition, risk management**  
574 **requirements, applicable legislation, and organizational policy.**

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

578

#### 579 **4.2.5 Operational infrastructure**

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

583 An enterprise and its specified service must:

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

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

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

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

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

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

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

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

606 **Ensure that employees are sufficiently trained, qualified, experienced, and current**  
607 **for the roles they fulfill. Such measures must be accomplished either by recruitment**  
608 **practices or through a specific training program. Where employees are undergoing**

609 **on-the-job training, they must only do so under the guidance of a mentor possessing**  
610 **the defined service experiences for the training being provided.**

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

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

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

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

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

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

619 Require a minimum of two person physical access control when accessing any  
620 cryptographic modules.

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

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

624

#### 625 **4.2.6 External Services and Components**

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

629 An enterprise and its specified service must:

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

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

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

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

642

#### 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

## 687 4.3 Assurance Level 3

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

### 690 4.3.1 Enterprise and Service Maturity

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

693 An enterprise and its specified service must:

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

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

697 *AL3\_CO\_ESM#020 Withdrawn*

698 Withdrawn

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

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

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

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

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

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

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



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

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

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

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

739 *AL3\_CO\_ESM#060 Ownership*

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

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

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

748

#### 749 **4.3.2 Notices and User Information**

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

753 An enterprise and its specified service must:

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

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

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

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

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

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

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

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

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

788 Require Subscribers and Subjects to:

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

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

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

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

800 *AL3\_CO\_NUI#060 Withdrawn*  
801 Withdrawn.

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

807 *AL3\_CO\_NUI#080 Withdrawn*  
808 Withdrawn.

809

### 810 **4.3.3 Information Security Management**

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

816 An enterprise and its specified service must:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

#### 895 **4.3.4 Security-Relevant Event (Audit) Records**

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

898 An enterprise and its specified service must:

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

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

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

908

### 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) there is 24/7 monitoring for unauthorized intrusions.

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

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

955

956 **4.3.6 External Services and Components**

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

960 An enterprise and its specified service must:

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

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

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

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

973

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



## 1018 4.4 Assurance Level 4

1019 Achieving AL4 requires meeting even more stringent criteria in addition to the criteria  
1020 required to achieve AL3.

### 1021 4.4.1 Enterprise and Service Maturity

1022 Criteria in this section address the establishment of the enterprise offering the service and  
1023 its basic standing as a legal and operational business entity.

1024 An enterprise and its specified service must:

1025 *ALA\_CO\_ESM#010 Established enterprise*

1026 Be a valid legal entity and a person with legal authority to commit the organization must  
1027 submit the signed assessment package.

1028 *ALA\_CO\_ESM#020 Withdrawn*

1029 Withdrawn

1030 *ALA\_CO\_ESM#030 Legal & Contractual compliance*

1031 Demonstrate that it understands and complies with any legal requirements incumbent on  
1032 it in connection with operation and delivery of the specified service, accounting for all  
1033 jurisdictions within which its services may be offered. Any specific contractual  
1034 requirements shall also be identified.

1035 **Guidance:** Kantara Initiative will not recognize a service which is not fully released for  
1036 the provision of services to its intended user/client community. Systems, or parts thereof,  
1037 which are not fully proven and released shall not be considered in an assessment and  
1038 therefore should not be included within the scope of the assessment package. Parts of  
1039 systems still under development, or even still being planned, are therefore ineligible for  
1040 inclusion within the scope of assessment.

1041 *ALA\_CO\_ESM#040 Financial Provisions*

1042 Provide documentation of financial resources that allow for the continued operation of the  
1043 service and demonstrate appropriate liability processes and procedures that satisfy the  
1044 degree of liability exposure being carried.

1045 **Guidance:** The organization must show that it has a budgetary provision to operate the  
1046 service for at least a twelve-month period, with a clear review of the budgetary planning  
1047 within that period so as to keep the budgetary provisions extended. It must also show  
1048 how it has determined the degree of liability protection required, in view of its exposure  
1049 per 'service' and the number of users it has. This criterion helps ensure that Kantara  
1050 Initiative does not grant Recognition to services that are not likely to be sustainable over  
1051 at least this minimum period of time.

1052 *ALA\_CO\_ESM#050 Data Retention and Protection*

1053 Specifically set out and demonstrate that it understands and complies with those legal and  
1054 regulatory requirements incumbent upon it concerning the retention and destruction of  
1055 private and identifiable information (personal and business) (i.e. its secure storage and  
1056 protection against loss, accidental public exposure, and/or improper destruction) and the  
1057 protection of private information (against unlawful or unauthorized access excepting that  
1058 permitted by the information owner or required by due process).

1059 *ALA\_CO\_ESM#055 Termination provisions*

1060 Define the practices in place for the protection of Subjects' private and secret information  
1061 related to their use of the service which must ensure the ongoing secure preservation and  
1062 protection of legally required records and for the secure destruction and disposal of any  
1063 such information whose retention is no longer legally required. Specific details of these  
1064 practices must be made available.

1065 **Guidance:** Termination covers the cessation of the business activities, the service  
1066 provider itself ceasing business operations altogether, change of ownership of the service-  
1067 providing business, and other similar events which change the status and/or operations of  
1068 the service provider in any way which interrupts the continued provision of the specific  
1069 service.

1070 *ALA\_CO\_ESM#060 Ownership*

1071 If the enterprise named as the CSP is a part of a larger entity, the nature of the relationship  
1072 with its parent organization, shall be disclosed to the assessors and, on their request, to  
1073 customers.

1074 *ALA\_CO\_ESM#070 Independent Management and Operations*

1075 Demonstrate that, for the purposes of providing the specified service, its management and  
1076 operational structures are distinct, autonomous, have discrete legal accountability, and  
1077 operate according to separate policies, procedures, and controls.

1078

#### 1079 **4.4.2 Notices and Subscriber Information/Agreements**

1080 Criteria in this section address the publication of information describing the service and  
1081 the manner of and any limitations upon its provision, and how users are required to accept  
1082 those terms.

1083 An enterprise and its specified service must:

1084 *ALA\_CO\_NUI#010 General Service Definition*

1085 Make available to the intended user community a Service Definition that includes all  
1086 applicable Terms, Conditions, and Fees, including any limitations of its usage, and  
1087 definitions of any terms having specific intention or interpretation. Specific provisions  
1088 are stated in further criteria in this section.

1089 **Guidance:** The intended user community encompasses potential and actual Subscribers,  
1090 Subjects, and relying parties.

1091 *ALA\_CO\_NUI#020 Service Definition inclusions*

1092 Make available a Service Definition for the specified service containing clauses that  
1093 provide the following information:

- 1094 a) Privacy, Identity Proofing & Verification, **Renewal/Re-issuance**, and Revocation  
1095 and Termination Policies;
- 1096 b) the country in or legal jurisdiction under which the service is operated;
- 1097 c) if different to the above, the legal jurisdiction under which Subscriber and any  
1098 relying party agreements are entered into;
- 1099 d) applicable legislation with which the service complies;
- 1100 e) obligations incumbent upon the CSP;
- 1101 f) obligations incumbent upon the Subscriber and Subject;
- 1102 g) notifications and guidance for relying parties, especially in respect of actions they  
1103 are expected to take should they choose to rely upon the service's product;
- 1104 h) statement of warranties;
- 1105 i) statement of liabilities toward both Subjects and Relying Parties;
- 1106 j) procedures for notification of changes to terms and conditions;
- 1107 k) steps the CSP will take in the event that it chooses or is obliged to terminate the  
1108 service;
- 1109 l) availability of the specified service per se and of its help desk facility.

1110 *ALA\_CO\_NUI#030 Due Notification*

1111 Have in place and follow appropriate policy and procedures to ensure that it notifies  
1112 Subscribers and Subjects in a timely and reliable fashion of any changes to the Service  
1113 Definition and any applicable Terms, Conditions, Fees, and Privacy Policy for the  
1114 specified service, and provide a clear means by which Subscribers and Subjects must  
1115 indicate that they wish to accept the new terms or terminate their subscription.

1116 *ALA\_CO\_NUI#040 User Acceptance*

1117 Require Subscribers and Subjects to:

- 1118 a) indicate, prior to receiving service, that they have read and accept the terms of  
1119 service as defined in the Service Definition, thereby indicating their properly-  
1120 informed opt-in;
- 1121 b) at periodic intervals, determined by significant service provision events (e.g.  
1122 issuance, re-issuance, renewal) and otherwise at least once every five years, re-  
1123 affirm their understanding and observance of the terms of service;
- 1124 c) always provide full and correct responses to requests for information.

1125 *ALA\_CO\_NUI#050 Record of User Acceptance*

1126 Obtain a record (hard-copy or electronic) of the Subscriber's and Subject's acceptance of  
1127 the terms and conditions of service, prior to initiating the service and thereafter reaffirm  
1128 the agreement at periodic intervals, determined by significant service provision events  
1129 (e.g. issuance, re-issuance, renewal) and otherwise at least once every five years.

1130 *ALA\_CO\_NUI#060 Withdrawn*

1131 Withdrawn.

1132 *ALA\_CO\_NUI#070* Change of Subscriber Information

1133 *Require and provide the mechanisms for Subscribers and Subjects to provide in a timely*  
1134 *manner full and correct amendments should any of their recorded information change, as*  
1135 *required under the terms of their use of the service, and only after the Subscriber's and/or*  
1136 *Subject's identity has been authenticated.*

1137 *ALA\_CO\_NUI#080* *Withdrawn*

1138 Withdrawn.

1139

#### 1140 **4.4.3 Information Security Management**

1141 These criteria address the way in which the enterprise manages the security of its  
1142 business, the specified service, and information it holds relating to its user community.  
1143 This section focuses on the key components that comprise a well-established and  
1144 effective Information Security Management System (ISMS), or other IT security  
1145 management methodology recognized by a government or professional body.

1146 An enterprise and its specified service must:

1147 *ALA\_CO\_ISM#010* *Documented policies and procedures*

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

1152 *ALA\_CO\_ISM#020* *Policy Management and Responsibility*

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

1157 *ALA\_CO\_ISM#030* *Risk Management*

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

1162 *ALA\_CO\_ISM#040* *Continuity of Operations Plan*

1163 Have and keep updated a continuity of operations plan that covers disaster recovery and  
1164 the resilience of the specified service and must show that **on-going review of this plan is**  
1165 **conducted as a part of the business' procedures.**

1166 *ALA\_CO\_ISM#050* *Configuration Management*

1167 Demonstrate that there is in place a configuration management system that at least  
1168 includes:

- 1169 a) version control for software system components;
- 1170 b) timely identification and installation of all organizationally-approved patches for  
1171 any software used in the provisioning of the specified service;
- 1172 c) version control and managed distribution for all documentation associated with  
1173 the specification, management, and operation of the system, covering both  
1174 internal and publicly available materials.

1175 *ALA\_CO\_ISM#060 Quality Management*

1176 Demonstrate that there is in place a quality management system that is appropriate for the  
1177 specified service.

1178 *ALA\_CO\_ISM#070 System Installation and Operation Controls*

1179 Apply controls during system development, procurement, installation, and operation that  
1180 protect the security and integrity of the system environment, hardware, software, and  
1181 communications having particular regard to:

- 1182 a) the software and hardware development environments, for customized  
1183 components;
- 1184 b) the procurement process for commercial off-the-shelf (COTS) components;
- 1185 c) contracted consultancy/support services;
- 1186 d) shipment of system components;
- 1187 e) storage of system components;
- 1188 f) installation environment security;
- 1189 g) system configuration;
- 1190 h) transfer to operational status.

1191 *ALA\_CO\_ISM#080 Internal Service Audit*

1192 Be subjected to a first-party audit at least once every 12 months for the effective  
1193 provision of the specified service by internal audit functions of the enterprise responsible  
1194 for the specified service, unless it can show that by reason of its organizational size or due  
1195 to other justifiable operational restrictions it is unreasonable to be so audited.

1196 **Guidance:** ‘First-party’ audits are those undertaken by an independent part of the same  
1197 organization which offers the service. The auditors cannot be involved in the  
1198 specification, development or operation of the service.

1199 Management systems require that there be internal audit conducted as an inherent part of  
1200 management review processes. Any third-party (i.e. independent) audit of the  
1201 management system is intended to show that the internal management system controls are  
1202 being appropriately applied, and for the purposes of fulfilling Kantara’s needs, a formal  
1203 Kantara Assessment performed by an Accredited Assessor should be considered as such.

1204 *ALA\_CO\_ISM#090 Withdrawn*  
1205 **Withdrawn.**

1206 *ALA\_CO\_ISM#100 Audit Records*

1207 Retain records of all audits, both internal and independent, for a period which, as a  
1208 minimum, fulfills its legal obligations and otherwise for greater periods either as it may  
1209 have committed to in its Service Definition or required by any other obligations it has  
1210 with/to a Subscriber or Subject, and which in any event is not less than 36 months. Such  
1211 records must be held securely and be protected against unauthorized access loss,  
1212 alteration, public disclosure, or unapproved destruction.

1213 *ALA\_CO\_ISM#110 Withdrawn*

1214 Withdrawn.

1215 *ALA\_CO\_ISM#120 Best Practice Security Management*

1216 Have in place a **certified** Information Security Management System (ISMS), or other IT  
1217 security management methodology recognized by a government or professional body, that  
1218 **has been assessed and found to be in compliance with the requirements of**  
1219 **ISO/IEC 27001 [IS27001] and which applies and is appropriate to the CSP in**  
1220 **question.** All requirements expressed in preceding criteria in this section must *inter alia*  
1221 fall wholly within the scope of this ISMS, or the selected recognized alternative.

1222 **4.4.4 Security-Related (Audit) Records**

1223 The criteria in this section are concerned with the need to provide an auditable log of all  
1224 events that are pertinent to the correct and secure operation of the service.

1225 An enterprise and its specified service must:

1226 *ALA\_CO\_SER#010 Security Event Logging*

1227 Maintain a log of all relevant security events concerning the operation of the service,  
1228 together with a **precise** record of the time at which the event occurred (time-stamp)  
1229 **provided by a trusted time-source** and retain such records with appropriate protection  
1230 and controls to ensure successful retrieval, accounting for service definition, risk  
1231 management requirements, applicable legislation, and organizational policy.

1232 **Guidance:** The trusted time source could be an external trusted service or a network time  
1233 server or other hardware timing device. The time source must be not only precise but  
1234 authenticatable as well.

1235

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) there is 24/7 monitoring for unauthorized intrusions.

1279 *ALA\_CO\_OPN#070 Logical access control*

1280 Employ logical access control mechanisms that ensure access to sensitive system  
1281 functions and controls is restricted to authorized personnel.

1282

#### 1283 **4.4.6 External Services and Components**

1284 This section addresses the relationships and obligations upon contracted parties both to  
1285 apply the policies and procedures of the enterprise and also to be available for assessment  
1286 as critical parts of the overall service provision.

1287 An enterprise and its specified service must:

##### 1288 *ALA\_CO\_ESC#010 Contracted Policies and Procedures*

1289 Where the enterprise uses external suppliers for specific packaged components of the  
1290 service or for resources which are integrated with its own operations and under its  
1291 control, ensure that those parties are engaged through reliable and appropriate contractual  
1292 arrangements which stipulate which critical policies, procedures, and practices sub-  
1293 contractors are required to fulfill.

##### 1294 *ALA\_CO\_ESC#020 Visibility of Contracted Parties*

1295 Where the enterprise uses external suppliers for specific packaged components of the  
1296 service or for resources which are integrated with its own operations and under its  
1297 control, ensure that the suppliers' compliance with contractually-stipulated policies and  
1298 procedures, and thus with the IAF Service Assessment Criteria, can be independently  
1299 verified, and subsequently monitored if necessary.

1300

#### 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 .

1313 **Guidance:** The reference to "parties requiring access to the CSP's services" is intended  
1314 to cover SP 800-63-2's reference to RPs (see cross-mapped EZP 63-2 clause).

##### 1315 *ALA\_CO\_SCO#020 Limited access to shared secrets*

1316 Ensure that:

- 1317 a) access to shared secrets shall be subject to discretionary controls which permit  
1318 access to those roles/applications which need such access;



- 1319 b) stored shared secrets are encrypted such that:  
1320 i) the encryption key for the shared secret file is encrypted under a key held in a  
1321 FIPS 140-2 [FIPS140-2] Level 2 (or higher) validated hardware  
1322 cryptographic module, or equivalent, as established by a recognized national  
1323 technical authority, or any FIPS 140-2 Level 3 or 4 validated cryptographic  
1324 module, or equivalent, as established by a recognized national technical  
1325 authority, and decrypted only as immediately required for an authentication  
1326 operation;  
1327 ii) they are protected as a key within the boundary of a FIPS 140-2 Level 2 (or  
1328 higher) validated hardware cryptographic module, or equivalent, as  
1329 established by a recognized national technical authority, or any FIPS 140-2  
1330 Level 3 or 4 cryptographic module, or equivalent, as established by a  
1331 recognized national technical authority, and are not exported from the module  
1332 in plaintext;  
1333 iii) they are split by an "*n from m*" cryptographic secret-sharing method;
- 1334 c) any long-term (i.e., not session) shared secrets are revealed only to the Subject  
1335 and the CSP's direct agents (bearing in mind (a) above).  
1336 **These roles should be defined and documented by the CSP in accordance with**  
1337 **AL4\_CO\_OPN#020 above.**  
1338

1339 **4.5 Compliance Tables**

1340 Use the following tables to correlate criteria for a particular Assurance Level (AL) and  
1341 the evidence offered to support compliance.

1342 Service providers preparing for an assessment can use the table appropriate to the AL at  
1343 which they are seeking approval to correlate evidence with criteria or to justify non-  
1344 applicability (e.g., "specific service types not offered").

1345 Assessors can use the tables to record the steps in their assessment and their  
1346 determination of compliance or failure.

1347 **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>	
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>	

1348

1349

1350

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

Clause	Description	Compliance
AL2_CO_ESM#010	<a href="#">Established enterprise</a>	
AL2_CO_ESM#020	Withdrawn	No conformity requirement
AL2_CO_ESM#030	<a href="#">Legal &amp; Contractual compliance</a>	
AL2_CO_ESM#040	<a href="#">Financial Provisions</a>	
AL2_CO_ESM#050	<a href="#">Data Retention and Protection</a>	
AL2_CO_ESM#055	<a href="#">Termination provisions</a>	
AL2_CO_NUI#010	<a href="#">General Service Definition</a>	
AL2_CO_NUI#020	<a href="#">Service Definition inclusions</a>	
AL2_CO_NUI#030	<a href="#">Due notification</a>	
AL2_CO_NUI#040	<a href="#">User Acceptance</a>	
AL2_CO_NUI#050	<a href="#">Record of User Acceptance</a>	
AL2_CO_NUI#060	Withdrawn	No conformity requirement
AL2_CO_NUI#070	<a href="#">Change of Subscriber Information</a>	
AL2_CO_NUI#080	Withdrawn	No conformity requirement
AL2_CO_ISM#010	<a href="#">Documented policies and procedures</a>	
AL2_CO_ISM#020	<a href="#">Policy Management and Responsibility</a>	
AL2_CO_ISM#030	<a href="#">Risk Management</a>	
AL2_CO_ISM#040	<a href="#">Continuity of Operations Plan</a>	
AL2_CO_ISM#050	<a href="#">Configuration Management</a>	
AL2_CO_ISM#060	<a href="#">Quality Management</a>	
AL2_CO_ISM#070	<a href="#">System Installation and Operation Controls</a>	
AL2_CO_ISM#080	<a href="#">Internal Service Audit</a>	
AL2_CO_ISM#090	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>	
AL2_CO_OPN#070	<a href="#">Logical access control</a>	

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

1351

1352

1353

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

<b>Clause</b>	<b>Description</b>	<b>Compliance</b>
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>	
AL3_CO_NUI#030	<a href="#">Due notification</a>	
AL3_CO_NUI#040	<a href="#">User Acceptance</a>	
AL3_CO_NUI#050	<a href="#">Record of User Acceptance</a>	
AL3_CO_NUI#060	Withdrawn	No conformity requirement
AL3_CO_NUI#070	<a href="#">Change of Subscriber Information</a>	
AL3_CO_NUI#080	Withdrawn	No conformity requirement
AL3_CO_ISM#010	<a href="#">Documented policies and procedures</a>	
AL3_CO_ISM#020	<a href="#">Policy Management and Responsibility</a>	
AL3_CO_ISM#030	<a href="#">Risk Management</a>	
AL3_CO_ISM#040	<a href="#">Continuity of Operations Plan</a>	
AL3_CO_ISM#050	<a href="#">Configuration Management</a>	
AL3_CO_ISM#060	<a href="#">Quality Management</a>	
AL3_CO_ISM#070	<a href="#">System Installation and Operation Controls</a>	
AL3_CO_ISM#080	<a href="#">Internal Service Audit</a>	
AL3_CO_ISM#090	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>	
AL3_CO_OPN#070	<a href="#">Logical access control</a>	
AL3_CO_ESC#010	<a href="#">Contracted policies and procedures</a>	
AL3_CO_ESC#020	<a href="#">Visibility of contracted parties</a>	
AL3_CO_SCO#010	<a href="#">Secure remote communications</a>	
AL3_CO_SCO#015	<a href="#">Verification / Authentication confirmation messages</a>	
AL3_CO_SCO#016	Withdrawn	
AL3_CO_SCO#020	<a href="#">Limited access to shared secrets</a>	

1354

1355

1356

**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>	
AL4_CO_ESM#060	<a href="#">Ownership</a>	
AL4_CO_ESM#070	<a href="#">Independent Management and Operations</a>	
AL4_CO_NUI#010	<a href="#">General Service Definition</a>	
AL4_CO_NUI#020	<a href="#">Service Definition inclusions</a>	
AL4_CO_NUI#030	<a href="#">Due Notification</a>	
AL4_CO_NUI#040	<a href="#">User Acceptance</a>	
AL4_CO_NUI#050	<a href="#">Record of User Acceptance</a>	
AL4_CO_NUI#060	Withdrawn	No conformity requirement
AL4_CO_NUI#070	<a href="#">Change of Subscriber Information</a>	
AL4_CO_NUI#080	Withdrawn	No conformity requirement
AL4_CO_ISM#010	<a href="#">Documented policies and procedures</a>	
AL4_CO_ISM#020	<a href="#">Policy Management and Responsibility</a>	
AL4_CO_ISM#030	<a href="#">Risk Management</a>	
AL4_CO_ISM#040	<a href="#">Continuity of Operations Plan</a>	
AL4_CO_ISM#050	<a href="#">Configuration Management</a>	
AL4_CO_ISM#060	<a href="#">Quality Management</a>	
AL4_CO_ISM#070	<a href="#">System Installation and Operation Controls</a>	
AL4_CO_ISM#080	<a href="#">Internal Service Audit</a>	
AL4_CO_ISM#090	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>	
AL4_CO_OPN#070	<a href="#">Logical access control</a>	
AL4_CO_ESC#010	<a href="#">Contracted Policies and Procedures</a>	
AL4_CO_ESC#020	<a href="#">Visibility of Contracted Parties</a>	
AL4_CO_SCO#010	<a href="#">Secure remote communications</a>	
AL4_CO_SCO#020	<a href="#">Limited access to shared secrets</a>	

1357



## 1358 **5 OPERATIONAL SERVICE ASSESSMENT CRITERIA**

---

1359 The Service Assessment Criteria in this section establish requirements for the operational  
1360 conformity of credential management services and their providers at all Assurance Levels  
1361 (AL) – refer to Section 2. These criteria are generally referred to elsewhere within IAF  
1362 documentation as OP-SAC.

1363 Previous editions of this document have these criteria set out in two distinct sections and  
1364 have used the terms CM-SAC and ID-SAC: the OP-SAC is the combination of those two  
1365 previous SAC sections, with optimizations necessary for their integration. To ensure  
1366 backwards compatibility with assessments already performed against previous editions of  
1367 this document the criteria within the OP-SAC continue to be identified either by a tag  
1368 “ALn\_ID\_ xxxx” or “ALn\_CM\_ xxxx”.

1369 Within each Assurance Level the criteria are divided into six Parts. Each part deals with a  
1370 specific functional aspect of the overall credential management process, including  
1371 identity proofing services (see Parts B, at each Assurance Level).

1372 Full Service Provision requires conformity to all of the following operational criteria at  
1373 the chosen Assurance Level. This may be demonstrated either by the Full Service  
1374 Provider fulfilling all of these criteria itself or by its service being a composition of  
1375 Service Components which must, collectively, fulfill all of these criteria, under the overall  
1376 management of the Full Service Provider. Providers of Service Components may  
1377 conform to a defined sub-set of these criteria (although, within Part A at each Assurance  
1378 Level, there is a small number of criteria which are mandatory for Component Services,  
1379 which are marked as such).

1380 The procedures and processes required to create a secure environment for management of  
1381 credentials and the particular technologies that are considered strong enough to meet the  
1382 assurance requirements differ considerably from level to level.

1383

### 1384 **5.1 Assurance Level 1**

#### 1385 **5.1.1 Part A - Credential Operating Environment**

1386 These criteria describe requirements for the overall operational environment in which  
1387 credential lifecycle management is conducted. The Common Organizational criteria  
1388 describe broad requirements. The criteria in this Part describe operational  
1389 implementation specifics

1390 These criteria apply to PINs and passwords, as well as SAML assertions.

1391 The criterion AL1\_CM\_CTR#030 is marked as **MANDATORY** for all Component  
1392 Services.

1393 **5.1.1.1 Not used**

1394 No stipulation.

1395 **5.1.1.2 Security Controls**

1396 An enterprise and its specified service must:

1397 *ALI\_CM\_CTR#010* *Withdrawn*

1398 *ALI\_CM\_CTR#020* *Protocol threat risk assessment and controls*

1399 Account for at least the following protocol threats and apply appropriate controls that  
1400 make the threats impractical:

- 1401 a) password guessing, such that there are at least 14 bits of entropy to resist an on-  
1402 line guessing attack against a selected user/password;
- 1403 b) message replay.

1404 *ALI\_CM\_CTR#025* *No stipulation*

1405 *ALI\_CM\_CTR#028* *No stipulation*

1406 *ALI\_CM\_CTR#030* *System threat risk assessment and controls*

1407 **MANDATORY.**

1408 Account for the following system threats and apply appropriate controls:

- 1409 a) the introduction of malicious code;
- 1410 b) compromised authentication arising from insider action;
- 1411 c) out-of-band attacks by other users and system operators (e.g., the ubiquitous  
1412 shoulder-surfing);
- 1413 d) spoofing of system elements/applications;
- 1414 e) malfeasance on the part of Subscribers and Subjects.

1415 **5.1.1.3 Storage of Long-term Secrets**

1416 *ALI\_CM\_STS#010* *Withdrawn*

1417 Withdrawn (AL1\_CO\_SCO#020 (a) & (b) enforce this requirement)

1418 **5.1.1.4 No stipulation**

1419 **5.1.1.5 Subject Options**

1420 *ALI\_CM\_OPN#010* *Withdrawn*

1421 Withdrawn – see AL1\_CM\_RNR#010.

1422

1423 **5.1.2 Part B - Credential Issuing**

1424 These criteria apply to the verification of the identity of the Subject of a credential and  
1425 with token strength and credential delivery mechanisms. They address requirements  
1426 levied by the use of various technologies to achieve **Assurance Level 1**.

1427 **5.1.2.1 Identity Proofing Policy**

1428 The specific service must show that it applies identity proofing policies and procedures  
1429 and that it retains appropriate records of identity proofing activities and evidence.

1430 The enterprise and its specified service must:

1431 *ALI\_CM\_IDP#010 Withdrawn*

1432 Withdrawn.

1433 *ALI\_CM\_IDP#020 Withdrawn*

1434 Withdrawn.

1435 *ALI\_CM\_IDP#030 Withdrawn*

1436 Withdrawn.

1437 *ALI\_ID\_POL#010 Unique service identity*

1438 Ensure that a unique identity is attributed to the specific service, such that credentials  
1439 issued by it can be distinguishable from those issued by other services, including services  
1440 operated by the same enterprise.

1441 *ALI\_ID\_POL#020 Unique Subject identity*

1442 Ensure that each applicant's identity is unique within the service's community of Subjects  
1443 and uniquely associable with tokens and/or credentials issued to that identity.

1444

1445 **5.1.2.2 Identity Verification**

1446 The enterprise or specific service:

1447 *ALI\_ID\_IDV#000 Identity Proofing classes*

1448 a) must include in its Service Definition at least one of the following classes of  
1449 identity proofing service, and;

1450 b) may offer any additional classes of identity proofing service it chooses, subject to  
1451 the nature and the entitlement of the CSP concerned;

1452 c) must fulfill the applicable assessment criteria according to its choice of identity  
1453 proofing service, i.e. conform to at least one of the criteria sets defined in:

1454 i) §5.1.2.3, "In-Person Public Identity Proofing";

1455 ii) §5.1.2.4, "Remote Public Identity Proofing".

1456

1457 **5.1.2.3 In-Person Public Identity Verification**

1458 If the specific service offers in-person identity proofing to applicants with whom it has no  
1459 previous relationship, then it must comply with the criteria in this section.

1460 An enterprise or specified service must:

1461 *ALI\_ID\_IPV#010 Required evidence*

1462 Accept a self-assertion of identity.

1463 *ALI\_ID\_IPV#020 Evidence checks*

1464 Accept self-attestation of evidence.

1465

1466 **5.1.2.4 Remote Public Identity Verification**

1467 If the specific service offers remote identity proofing to applicants with whom it has no  
1468 previous relationship, then it must comply with the criteria in this section.

1469 An enterprise or specified service must:

1470 *ALI\_ID\_RPV#010 Required evidence*

1471 Require the applicant to provide a contact telephone number or email address.

1472 *ALI\_ID\_RPV#020 Evidence checks*

1473 Verify the provided information by either:

1474 a) confirming the request by calling the number;

1475 b) successfully sending a confirmatory email and receiving a positive  
1476 acknowledgement.

1477

1478 **5.1.2.5 No stipulation**

1479

1480 **5.1.2.6 No stipulation**

1481

1482 **5.1.2.7 Issuing Derived Credentials**

1483 Where the Applicant already possesses recognized original credentials the CSP may  
1484 choose to accept the verified identity of the Applicant as a substitute for identity proofing,  
1485 subject to the following specific provisions. All other requirements of Assurance Level 1  
1486 identity proofing must also be observed.

1487 *AL1\_ID\_IDC#010 Authenticate Original Credential*  
1488 Prior to issuing any derived credential the original credential on which the identity-  
1489 proofing relies must be proven to be in the possession and under the control of the  
1490 Applicant.

#### 1491 **5.1.2.8 Secondary Identity Verification**

1492 In each of the above cases, an enterprise or specified service must:

1493 *AL1\_ID\_SCV#010 Secondary checks*  
1494 Have in place additional measures (e.g., require additional documentary evidence, delay  
1495 completion while out-of-band checks are undertaken) to deal with any anomalous  
1496 circumstances that can be reasonably anticipated (e.g., a legitimate and recent change of  
1497 address that has yet to be established as the address of record).

#### 1498 **5.1.2.9 Identity-proofing Records**

1499 *AL1\_ID\_VRC#010 No stipulation*

1500 *AL1\_ID\_VRC#020 No stipulation*

1501 *AL1\_ID\_VRC#025 Provide Subject Identity Records*

1502 If required, provide to qualifying parties a unique identity for each Subscriber and their  
1503 associated tokens and credentials.

1504 *AL1\_ID\_VRC#030 No stipulation*

1505 *AL2\_CM\_IDP#040 Revision to Subject Information*

1506 Provide a means for Subjects to amend their stored information after registration.

#### 1507 **5.1.2.10 Credential Creation**

1508 These criteria address the requirements for creation of credentials that can only be used at  
1509 AL1. Any credentials/tokens that comply with the criteria stipulated for AL2 and higher  
1510 are acceptable at AL1.

1511 An enterprise and its specified service must:

1512 *AL1\_CM\_CRN#010 Authenticated Request*

1513 Only accept a request to generate a credential and bind it to an identity if the source of the  
1514 request can be authenticated as being authorized to perform identity proofing at AL1 or  
1515 higher.

1516 *AL1\_CM\_CRN#020 No stipulation*

1517 *AL1\_CM\_CRN#030 Credential uniqueness*

1518 Allow the Subject to select a credential (e.g., UserID) that is verified to be unique within  
1519 the specified service's community and assigned uniquely to a single identity Subject.

1520 *AL1\_CM\_CRN#035 Convey credential*

1521 Be capable of conveying the unique identity information associated with a credential to  
1522 Verifiers and Relying Parties.

1523 *ALI\_CM\_CRN#040 Token strength*

1524 Ensure that the single-factor token associated with the credential has the one of the  
1525 following set of characteristics:

1526 a) For a memorized secret, apply a rule-set such that there shall be a minimum of 14  
1527 bits of entropy in the pin or pass-phrase;

1528 b) For a knowledge-based question, apply a rule-set such that there shall be:

1529 i) a minimum of 14 bits of entropy in the pin or pass-phrase OR;

1530 ii) a set of knowledge-based questions created by the user OR;

1531 iii) a set of knowledge-based questions selected by the user from a service-  
1532 generated list of at least five questions.

1533

1534 Note – null or empty answers in any case above shall not be permitted.

1535

1536 Only allow password tokens that have a resistance to online guessing attack against a  
1537 selected user/password of at least 1 in  $2^{14}$  (16,384), accounting for state-of-the-art attack  
1538 strategies, and at least 10 bits of min-entropy.

1539 **5.1.2.11 No stipulation**

1540 **5.1.2.12 No stipulation**

1541

### 1542 **5.1.3 Part C - Credential Renewal and Re-issuing**

1543 These criteria apply to the renewal and re-issuing of credentials. They address  
1544 requirements levied by the use of various technologies to achieve the appropriate  
1545 Assurance Level 1.

#### 1546 **5.1.3.1 Renewal/Re-issuance Procedures**

1547 These criteria address general renewal and re-issuance functions, to be exercised as  
1548 specific controls in these circumstances while continuing to observe the general  
1549 requirements established for initial credential issuance.

1550 An enterprise and its specified service must:

1551 *ALI\_CM\_RNR#010 Changeable PIN/Password*

1552 Permit Subjects to change their PINs/passwords.

1553

1554 **5.1.4 Part D - Credential Revocation**

1555 These criteria deal with credential revocation and the determination of the legitimacy of a  
1556 revocation request.

1557 An enterprise and its specified service must:

1558 **5.1.4.1 No stipulation**

1559 **5.1.4.2 No stipulation**

1560 **5.1.4.3 No stipulation**

1561 **5.1.4.4 Secure Revocation Request**

1562 This criterion applies when revocation requests between remote components of a service  
1563 are made over a secured communication.

1564 An enterprise and its specified service must:

1565 *ALI\_CM\_SRR#010 Submit Request*

1566 Submit a request for revocation to the Credential Issuer service (function), using a  
1567 secured network communication, if necessary.

1568

1569 **5.1.5 Part E - Credential Status Management**

1570 These criteria deal with credential status management, such as the receipt of requests for  
1571 new status information arising from a new credential being issued or a revocation or other  
1572 change to the credential that requires notification. They also deal with the provision of  
1573 status information to requesting parties (Verifiers, Relying Parties, courts and others  
1574 having regulatory authority, etc.) having the right to access such information.

1575 **5.1.5.1 Status Maintenance**

1576 An enterprise and its specified service must:

1577 *ALI\_CM\_CSM#010 Maintain Status Record*

1578 Maintain a record of the status of all credentials issued.

1579 *ALI\_CM\_CSM#020 No stipulation*

1580 *ALI\_CM\_CSM#030 No stipulation*

1581 *ALI\_CM\_CSM#040 Status Information Availability*

1582 Provide, with 95% availability, a secure automated mechanism to allow relying parties to  
1583 determine credential status and authenticate the Claimant's identity.

1584

1585 **5.1.6 Part F - Credential Verification/Authentication**

1586 These criteria apply to credential validation and identity authentication.

1587 **5.1.6.1 Assertion Security**

1588 An enterprise and its specified service must:

1589 *ALI\_CM\_ASS#010 Validation and Assertion Security*

1590 Provide validation of credentials to a Relying Party using a protocol that:

- 1591 a) requires authentication of the specified service or of the validation source;
- 1592 b) ensures the integrity of the authentication assertion;
- 1593 c) protects assertions against manufacture, modification and substitution, and
- 1594 secondary authenticators from manufacture;

1595 and which, specifically:

- 1596 d) creates assertions which are specific to a single transaction;
- 1597 e) where assertion references are used, generates a new reference whenever a new
- 1598 assertion is created;
- 1599 f) when an assertion is provided indirectly, either signs the assertion or sends it via a
- 1600 protected channel, using a strong binding mechanism between the secondary
- 1601 authenticator and the referenced assertion;
- 1602 g) requires the secondary authenticator to:
  - 1603 i) be signed when provided directly to Relying Party, or;
  - 1604 ii) have a minimum of 64 bits of entropy when provision is indirect (i.e.
  - 1605 through the credential user).

1606 *ALI\_CM\_ASS#015 No stipulation*

1607 *ALI\_CM\_ASS#018 No stipulation*

1608 *ALI\_CM\_ASS#020 No Post Authentication*

1609 *Not* authenticate credentials that have been revoked.

1610 *ALI\_CM\_ASS#030 Proof of Possession*

1611 Use an authentication protocol that requires the claimant to prove possession and control

1612 of the authentication token.

1613 *ALI\_CM\_ASS#035 Limit authentication attempts (*

1614 *Limit the number of failed authentication attempts to no more than 100 in any 30-day*

1615 *period.*

1616 *ALI\_CM\_ASS#040 Assertion Lifetime*

1617 Generate assertions so as to indicate and effect their expiration within:

- 1618 a) 12 hours after their creation, where the service shares a common internet domain
- 1619 with the Relying Party;



1620 b) five minutes after their creation, where the service does not share a common  
1621 internet domain with the Relying Party.

1622

1623 **5.1.6.2 Authenticator-generated challenges**

1624 No stipulation.

1625 **5.1.6.3 Multi-factor authentication**

1626 No stipulation.

1627 **5.1.6.4 Verifier's assertion schema**

1628 Note: Since assertions and related schema can be complex and may be modeled directly  
1629 on the needs and preferences of the participants, the details of such schema fall outside  
1630 the scope of the SAC's herein, which are expressed observing, insofar as is feasible, a  
1631 technology-agnostic policy. The following criteria, therefore, are perhaps more open to  
1632 variable conformity through their final implementation than are others in this document.

1633 These criteria are derived directly from NIST SP 800-63-2 and have been expressed in as  
1634 generic a manner as they can be.

1635 An enterprise and its specified service must:

1636 *ALI\_CM\_VAS#010 No stipulation*

1637 No stipulation.

1638 *ALI\_CM\_VAS#020 No stipulation*

1639 No stipulation.

1640 *ALI\_CM\_VAS#030 Assertion assurance level*

1641 Create assertions which, either explicitly or implicitly (using a mutually-agreed  
1642 mechanism), indicate the assurance level at which the initial authentication of the Subject  
1643 was made.

1644 *ALI\_CM\_VAS#040 No stipulation*

1645 No stipulation.

1646 *ALI\_CM\_VAS#050 No stipulation*

1647 No stipulation.

1648 *ALI\_CM\_VAS#060 No assertion manufacture/modification*

1649 Ensure that it is impractical to manufacture an assertion or assertion reference by using at  
1650 least one of the following techniques:

1651 a) Signing the assertion;

- 1652 b) Encrypting the assertion using a secret key shared with the RP;
- 1653 c) Creating an assertion reference which has a minimum of 64 bits of entropy;
- 1654 d) Sending the assertion over a protected channel during a mutually-authenticated  
1655 session.
- 1656 *ALI\_CM\_VAS#070 No stipulation*  
1657 No stipulation.
- 1658 *ALI\_CM\_VAS#080 Single-use assertions*  
1659 Limit to a single transaction the use of assertions which do not support proof of  
1660 ownership.
- 1661 *ALI\_CM\_VAS#090 Single-use assertion references*  
1662 Limit to a single transaction the use of assertion references.
- 1663 *ALI\_CM\_VAS#100 Bind reference to assertion*  
1664 Provide a strong binding between the assertion reference and the corresponding assertion,  
1665 based on integrity-protected (or signed) communications over which the Verifier has been  
1666 authenticated.
- 1667 *ALI\_CM\_VAS#110 Assertion expiration*  
1668 Set assertions to expire such that:
- 1669 a) those used outside of the internet domain of the Verifier become invalid 5 minutes  
1670 after their creation; or
- 1671 b) those used within a single internet domain become invalid 12 hours after their  
1672 creation (including assertions contained in or referenced by cookies).
- 1673

## 1674 5.2 Assurance Level 2

### 1675 5.2.1 Part A - Credential Operating Environment

1676 These criteria describe requirements for the overall operational environment in which  
1677 credential lifecycle management is conducted. The Common Organizational criteria  
1678 describe broad requirements. The criteria in this Part describe operational  
1679 implementation specifics.

1680 These criteria apply to passwords, as well as acceptable SAML assertions.

1681 The following three criteria are **MANDATORY** for all Services, Full or Component, and  
1682 are individually marked as such:

1683 AL2\_CM\_CPP#010, AL2\_CM\_CPP#030, AL2\_CM\_CTR#030.

#### 1684 5.2.1.1 Credential Policy and Practices

1685 These criteria apply to the policy and practices under which credentials are managed.

1686 An enterprise and its specified service must:

1687 *AL2\_CM\_CPP#010 Credential Policy and Practice Statement*

1688 **MANDATORY.**

1689 **Include in its Service Definition a description of the policy against which it issues**  
1690 **credentials and the corresponding practices it applies in their management. At a**  
1691 **minimum, the Credential Policy and Practice Statement must specify:**

- 1692 a) **if applicable, any OIDs related to the Practice and Policy Statement;**
- 1693 b) **how users may subscribe to the service/apply for credentials and how users'**  
1694 **credentials will be delivered to them;**
- 1695 c) **how Subjects acknowledge receipt of tokens and credentials and what**  
1696 **obligations they accept in so doing (including whether they consent to**  
1697 **publication of their details in credential status directories);**
- 1698 d) **how credentials may be renewed, modified, revoked, and suspended,**  
1699 **including how requestors are authenticated or their identity re-proven;**
- 1700 e) **what actions a Subject must take to terminate a subscription;**
- 1701 f) **how records are retained and archived.**

1702 *AL2\_CM\_CPP#020 No stipulation*

1703 *AL2\_CM\_CPP#030 Management Authority*

1704 **MANDATORY.**

1705 **Have a nominated management body with authority and responsibility for**  
1706 **approving the Credential Policy and Practice Statement and for its implementation.**

1707 **5.2.1.2 Security Controls**

1708 An enterprise and its specified service must:

1709 *AL2\_CM\_CTR#010* **Withdrawn**

1710 **Withdrawn.**

1711 *AL2\_CM\_CTR#020* *Protocol threat risk assessment and controls*

1712 Account for at least the following protocol threats **in its risk assessment** and apply  
1713 **[omitted]** controls that **make the threats impractical and reduce them to acceptable risk**  
1714 **levels:**

- 1715 a) password guessing, such that **there are at least 24 bits of entropy to resist** an on-  
1716 line guessing attack against a selected **user/password**
- 1717 b) message replay **[Omitted];**
- 1718 c) **eavesdropping** **[Omitted];**
- 1719 d) **no stipulation;**
- 1720 e) **man-in-the-middle attack;**
- 1721 f) **session hijacking.**

1722 *AL2\_CM\_CTR#025* *Authentication protocols*

1723 **Apply only authentication protocols which, through a comparative risk assessment**  
1724 **which takes into account the target Assurance Level, are shown to have resistance to**  
1725 **attack at least as strong as that provided by commonly-recognized protocols such as:**

- 1726 a) **tunneling;**
- 1727 b) **zero knowledge-based;**
- 1728 c) **SAML [Omitted].**

1729 **Guidance:** Whilst many authentication protocols are well-established and may be  
1730 mandated or strongly-recommended by specific jurisdictions or sectors (e.g. standards  
1731 published by national SDOs or applicable to government-specific usage) this criterion  
1732 gives flexibility to advanced and innovative authentication protocols for which adequate  
1733 strength can be shown to be provided by the protocol applied with the specific service.

1734 *AL2\_CM\_CTR#028* *One-time passwords*

1735 **Use only one-time passwords which:**

- 1736 a) **are generated using an approved block-cipher or hash function to combine a**  
1737 **symmetric key, stored on the device, with a nonce;**
- 1738 b) **derive the nonce from a date and time, or a counter generated on the device;**
- 1739 c) **have a limited lifetime, in the order of minutes.**

1740 *AL2\_CM\_CTR#030* *System threat risk assessment and controls*

1741 **MANDATORY.**

1742 Account for the following system threats **in its risk assessment** and apply **[omitted]**  
1743 controls **that reduce them to acceptable risk levels:**

- 1744 a) the introduction of malicious code;

- 1745 b) compromised authentication arising from insider action;  
1746 c) out-of-band attacks by both users and system operators (e.g., the ubiquitous  
1747 shoulder-surfing);  
1748 d) spoofing of system elements/applications;  
1749 e) malfeasance on the part of Subscribers and Subjects;  
1750 f) **intrusions leading to information theft.**
- 1751 *AL2\_CM\_CTR#040 Specified Service's Key Management*  
1752 **Specify and observe procedures and processes for the generation, storage, and**  
1753 **destruction of its own cryptographic keys used for securing the specific service's**  
1754 **assertions and other publicized information. At a minimum, these should address:**
- 1755 a) **the physical security of the environment;**  
1756 b) **access control procedures limiting access to the minimum number of**  
1757 **authorized personnel;**  
1758 c) **public-key publication mechanisms;**  
1759 d) **application of controls deemed necessary as a result of the service's risk**  
1760 **assessment;**  
1761 e) **destruction of expired or compromised private keys in a manner that**  
1762 **prohibits their retrieval, or their archival in a manner that prohibits their**  
1763 **reuse;**  
1764 f) **applicable cryptographic module security requirements, quoting FIPS 140-2**  
1765 **[FIPS140-2] or equivalent, as established by a recognized national technical**  
1766 **authority.**

1767 **5.2.1.3 Storage of Long-term Secrets**

1768 *AL2\_CM\_STS#010 Withdrawn*  
1769 Withdrawn (AL2\_CO\_SCO#020 (a) & (b) enforce this requirement).

1770 **5.2.1.4 No stipulation**

1771 **5.2.1.5 No stipulation**

1772 *AL2\_CM\_OPN#010 Withdrawn*  
1773 Withdrawn – see AL2\_CM\_RNR#010.

1774

1775 **5.2.2 Part B - Credential Issuing**

1776 These criteria apply to the verification of the identity of the Subject of a credential and  
1777 with token strength and credential delivery mechanisms. They address requirements  
1778 levied by the use of various technologies to achieve Assurance Level 2.

1779 **5.2.2.1 Identity Proofing Policy**

1780 The specific service must show that it applies identity proofing policies and procedures  
1781 and that it retains appropriate records of identity proofing activities and evidence.

1782 The enterprise and its specified service must:

1783 *AL2\_CM\_IDP#010 Withdrawn*

1784 Withdrawn.

1785 *AL2\_CM\_IDP#020 Withdrawn*

1786 Withdrawn.

1787 *AL2\_CM\_IDP#030 Withdrawn*

1788 Withdrawn

1789 *AL2\_ID\_POL#010 Unique service identity*

1790 Ensure that a unique identity is attributed to the specific service, such that credentials  
1791 issued by it can be distinguishable from those issued by other services, including services  
1792 operated by the same enterprise.

1793 *AL2\_ID\_POL#020 Unique Subject identity*

1794 Ensure that each applicant's identity is unique within the service's community of Subjects  
1795 and uniquely associable with tokens and/or credentials issued to that identity.

1796 **Guidance:** Cf. AL2\_CM\_CRN#020 which expresses a very similar requirement.

1797 Although presenting repetition for a single provider, if the identity-proofing functions and  
1798 credential management functions are provided by separate CSPs, each needs to fulfill this  
1799 requirement.

1800 *AL2\_ID\_POL#030 Published Proofing Policy*

1801 **Make available the Identity Proofing Policy under which it verifies the identity of**  
1802 **applicants<sup>1</sup> in form, language, and media accessible to the declared community of**  
1803 **Users.**

1804 *AL2\_ID\_POL#040 Adherence to Proofing Policy*

1805 **Perform all identity proofing strictly in accordance with its published Identity**  
1806 **Proofing Policy.**

1807

---

<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.

1808 **5.2.2.2 Identity Verification**

1809 The enterprise or specific service:

1810 *AL2\_ID\_IDV#000 Identity Proofing classes*

- 1811 a) must include in its Service Definition at least one of the following classes of  
1812 identity proofing service, and;
- 1813 b) may offer any additional classes of identity proofing service it chooses, Subject to  
1814 the nature and the entitlement of the CSP concerned;
- 1815 c) must fulfill the applicable assessment criteria according to its choice of identity  
1816 proofing service, i.e. conform to at least one of the criteria sets defined in:
- 1817 i) §5.2.2.3, “[In-Person Public Identity Verification](#)”;
- 1818 ii) §5.2.2.4, “[Remote Public Identity Verification](#)”;
- 1819 iii) §5.2.2.5, “[Current Relationship Identity Verification](#)”;
- 1820 iv) §5.2.2.6, “[Affiliation Identity Verification](#)”;

1821 **although, in any of the above cases, the criteria defined in §5.2.2.7 may be**  
1822 **substituted for identity proofing where the Applicant already possesses a**  
1823 **recognized credential at Level 3 or 4.**

1824 *AL2\_ID\_IDV#010 - Identity Verification Measures*

1825 **For each identity proofing service offered (see above [*i.e.* AL2\_ID\_IDV#000]) justify**  
1826 **the identity verification measures applied by describing how these meet or exceed**  
1827 **the requirements of applicable policies, regulations, adopted standards and other**  
1828 **relevant conditions in order to maintain a level of rigour consistent with the**  
1829 **applicable Assurance Level.**

1830 **Guidance:** Although strict requirements for identity proofing and verification can be  
1831 defined, a real-world approach must account for instances where there is not 100%  
1832 certitude. To cope with this CSPs need to have a set of prescribed (through policy – see  
1833 AL2\_ID\_POL#030) and applied measures (see AL2\_ID\_POL#040) which observe  
1834 policy, identify the measures taken according to the degree of certitude determined by  
1835 each step in the verification process and what additional measures are taken. The CSP  
1836 must present a case which shows that their solution is sufficient to ensure that the basic  
1837 requirements of the applicable AL are met or exceeded.

1838 Note that in each set of proofing service criteria below there are criteria with specific  
1839 requirements for evidence checks and an additional criterion for ‘secondary’ checks, all of  
1840 which have an interplay with these overall requirements to have a policy and practice  
1841 statement and to demonstrate processes which sustain confidence that AL2 is being  
1842 achieved.

1843 **5.2.2.3 In-Person Public Identity Proofing**

1844 If the specific service offers in-person identity proofing to applicants with whom it has no  
1845 previous relationship, then it must comply with the criteria in this section.

1846 The enterprise or specified service must:

1847 *AL2\_ID\_IPV#010 Required evidence*

1848 **Ensure that the applicant is in possession of a primary Government Picture ID**  
1849 **document that bears a photographic image of the holder.**

1850 *AL2\_ID\_IPV#020 Evidence checks*

1851 **Have in place and apply processes which ensure that the presented document:**

- 1852 a) **appears to be a genuine document properly issued by the claimed issuing**  
1853 **authority and valid at the time of application;**  
1854 b) **bears a photographic image of the holder that matches that of the applicant;**  
1855 c) **provides all reasonable certainty that the identity exists and that it uniquely**  
1856 **identifies the applicant.**  
1857

1858 **5.2.2.4 Remote Public Identity Proofing**

1859 If the specific service offers remote identity proofing to applicants with whom it has no  
1860 previous relationship, then it must comply with the criteria in this section.

1861 An enterprise or specified service must:

1862 *AL2\_ID\_RPV#010 Required evidence*

1863 **Ensure that the applicant submits the references of and attests to current possession**  
1864 **of a primary Government Picture ID document, and one of:**

- 1865 a) **a second Government ID;**  
1866 b) **an employee or student ID number;**  
1867 c) **a financial account number (e.g., checking account, savings account, loan or**  
1868 **credit card) or;**  
1869 d) **a utility service account number (e.g., electricity, gas, or water) for an address**  
1870 **matching that in the primary document;**  
1871 e) **a telephone service account.**

1872 **Ensure that the applicant provides additional verifiable personal information that at**  
1873 **a minimum must include:**

- 1874 f) **a name that matches the referenced photo-ID;**  
1875 g) **date of birth and;**  
1876 h) **current address [omitted];**



1877 i) **for a telephone service account, the demonstrable ability to send or receive**  
1878 **messages at the phone number.**

1879

1880 **Additional information may be requested so as to ensure a unique identity, and**  
1881 **alternative information may be sought where the enterprise can show that it leads to**  
1882 **at least the same degree of certitude when verified.**

1883

1884 *AL2\_ID\_RPV#020 Evidence checks*

1885 **Inspection and analysis of records against the provided identity references with the**  
1886 **specified issuing authorities/institutions or through similar databases:**

- 1887 a) **the existence of such records with matching name and reference numbers;**  
1888 b) **corroboration of date of birth, current address of record, and other personal**  
1889 **information sufficient to ensure a unique identity;**  
1890 c) **dynamic verification of personal information previously provided by or**  
1891 **likely to be known only by the applicant;**  
1892 d) **for a telephone service account, confirmation that the phone number is**  
1893 **associated in Records with the Applicant's name and address of record and**  
1894 **by having the applicant demonstrate that they are able to send or receive**  
1895 **messages at the phone number.**

1896 **Confirm address, phone number or email of record by at least one of the following**  
1897 **means:**

- 1898 e) **RA sends notice to an address of record confirmed in the records check and**  
1899 **receives a mailed or telephonic reply from applicant;**  
1900 f) **RA issues credentials in a manner that confirms the address of record**  
1901 **supplied by the applicant, for example by requiring applicant to enter on-line**  
1902 **some information from a notice sent to the applicant;**  
1903 g) **RA issues credentials in a manner that confirms ability of the applicant to**  
1904 **receive telephone communications at telephone number or email at email**  
1905 **address associated with the applicant in records.**  
1906 h) **Any secret sent over an unprotected channel shall be reset upon first use and**  
1907 **shall be valid for a maximum lifetime of seven days.**

1908 **Additional checks should be performed so as to establish the uniqueness of the**  
1909 **claimed identity (see AL2\_ID\_SCV#010).**

1910 **Alternative checks may be performed where the enterprise can show that they lead**  
1911 **to at least the same degree of certitude (see AL2\_ID\_SCV#010).**

1912

1913 **5.2.2.5 Current Relationship Identity Proofing**

1914 If the specific service offers identity proofing to applicants with whom it has a current  
1915 relationship, then it must comply with the criteria in this section.

1916 The enterprise or specified service must:

1917 *AL2\_ID\_CRV#010 Required evidence*

1918 **Ensure that it has previously exchanged with the applicant a shared secret (e.g., a  
1919 PIN or password) that meets AL2 (or higher) entropy requirements<sup>2</sup>.**

1920 *AL2\_ID\_CRV#020 Evidence checks*

1921 **Ensure that it has:**

- 1922 a) **only issued the shared secret after originally establishing the applicant’s**  
1923 **identity:**  
1924 **i) with a degree of rigor equivalent to that required under either the AL2**  
1925 **(or higher) requirements for in-person or remote public verification;**  
1926 **or**  
1927 **ii) by complying with regulatory requirements effective within the**  
1928 **applicable jurisdiction which set forth explicit proofing requirements**  
1929 **which include a prior in-person appearance by the applicant and are**  
1930 **defined as meeting AL2 (or higher) requirements;**  
1931 b) **an ongoing business relationship sufficient to satisfy the enterprise of the**  
1932 **applicant’s continued personal possession of the shared secret.**  
1933

1934 **5.2.2.6 Affiliation Identity Proofing**

1935 If the specific service offers identity proofing to applicants on the basis of some form of  
1936 affiliation, then it must comply with the criteria in this section for the purposes of  
1937 establishing that affiliation, in addition to the previously stated requirements for the  
1938 verification of the individual’s identity.

1939 The enterprise or specified service must:

1940 *AL2\_ID\_AJV#000 Meet preceding criteria*

1941 **Meet all the criteria set out above, under §5.2.2.5, “[Current Relationship](#)  
1942 [Verification](#)”.**

1943 *AL2\_ID\_AJV#010 Required evidence*

1944 **Ensure that the applicant possesses:**

- 1945 a) **identification from the organization with which it is claiming affiliation;**

---

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

- 1946 b) **agreement from the organization that the applicant may be issued a**  
1947 **credential indicating that an affiliation exists.**

1948 *AL2\_ID\_AFV#020 Evidence checks*

1949 **Have in place and apply processes which ensure that the presented documents:**

- 1950 a) **each appear to be a genuine document properly issued by the claimed issuing**  
1951 **authorities and valid at the time of application;**  
1952 b) **refer to an existing organization with a contact address;**  
1953 c) **indicate that the applicant has some form of recognizable affiliation with the**  
1954 **organization;**  
1955 d) **appear to grant the applicant an entitlement to obtain a credential indicating**  
1956 **its affiliation with the organization.**  
1957

### 1958 **5.2.2.7 Identity-proofing based on Recognized Credentials**

1959 Where the Applicant already possesses recognized original credentials the CSP may  
1960 choose to accept the verified identity of the Applicant as a substitute for identity proofing,  
1961 subject to the following specific provisions. All other requirements of **Assurance Level**  
1962 **2** identity proofing must also be observed.

1963 *AL2\_ID\_IDC#010 Authenticate Original Credential*

1964 Prior to issuing any derived credential the original credential on which the identity-  
1965 proofing relies must be:

- 1966 a) **authenticated by a source trusted by the CSP as being valid and un-revoked;**  
1967 b) **issued at Assurance Level 3 or 4;**  
1968 c) **issued in the same name as that which the Applicant is claiming;**  
1969 d) **proven to be in the possession and under the control of the Applicant.**

1970 **Guidance:** This is the equivalent of recording the details of id documents provided  
1971 during (e.g.) face-face id-proofing.

1972 *AL2\_ID\_IDC#020 Record Original Credential*

1973 **Record the details of the original credential.**

1974 *AL2\_ID\_IDC#030 Issue Derived Credential*

1975 **Before issuing the derived credential ensure that:**

- 1976 a) **for in-person issuance, the claimant is the Applicant;**  
1977 b) **for remote issuance, token activation requires proof of possession of both the**  
1978 **derived token and the original Level 3 or Level 4 token.**  
1979

1980 **5.2.2.8 Secondary Identity-proofing**

1981 In each of the above cases, the enterprise or specified service must:

1982 *AL2\_ID\_SCV#010 Secondary checks*

1983 Have in place additional measures (e.g., require additional documentary evidence, delay  
1984 completion while out-of-band checks are undertaken) to deal with any anomalous  
1985 circumstances that can be reasonably anticipated (e.g., a legitimate and recent change of  
1986 address that has yet to be established as the address of record).

1987

1988 **5.2.2.9 Identity-proofing Records**

1989 The specific service must retain records of the identity proofing (verification) that it  
1990 undertakes and provide them to qualifying parties when so required.

1991 An enterprise or specified service must:

1992 *AL2\_ID\_VRC#010 Verification Records for Personal Applicants*

1993 **Log, taking account of all applicable legislative and policy obligations, a record of**  
1994 **the facts of the verification process, including a reference relating to the verification**  
1995 **processes and the date and time of verification.**

1996 **Guidance:** The facts of the verification process should include the specific record  
1997 information (source, unique reference, value/content) used in establishing the applicant's  
1998 identity, and will be determined by the specific processes used and documents accepted  
1999 by the CSP. The CSP need not retain these records itself if it uses a third-party service  
2000 which retains such records securely and to which the CSP has access when required, in  
2001 which case it must retain a record of the identity of the third-party service providing the  
2002 verification service or the location at which the (in-house) verification was performed.

2003 *AL2\_ID\_VRC#020 Verification Records for Affiliated Applicants*

2004 **In addition to the foregoing, log, taking account of all applicable legislative and**  
2005 **policy obligations, a record of the additional facts of the verification process**  
2006 **[omitted]. At a minimum, records of identity information must include:**

- 2007 a) **the Subject's<sup>3</sup> full name;**  
2008 b) **the Subject's current address of record;**  
2009 c) **the Subject's current telephone or email address of record;**  
2010 d) **the Subscriber's acknowledgement for issuing the Subject with a credential;**  
2011 e) **type, issuing authority, and reference number(s) of all documents checked in**  
2012 **the identity proofing process.**

---

<sup>3</sup> At this stage, the Subject is the entity acting in the role of Applicant, in anticipation of being issued a credential in which they shall be identified as the 'Subject' of that credential.

- 2013 *AL2\_ID\_VRC#025 Provide Subject identity records*  
2014 If required, provide to qualifying parties **records of identity proofing to the extent**  
2015 **permitted by applicable legislation and/or agreed by the Subscriber.**
- 2016 *AL2\_ID\_VRC#030 Record Retention*  
2017 **Either retain, securely, the record of the verification process for the duration of the**  
2018 **Subject account plus a further period sufficient to allow fulfillment of any period**  
2019 **required legally, contractually or by any other form of binding agreement or**  
2020 **obligation, or submit same record to a client CSP that has undertaken to retain the**  
2021 **record for the requisite period or longer.**
- 2022 *AL2\_CM\_IDP#040 Revision to Subject information*  
2023 Provide a means for Subjects to **securely** amend their stored information after  
2024 registration, **either by re-proving their identity, as in the initial registration process,**  
2025 **or by using their credentials to authenticate their revision.**
- 2026 **5.2.2.10 Credential Creation**
- 2027 These criteria define the requirements for creation of credentials whose highest use is at  
2028 AL2. Credentials/tokens that comply with the criteria stipulated at AL3 and higher are  
2029 also acceptable at AL2 and below.
- 2030 Note, however, that a token and credential required by a higher AL but created according  
2031 to these criteria may not necessarily provide that higher level of assurance for the claimed  
2032 identity of the Subject. Authentication can only be provided at the assurance level at  
2033 which the identity is proven.
- 2034 An enterprise and its specified service must:
- 2035 *AL2\_CM\_CRN#010 Authenticated Request*  
2036 Only accept a request to generate a credential and bind it to an identity if the source of the  
2037 request can be authenticated, **i.e., Registration Authority, as being authorized to**  
2038 **perform identity proofing at AL2 or higher.**
- 2039 *AL2\_CM\_CRN#020 Unique identity*  
2040 **Ensure that the identity which relates to a specific applicant is unique within the**  
2041 **specified service, including identities previously used and that are now cancelled,**  
2042 **other than its re-assignment to the same applicant.**
- 2043 **Guidance:** This requirement is intended to prevent identities that may exist in a Relying  
2044 Party's access control list from possibly representing a different physical person.  
2045 Cf. *AL2\_CM\_POL#020* which expresses a very similar requirement. Although  
2046 presenting repetition for a single provider, if the identity-proofing functions and  
2047 credential management functions are provided by separate CSPs, each needs to fulfill this  
2048 requirement.
- 2049 *AL2\_CM\_CRN#030 Credential uniqueness*

2050 Allow the Subject to select a credential (e.g., UserID) that is verified to be unique within  
2051 the specified service's community and assigned uniquely to a single identity Subject.

2052 *AL2\_CM\_CRN#035 Convey credential*

2053 Be capable of conveying the unique identity information associated with a credential to  
2054 Verifiers and Relying Parties.

2055 *AL2\_CM\_CRN#040 Token strength*

2056 Ensure that the single-factor token associated with the credential has the one of the  
2057 following set of characteristics:

2058 a) For a memorized secret, apply a rule-set such that there shall be a minimum of **24**  
2059 bits of entropy in the pin or pass-phrase;

2060 b) For a knowledge-based question, apply a rule-set such that there shall be:

2061 i) a minimum of **20** bits of entropy in the pin or pass-phrase OR;

2062 ii) a set of knowledge-based questions created by the user OR;

2063 iii) a set of knowledge-based questions selected by the user from a service-generated  
2064 list of at least **seven** questions.

2065

2066 Note – null or empty answers in either case above shall not be permitted.

2067 c) For a look-up token, apply a rule-set such that there shall be a minimum of **20**  
2068 bits of entropy in the secret phrase(s);

2069 d) For an out-of-band token, ensure that the token is uniquely addressable and  
2070 supports communication over a channel that is separate from the primary  
2071 channel for e-authentication;

2072 e) For a one-time-password device, generate one-time passwords using an  
2073 approved block cipher or hash function to combine a nonce and a symmetric  
2074 key;

2075 f) Use a cryptographic device validated at FIPS 140-2 Level 1 or higher.

2076

2077 **[Omitted]**

2078 *AL2\_CM\_CRN#050 One-time password strength*

2079 **Only allow password tokens that have a resistance to online guessing attack against**  
2080 **a selected user/password of at least 1 in  $2^{14}$  (16,384), accounting for state-of-the-art**  
2081 **attack strategies, and at least 10 bits of min-entropy** Error! Bookmark not defined.

2082 *AL2\_CM\_CRN#055 One-time password lifetime*

2083 **Set the minimum valid lifetime for the one-time password to a value commensurate**  
2084 **with service usage and in no case greater than fifteen minutes.**

2085 *AL2\_CM\_CRN#060 Software cryptographic token strength*

2086 **Ensure that software cryptographic keys stored on general-purpose devices are**  
2087 **protected by a key and cryptographic protocol that are evaluated against FIPS 140-2**  
2088 **[FIPS140-2] Level 1, or equivalent, as established by a recognized national technical**  
2089 **authority.**

2090 **[Omitted]**

2091 *AL2\_CM\_CRN#070 Hardware token strength*

2092 **Ensure that hardware tokens used to store cryptographic keys employ a**  
2093 **cryptographic module that is evaluated against FIPS 140-2 [FIPS140-2] Level 1 or**  
2094 **higher, or equivalent, as established by a recognized national technical authority.**

2095 **[Omitted]**

2096 *AL2\_CM\_CRN#075 No stipulation*

2097 *AL2\_CM\_CRN#080 No stipulation*

2098 *AL2\_CM\_CRN#090 Nature of Subject*

2099 **Record the nature of the Subject of the credential (which must correspond to the**  
2100 **manner of identity proofing performed), i.e., physical person, a named person acting**  
2101 **on behalf of a corporation or other legal entity, corporation or legal entity, or**  
2102 **corporate machine entity, in a manner that can be unequivocally associated with the**  
2103 **credential and the identity that it asserts. [Omitted]**

2104 *AL2\_CM\_CRN#095 Pseudonym's Real Identity*

2105 **If the credential is based upon a pseudonym this must be indicated in the credential**  
2106 **and a record of the real identity retained.**

#### 2107 **5.2.2.11 Subject Key Pair Generation**

2108 No stipulation.

#### 2109 **5.2.2.12 Credential Delivery**

2110 An enterprise and its specified service must:

2111 *AL2\_CM\_CRD#010 Notify Subject of Credential Issuance*

2112 **Notify the Subject of the credential's issuance and, if necessary, confirm the**  
2113 **Subject's contact information by:**

- 2114 a) **sending notice to the address of record confirmed during identity proofing**  
2115 **or;**  
2116 b) **issuing the credential(s) in a manner that confirms the address of record**  
2117 **supplied by the applicant during identity proofing or;**  
2118 c) **issuing the credential(s) in a manner that confirms the ability of the applicant**  
2119 **to receive telephone communications at a fixed-line telephone number or**  
2120 **postal address supplied by the applicant during identity proofing.**

2121

2122 *AL2\_CM\_CRD#015 Confirm Applicant's identity (in person)*

2123 **Prior to delivering the credential, require the Applicant to identify themselves in**  
2124 **person in any new transaction (beyond the first transaction or encounter) by either:**

2125 (a) using a temporary secret which was established during a prior  
2126 transaction or encounter, or sent to the Applicant's phone number, email  
2127 address, or physical address of record, or;

2128 (b) matching a biometric sample against a reference sample that was  
2129 recorded during a prior encounter.

2130 *AL2\_CM\_CRD#016 Confirm Applicant's identity (remotely)*

2131 **Prior to delivering the credential, require the Applicant to identify themselves in any**  
2132 **new electronic transaction (beyond the first transaction or encounter) by presenting**  
2133 **a temporary secret which was established during a prior transaction or encounter,**  
2134 **or sent to the Applicant's phone number, email address, or physical address of**  
2135 **record.**

2136

### 2137 **5.2.3 Part C - Credential Renewal and Re-issuing**

2138 These criteria apply to the renewal and re-issuing of credentials. They address  
2139 requirements levied by the use of various technologies to achieve Assurance Level 2.

#### 2140 **5.2.3.1 Renewal/Re-issuance Procedures**

2141 These criteria address general renewal and re-issuance functions, to be exercised as  
2142 specific controls in these circumstances while continuing to observe the general  
2143 requirements established for initial credential issuance.

2144 An enterprise and its specified service must:

2145 *AL2\_CM\_RNR#010 Changeable PIN/Password*

2146 Permit Subjects to change their [omitted] passwords, but employ reasonable practices  
2147 with respect to password resets and repeated password failures.

2148 *AL2\_CM\_RNR#020 Proof-of-possession on Renewal/Re-issuance*

2149 **Subjects wishing to change their passwords must demonstrate that they are in**  
2150 **possession of the unexpired current token prior to the CSP proceeding to renew or**  
2151 **re-issue it.**

2152 *AL2\_CM\_RNR#030 Renewal/Re-issuance limitations*

2153 a) not renew but may re-issue Passwords;

2154 b) neither renew nor re-issue expired tokens;

2155 c) neither set to default nor re-use any token secrets;



2156 **d) conduct all renewal / re-issuance interactions with the Subject over a**  
2157 **protected channel such as SSL/TLS.**

2158 **Guidance:** Renewal is considered as an extension of usability, whereas re-issuance  
2159 requires a change.

2160 *AL2\_CM\_RNR#040 No stipulation*

2161 **No stipulation.**

2162 *AL2\_CM\_RNR#050 Record Retention*

2163 **Retain, securely, the record of any renewal/re-issuance process for the duration of**  
2164 **the Subscriber's account plus a further period sufficient to allow fulfillment of any**  
2165 **period required legally, contractually or by any other form of binding agreement or**  
2166 **obligation, or submit same record to a client CSP that has undertaken to retain the**  
2167 **record for the requisite period or longer.**

2168

## 2169 **5.2.4 Part D - Credential Revocation**

2170 These criteria deal with credential revocation and the determination of the legitimacy of a  
2171 revocation request.

### 2172 **5.2.4.1 Revocation Procedures**

2173 These criteria address general revocation functions, such as the processes involved and  
2174 the basic requirements for publication.

2175 An enterprise and its specified service must:

2176 *AL2\_CM\_RVP#010 Revocation procedures*

2177 **a) State the conditions under which revocation of an issued credential may**  
2178 **occur;**

2179 **b) State the processes by which a revocation request may be submitted;**

2180 **c) State the persons and organizations from which a revocation request will be**  
2181 **accepted;**

2182 **d) State the validation steps that will be applied to ensure the validity (identity)**  
2183 **of the Revocant, and;**

2184 **e) State the response time between a revocation request being accepted and the**  
2185 **publication of revised certificate status.**

2186 *AL2\_CM\_RVP#020 Secure status notification*

2187 **Ensure that published credential status notification information can be relied upon**  
2188 **in terms of the enterprise of its origin (i.e., its authenticity) and its correctness (i.e.,**  
2189 **its integrity).**

2190 *AL2\_CM\_RVP#030 Revocation publication*

2191 **Unless the credential will expire automatically within 72 hours:**

2192 **Ensure that published credential status notification is revised within 72 hours of the**  
2193 **receipt of a valid revocation request, such that any subsequent attempts to use that**  
2194 **credential in an authentication shall be unsuccessful.**

2195 *AL2\_CM\_RVP#040 Verify revocation identity*

2196 **Establish that the identity for which a revocation request is received is one that was**  
2197 **issued by the specified service.**

2198 *AL2\_CM\_RVP#045 Notification of Revoked Credential*

2199 **When a verification / authentication request results in notification of a revoked**  
2200 **credential one of the following measures shall be taken:**

2201 **a) the confirmation message shall be time-stamped, or;**

2202 **b) the session keys shall expire with an expiration time no longer than that of**  
2203 **the applicable revocation list, or;**

2204 **c) the time-stamped message, binding, and credential shall all be signed by the**  
2205 **service.**

2206 *AL2\_CM\_RVP#050 Revocation Records*

2207 **Retain a record of any revocation of a credential that is related to a specific identity**  
2208 **previously verified, solely in connection to the stated credential. At a minimum,**  
2209 **records of revocation must include:**

2210 **a) the Revocant's full name;**

2211 **b) the Revocant's authority to revoke (e.g., Subscriber, the Subject themselves,**  
2212 **someone acting with the Subscriber's or the Subject's power of attorney, the**  
2213 **credential issuer, law enforcement, or other legal due process);**

2214 **c) the Credential Issuer's identity (if not directly responsible for the identity**  
2215 **proofing service);**

2216 **d) the identity associated with the credential (whether the Subject's name or a**  
2217 **pseudonym);**

2218 **e) the reason for revocation.**

2219 *AL2\_CM\_RVP#060 Record Retention*

2220 **Retain, securely, the record of the revocation process for the duration of the**  
2221 **Subscriber's account plus 7.5 years.**

#### 2222 **5.2.4.2 Verify Revocant's Identity**

2223 Revocation of a credential requires that the requestor and the nature of the request be  
2224 verified as rigorously as the original identity proofing. The enterprise should not act on a  
2225 request for revocation without first establishing the validity of the request (if it does not,  
2226 itself, determine the need for revocation).

2227 In order to do so, the enterprise and its specified service must:

2228 *AL2\_CM\_RVR#010 Verify revocation identity*  
2229 **Establish that the credential for which a revocation request is received was one that**  
2230 **was issued by the specified service, applying the same process and criteria as would**  
2231 **be applied to an original identity proofing.**

2232 *AL2\_CM\_RVR#020 Revocation reason*  
2233 **Establish the reason for the revocation request as being sound and well founded, in**  
2234 **combination with verification of the Revocant, according to AL2\_ID\_RVR#030,**  
2235 **AL2\_ID\_RVR#040, or AL2\_ID\_RVR#050.**

2236 *AL2\_CM\_RVR#030 Verify Subscriber as Revocant*  
2237 **When the Subscriber or Subject seeks revocation of the Subject's credential, the**  
2238 **enterprise must:**

- 2239 a) **if in person, require presentation of a primary Government Picture ID**
- 2240 **document that shall be electronically verified by a record check against the**
- 2241 **provided identity with the specified issuing authority's records;**
- 2242 b) **if remote:**
  - 2243 i. **electronically verify a signature against records (if available),**
  - 2244 **confirmed with a call to a telephone number of record, or;**
  - 2245 ii. **authenticate an electronic request as being from the same Subscriber or**
  - 2246 **Subject, supported by a credential at Assurance Level 2 or higher.**

2247 *AL2\_CM\_RVR#040 CSP as Revocant*  
2248 **Where a CSP seeks revocation of a Subject's credential, the enterprise must**  
2249 **establish that the request is either:**

- 2250 a) **from the specified service itself, with authorization as determined by**
- 2251 **established procedures, or;**
- 2252 b) **from the client Credential Issuer, by authentication of a formalized request**
- 2253 **over the established secure communications network.**

2254 *AL2\_CM\_RVR#050 Verify Legal Representative as Revocant*  
2255 **Where the request for revocation is made by a law enforcement officer or**  
2256 **presentation of a legal document, the enterprise must:**

- 2257 a) **if in-person, verify the identity of the person presenting the request;**
- 2258 b) **if remote:**
  - 2259 i. **in paper/facsimile form, verify the origin of the legal document by a**
  - 2260 **database check or by telephone with the issuing authority, or;**
  - 2261 ii. **as an electronic request, authenticate it as being from a recognized**
  - 2262 **legal office, supported by a credential at Assurance Level 2 or higher.**

2264 **5.2.4.3 No stipulation**

2265 **5.2.4.4 Secure Revocation Request**

2266 This criterion applies when revocation requests must be communicated between remote  
2267 components of the service organization.

2268 An enterprise and its specified service must:

2269 *AL2\_CM\_SRR#010 Submit Request*

2270 Submit a request for the revocation to the Credential Issuer service (function), using a  
2271 secured network communication.

2272

2273 **5.2.5 Part E - Credential Status Management**

2274 These criteria deal with credential status management, such as the receipt of requests for  
2275 new status information arising from a new credential being issued or a revocation or other  
2276 change to the credential that requires notification. They also deal with the provision of  
2277 status information to requesting parties (Verifiers, Relying Parties, courts and others  
2278 having regulatory authority, etc.) having the right to access such information.

2279 **5.2.5.1 Status Maintenance**

2280 An enterprise and its specified service must:

2281 *AL2\_CM\_CSM#010 Maintain Status Record*

2282 Maintain a record of the status of all credentials issued.

2283 *AL2\_CM\_CSM#020 Validation of Status Change Requests*

2284 **Authenticate all requestors seeking to have a change of status recorded and**  
2285 **published and validate the requested change before considering processing the**  
2286 **request. Such validation should include:**

2287 a) **the requesting source as one from which the specified service expects to**  
2288 **receive such requests;**

2289 b) **if the request is not for a new status, the credential or identity as being one**  
2290 **for which a status is already held.**

2291 *AL2\_CM\_CSM#030 Revision to Published Status*

2292 **Process authenticated requests for revised status information and have the revised**  
2293 **information available for access within a period of 72 hours.**

2294 *AL2\_CM\_CSM#040 Status Information Availability*

2295 Provide, with 95% availability, a secure automated mechanism to allow relying parties to  
2296 determine credential status and authenticate the Claimant's identity.

2297 *AL2\_CM\_CSM#050 Inactive Credentials*

2298 **Disable any credential that has not been successfully used for authentication during**  
2299 **a period of 18 months.**

2300

## 2301 **5.2.6 Part F - Credential Verification/Authentication**

2302 These criteria apply to credential validation and identity authentication.

### 2303 **5.2.6.1 Assertion Security**

2304 An enterprise and its specified service must:

2305 *AL2\_CM\_ASS#010 Validation and Assertion Security*

2306 Provide validation of credentials to a Relying Party using a protocol that:

- 2307 a) requires authentication of the specified service, itself, or of the validation source;
- 2308 b) ensures the integrity of the authentication assertion;
- 2309 c) protects assertions against manufacture, modification, **substitution and**  
2310 **disclosure**, and secondary authenticators from manufacture, **capture and replay**;
- 2311 **d) uses approved cryptography techniques;**

2312 and which, specifically:

- 2313 e) creates assertions which are specific to a single transaction;
- 2314 f) where assertion references are used, generates a new reference whenever a new  
2315 assertion is created;
- 2316 g) when an assertion is provided indirectly, either signs the assertion or sends it via a  
2317 protected channel, using a strong binding mechanism between the secondary  
2318 authenticator and the referenced assertion;
- 2319 **h) send assertions either via a channel mutually-authenticated with the Relying**  
2320 **Party, or signed and encrypted for the Relying Party;**
- 2321 i) requires the secondary authenticator to:
  - 2322 i) be signed when provided directly to Relying Party, or;
  - 2323 ii) have a minimum of 64 bits of entropy when provision is indirect (i.e.  
2324 through the credential user);
  - 2325 **iii) be transmitted to the Subject through a protected channel which is**  
2326 **linked to the primary authentication process in such a way that**  
2327 **session hijacking attacks are resisted;**
  - 2328 **iv) not be subsequently transmitted over an unprotected channel or to an**  
2329 **unauthenticated party while it remains valid.**

2330 *AL2\_CM\_ASS#013 No Stipulation*

2331 *AL2\_CM\_ASS#015 No False Authentication*

2332 **Employ techniques which ensure that system failures do not result in ‘false positive**  
2333 **authentication’ errors.**

2334 *AL2\_CM\_ASS#020 No Post Authentication*

2335 *Not* authenticate credentials that have been revoked **unless the time of the transaction**  
2336 **for which verification is sought precedes the time of revocation of the credential.**

2337 **Guidance:** The purpose in this criterion is that, if a verification is intended to refer to the  
2338 status of a credential at a specific historical point in time, e.g. to determine whether the  
2339 Claimant was entitled to act as a signatory in a specific capacity at the time of the  
2340 transaction, this may be done. It is implicit in this thinking that both the request and the  
2341 response indicate the historical nature of the query and response; otherwise the default  
2342 time is 'now'. If no such service is offered then this criterion may simply be  
2343 'Inapplicable', for that reason.

2344 *AL2\_CM\_ASS#030 Proof of Possession*

2345 Use an authentication protocol that requires the claimant to prove possession and control  
2346 of the authentication token.

2347 *AL2\_CM\_ASS#035 Limit authentication attempts*

2348 **Unless the token authenticator has at least 64 bits of entropy,** limit the number of  
2349 failed authentication attempts to no more than 100 in any 30-day period.

2350 *AL2\_CM\_ASS#040 Assertion Lifetime*

2351 Generate assertions so as to indicate and effect their expiration:

- 2352 a) 12 hours after their creation, where the service shares a common internet domain  
2353 with the Relying Party;
- 2354 b) five minutes after their creation, where the service does not share a common  
2355 internet domain with the Relying Party.

#### 2356 **5.2.6.2 Authenticator-generated challenges**

2357 An enterprise and its specified service must:

2358 *AL2\_CM\_AGC#010 Entropy level*

2359 **Create authentication secrets to be used during the authentication exchange (i.e.**  
2360 **with out-of-band or cryptographic device tokens) with a degree of entropy**  
2361 **appropriate to the token type in question.**

#### 2362 **5.2.6.3 Multi-factor authentication**

2363 An enterprise and its specified service must:

2364 *AL2\_CM\_MFA#010 Permitted multi-factor tokens*

2365 **Require two tokens which, when used in combination within a single authentication**  
2366 **exchange, are acknowledged as providing an equivalence of AL2, as determined by a**  
2367 **recognized national technical authority.**

2368 **5.2.6.4 Verifier's assertion schema**

2369 Note: Since assertions and related schema can be complex and may be modeled directly  
2370 on the needs and preferences of the participants, the details of such schema fall outside  
2371 the scope of the SAC's herein, which are expressed observing, insofar as is feasible, a  
2372 technology-agnostic policy. The following criteria, therefore, are perhaps more open to  
2373 variable conformity through their final implementation than are others in this document.

2374 These criteria are derived directly from NIST SP 800-63-2 and have been expressed in as  
2375 generic a manner as they can be.

2376 *Editor's note: I have avoided reference to the RP here – I am concerned as to what the*  
2377 *SAC requires services to do, not who might be using their products. SAC do not refer to*  
2378 *RPs.*

2379 An enterprise and its specified service must:

2380 *AL2\_CM\_VAS#010 Approved cryptography*

2381 **Apply assertion protocols which use cryptographic techniques approved by a**  
2382 **national authority or other generally-recognized authoritative body.**

2383 *AL2\_CM\_VAS#020 No stipulation*

2384 No stipulation.

2385 *AL2\_CM\_VAS#030 Assertion assurance level*

2386 Create assertions which, either explicitly or implicitly (using a mutually-agreed  
2387 mechanism), indicate the assurance level at which the initial authentication of the Subject  
2388 was made.

2389 *AL2\_CM\_VAS#040 Notify pseudonyms*

2390 **Create assertions which indicate whether the Subscriber name in the credential**  
2391 **subject to verification is a pseudonym.**

2392 *AL2\_CM\_VAS#050 Specify recipient*

2393 **Create assertions which identify the intended recipient of the verification such that**  
2394 **the recipient may validate that it is intended for them.**

2395 *AL2\_CM\_VAS#060 No assertion manufacture/modification*

2396 Ensure that it is impractical to manufacture an assertion or assertion reference by using at  
2397 least one of the following techniques:

- 2398 a) Signing the assertion;  
2399 b) Encrypting the assertion using a secret key shared with the RP;  
2400 c) Creating an assertion reference which has a minimum of 64 bits of entropy;  
2401 d) Sending the assertion over a protected channel during a mutually-authenticated  
2402 session.

2403 *AL2\_CM\_VAS#070 Assertion protections*

- 2404 **Provide protection of assertion-related data such that:**
- 2405 a) **both assertions and assertion references are protected against capture and**  
2406 **re-use;**
- 2407 b) **assertions are also protected against redirection;**  
2408 [US / EZP800-63-2: §9.3.2.2.2]
- 2409 c) **assertions, assertion references and session cookies used for authentication**  
2410 **purposes, including any which are re-directed, are protected against session**  
2411 **hijacking, for at least the duration of their validity (see AL2\_CM\_VAS#110).**
- 2412 *AL2\_CM\_VAS#080 Single-use assertions*
- 2413 Limit to a single transaction the use of assertions which do not support proof of  
2414 ownership.
- 2415 *AL2\_CM\_VAS#090 Single-use assertion references*
- 2416 Limit to a single transaction the use of assertion references.
- 2417 *AL2\_CM\_VAS#100 Bind reference to assertion*
- 2418 Provide a strong binding between the assertion reference and the corresponding assertion,  
2419 based on integrity-protected (or signed) communications over which the Verifier has been  
2420 authenticated.
- 2421 *AL2\_CM\_VAS#110 Assertion expiration*
- 2422 Set assertions to expire such that:
- 2423 a) those used outside of the internet domain of the Verifier become invalid 5 minutes  
2424 after their creation; or
- 2425 b) those used within a single internet domain become invalid 12 hours after their  
2426 creation (including assertions contained in or referenced by cookies).
- 2427
- 2428



## 2429 5.3 Assurance Level 3

### 2430 5.3.1 Part A - Credential Operating Environment

2431 These criteria describe requirements for the overall operational environment in which  
2432 credential lifecycle management is conducted. The Common Organizational criteria  
2433 describe broad requirements. The criteria in this Part describe operational  
2434 implementation specifics.

2435 These criteria apply to one-time password devices and soft crypto applications protected  
2436 by passwords or biometric controls, as well as cryptographically-signed SAML  
2437 assertions.

2438 The following four criteria are **MANDATORY** for all Services, Full or Component, and  
2439 are individually marked as such:

2440 AL3\_CM\_CPP#010, AL3\_CM\_CPP#030, AL3\_CM\_CTR#030, AL3\_CM\_SER#010.

2441

#### 2442 5.3.1.1 Credential Policy and Practices

2443 These criteria apply to the policy and practices under which credentials are managed.

2444 An enterprise and its specified service must:

2445 *AL3\_CM\_CPP#010 Credential Policy and Practice Statement*

2446 **MANDATORY.**

2447 Include in its Service Definition a full description of the policy against which it issues  
2448 credentials and the corresponding practices it applies in their issuance. At a minimum,  
2449 the Credential Policy and Practice Statement must specify:

- 2450 a) if applicable, any OIDs related to the Credential Policy and Practice Statement;
- 2451 b) how users may subscribe to the service/apply for credentials and how the users'  
2452 credentials will be delivered to them;
- 2453 c) how Subscribers and/or Subjects acknowledge receipt of tokens and credentials  
2454 and what obligations they accept in so doing (including whether they consent to  
2455 publication of their details in credential status directories);
- 2456 d) how credentials may be renewed, modified, revoked, and suspended, including  
2457 how requestors are authenticated or their identity proven;
- 2458 e) what actions a Subscriber or Subject must take to terminate a subscription;
- 2459 f) how records are retained and archived.

2460 *AL3\_CM\_CPP#020 No stipulation*

2461 *AL3\_CM\_CPP#030 Management Authority*

2462 **MANDATORY.**

2463 Have a nominated or appointed high-level management body with authority and  
2464 responsibility for approving the Certificate Policy and Certification Practice Statement,  
2465 including ultimate responsibility for their proper implementation.

2466

### 2467 **5.3.1.2 Security Controls**

2468 *AL3\_CM\_CTR#010* **Withdrawn**

2469 *AL3\_CM\_CTR#020* *Protocol threat risk assessment and controls*

2470 Account for at least the following protocol threats in its risk assessment and apply  
2471 controls that **make the threats impractical** and reduce them to acceptable risk levels:

- 2472 a) password guessing, such that **[Omitted]** the resistance to an on-line guessing  
2473 attack against a selected user/password **is at least 1 in 2<sup>14</sup> (16,384)**;
- 2474 b) message replay**[Omitted]**;
- 2475 c) eavesdropping**[Omitted]**;
- 2476 **d) relying party (verifier) impersonation****[Omitted]**;
- 2477 e) man-in-the-middle attack;
- 2478 **f) session hijacking****[Omitted]**.

2479 **The above list shall not be considered to be a complete list of threats to be addressed**  
2480 **by the risk assessment.**

2481 *AL3\_CM\_CTR#025* *Permitted authentication protocols*

2482 **For non-PKI credentials**, **apply only** authentication protocols **which, through a**  
2483 **comparative risk assessment which takes into account the target Assurance Level, are**  
2484 **shown to have resistance to attack at least as strong as that provided by commonly-**  
2485 **recognized protocols such as:**

- 2486 d) tunneling;
- 2487 e) zero knowledge-based;
- 2488 f) SAML **[Omitted]**.

2489 *AL3\_CM\_CTR#028* *No Stipulation*

2490 *AL3\_CM\_CTR#030* *System threat risk assessment and controls*

2491 **MANDATORY.**

2492 Account for the following system threats in its risk assessment and apply controls that  
2493 reduce them to acceptable risk levels:

- 2494 a) the introduction of malicious code;
- 2495 b) compromised authentication arising from insider action;
- 2496 c) out-of-band attacks by both users and system operators (e.g., shoulder-surfing);
- 2497 d) spoofing of system elements/applications;
- 2498 e) malfeasance on the part of Subscribers and Subjects;

2499 f) intrusions leading to information theft.

2500 The above list shall not be considered to be a complete list of threats to be addressed by  
2501 the risk assessment.

2502 *AL3\_CM\_CTR#040 Specified Service's Key Management*

2503 Specify and observe procedures and processes for the generation, storage, and destruction  
2504 of its own cryptographic keys used for securing the specific service's assertions and other  
2505 publicized information. At a minimum, these should address:

- 2506 a) the physical security of the environment;
- 2507 b) access control procedures limiting access to the minimum number of authorized  
2508 personnel;
- 2509 c) public-key publication mechanisms;
- 2510 d) application of controls deemed necessary as a result of the service's risk  
2511 assessment;
- 2512 e) destruction of expired or compromised private keys in a manner that prohibits  
2513 their retrieval or their archival in a manner that prohibits their reuse;
- 2514 f) applicable cryptographic module security requirements, quoting FIPS 140-2  
2515 [FIPS140-2] or equivalent, as established by a recognized national technical  
2516 authority.  
2517

### 2518 5.3.1.3 Storage of Long-term Secrets

2519 An enterprise and its specified service must:

2520 *AL3\_CM\_STS#010 Withdrawn*

2521 Withdrawn (AL3\_CO\_SCO#020 (a) & (b) enforce this requirement).

2522 *AL3\_CM\_STS#020 Stored Secret Encryption*

2523 **Encrypt such shared secret files so that:**

- 2524 a) **the encryption key for the shared secret file is encrypted under a key held in**  
2525 **a FIPS 140-2 [FIPS140-2] Level 2 or higher validated hardware or software**  
2526 **cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module,**  
2527 **or equivalent, as established by a recognized national technical authority;**
- 2528 b) **the shared secret file is decrypted only as immediately required for an**  
2529 **authentication operation;**
- 2530 c) **shared secrets are protected as a key within the boundary of a FIPS 140-2**  
2531 **Level 2 or higher validated hardware cryptographic module or any FIPS**  
2532 **140-2 Level 3 or 4 cryptographic module and are not exported from the**  
2533 **module in plain text, or equivalent, as established by a recognized national**  
2534 **technical authority;**
- 2535 d) **shared secrets are split by an "n from m" cryptographic secret sharing**  
2536 **method.**  
2537

2538 **5.3.1.4 Security-relevant Event (Audit) Records**

2539 These criteria describe the need to provide an auditable log of all events that are pertinent  
2540 to the correct and secure operation of the service. The common organizational criteria  
2541 applying to provision of an auditable log of all security-related events pertinent to the  
2542 correct and secure operation of the service must also be considered carefully. These  
2543 criteria carry implications for credential management operations.

2544 In the specific context of a certificate management service, an enterprise and its specified  
2545 service must:

2546 *AL3\_CM\_SER#010 Security event logs*

2547 **MANDATORY**, to the extent that the sub-items relate to the scope of service.

2548 Ensure that such audit records include:

- 2549 a) the identity of the point of registration (irrespective of whether internal or  
2550 outsourced);  
2551 b) generation of the Subject's keys or the evidence that the Subject was in possession of  
2552 both parts of their own key-pair;  
2553 c) generation of the Subject's certificate;  
2554 d) dissemination of the Subject's certificate;  
2555 e) any revocation or suspension associated with the Subject's certificate.  
2556

2557 **5.3.1.5 Subject options**

2558 *AL3\_CM\_OPN#010 Withdrawn*

2559 Withdrawn – see AL3\_CM\_RNR#010.

2560

2561 **5.3.2 Part B - Credential Issuing**

2562 These criteria apply to the verification of the identity of the Subject of a credential and  
2563 with token strength and credential delivery mechanisms. They address requirements  
2564 levied by the use of various technologies to achieve Assurance Level 3.

2565 **5.3.2.1 Identity Proofing Policy**

2566 The specific service must show that it applies identity proofing policies and procedures  
2567 and that it retains appropriate records of identity proofing activities and evidence.

2568 The enterprise and its specified service must:

2569 *AL3\_CM\_IDP#010 Withdrawn*

2570 Withdrawn.

2571 *AL3\_CM\_IDP#020 Withdrawn*

- 2572 Withdrawn.
- 2573 *AL3\_CM\_IDP#030 Withdrawn*
- 2574 Withdrawn.
- 2575 *AL3\_ID\_POL#010 Unique service identity*
- 2576 Ensure that a unique identity is attributed to the specific service, such that credentials
- 2577 issued by it can be distinguishable from those issued by other services, including services
- 2578 operated by the same enterprise.
- 2579 *AL3\_ID\_POL#020 Unique Subject identity*
- 2580 Ensure that each applicant's identity is unique within the service's community of Subjects
- 2581 and uniquely associable with tokens and/or credentials issued to that identity.
- 2582 **Guidance:** Cf. AL3\_CM\_CRN#020 which expresses a very similar requirement.
- 2583 Although presenting repetition for a single provider, if the identity-proofing functions and
- 2584 credential management functions are provided by separate CSPs, each needs to fulfill this
- 2585 requirement.
- 2586 *AL3\_ID\_POL#030 Published Proofing Policy*
- 2587 Make available the Identity Proofing Policy under which it verifies the identity of
- 2588 applicants<sup>4</sup> in form, language, and media accessible to the declared community of Users.
- 2589 *AL3\_ID\_POL#040 Adherence to Proofing Policy*
- 2590 Perform all identity proofing strictly in accordance with its published Identity Proofing
- 2591 Policy, **through application of the procedures and processes set out in its Identity**
- 2592 **Proofing Practice Statement (IdPPS).**
- 2593
- 2594 **5.3.2.2 Identity Proofing**
- 2595 The enterprise or specific service:
- 2596 *AL3\_ID\_IDV#000 Identity Proofing classes*
- 2597 a) must include in its Service Definition at least one of the following classes of
- 2598 identity proofing services, and;
- 2599 b) may offer any additional classes of identity proofing service it chooses, Subject to
- 2600 the nature and the entitlement of the CSP concerned;
- 2601 c) must fulfill the applicable assessment criteria according to its choice of identity
- 2602 proofing service, i.e. conform to at least one of the criteria sets defined in:

---

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

- 2603 i) §5.3.2.3, “[In-Person Public Identity Verification](#)”;
- 2604 ii) §5.3.2.4, “[Remote Public Identity Verification](#)”;
- 2605 iii) §5.2.2.5, “[Current Relationship Identity Verification](#)”;
- 2606 iv) §5.3.2.6, “[Affiliation Identity Verification](#)”;

2607 although, in any of the above cases, the criteria defined in §5.3.2.7 may be  
2608 substituted for identity proofing where the Applicant already possesses a  
2609 recognized credential at **Level 4**

2610

#### 2611 *AL3\_ID\_IDV#010 - Identity Verification Measures*

2612 For each identity proofing service offered (see above [*i.e.* A32\_IDV#000]) justify the  
2613 identity verification measures **described in its IdPPS (see AL3\_ID\_POL#040)** by  
2614 describing how these meet or exceed the requirements of applicable policies, regulations,  
2615 adopted standards and other relevant conditions in order to maintain a level of rigour  
2616 consistent with the AL3.

2617 **Guidance:** Although strict requirements for identity proofing and verification can be  
2618 defined, a real-world approach must account for instances where there is not 100%  
2619 certitude. To cope with this CSPs need to have a set of prescribed (through policy – see  
2620 AL3\_ID\_POL#030) and applied measures (see AL3\_ID\_POL#040) which observe  
2621 policy, identify the measures taken according to the degree of certitude determined by  
2622 each step in the verification process and what additional measures are taken. The CSP  
2623 must present a case which shows that their solution is sufficient to ensure that the basic  
2624 requirements of the applicable AL are met or exceeded.

2625 Note that in each set of proofing service criteria below there are criteria with specific  
2626 requirements for evidence checks and an additional criterion for ‘secondary’ checks, all of  
2627 which have an interplay with these overall requirements to have a policy and practice  
2628 statement and to demonstrate processes which sustain confidence that AL3 is being  
2629 achieved.

#### 2630 **5.3.2.3 In-Person Public Identity Proofing**

2631 A specific service that offers identity proofing to applicants with whom it has no previous  
2632 relationship must comply with the criteria in this section.

2633 The enterprise or specified service must:

2634 *AL3\_ID\_IPV#010 Required evidence*

2635 Ensure that the applicant is in possession of a primary Government Picture ID document  
2636 that bears a photographic image of the holder.

2637 *AL3\_ID\_IPV#020 Evidence checks*

2638 **Have in place and apply processes which ensure** that the presented document:

- 2639 a) appears to be a genuine document properly issued by the claimed issuing  
2640 authority and valid at the time of application;  
2641 b) bears a photographic image of the holder that matches that of the applicant;  
2642 c) **is electronically verified by a record check with the specified issuing**  
2643 **authority or through similar databases that:**  
2644 i) **establishes the existence of such records with matching name and**  
2645 **reference numbers;**  
2646 ii) **corroborates date of birth, current address of record, and other**  
2647 **personal information sufficient to ensure a unique identity;**  
2648 d) provides all reasonable certainty that the identity exists and that it uniquely  
2649 identifies the applicant.  
2650

#### 2651 **5.3.2.4 Remote Public Identity Proofing**

2652 A specific service that offers remote identity proofing to applicants with whom it has no  
2653 previous relationship must comply with the criteria in this section.

2654 The enterprise or specified service must:

2655 *AL3\_ID\_RPV#010 Required evidence*

2656 Ensure that the applicant submits the references of and attests to current possession of a  
2657 primary Government Picture ID document, and one of:

- 2658 a) a second Government ID;  
2659 b) an employee or student ID number;  
2660 c) a financial account number (e.g., checking account, savings account, loan, or  
2661 credit card), or;  
2662 d) a utility service account number (e.g., electricity, gas, or water) for an address  
2663 matching that in the primary document.

2664 Ensure that the applicant provides additional verifiable personal information that at a  
2665 minimum must include:

- 2666 e) a name that matches the referenced photo-ID;  
2667 f) date of birth;  
2668 g) current address [omitted].

2669 Additional information may be requested so as to ensure a unique identity, and alternative  
2670 information may be sought where the enterprise can show that it leads to at least the same  
2671 degree of certitude when verified.

2672 *AL3\_ID\_RPV#020 Evidence checks*

2673 **Electronically verify by a record check** against the provided identity references with the  
2674 specified issuing authorities/institutions or through similar databases:

- 2675 a) the existence of such records with matching name and reference numbers;

- 2676 b) corroboration of date of birth, current address of record, **or personal telephone**  
2677 **number**, and other personal information sufficient to ensure a unique identity;  
2678 c) dynamic verification of personal information previously provided by or likely to  
2679 be known only by the applicant  
2680 d) for a telephone service account, confirmation that the phone number is associated  
2681 in Records with the Applicant's name and address of record and by having the  
2682 applicant demonstrate that they are able to send or receive messages at the phone  
2683 number.

2684 Confirm address, phone number or email of record by at least one of the following  
2685 means:

- 2686 e) RA sends notice to an address of record confirmed in the records check and  
2687 receives a mailed or telephonic reply from applicant;  
2688 f) RA issues credentials in a manner that confirms the address of record supplied by  
2689 the applicant, for example by requiring applicant to enter on-line some  
2690 information from a notice sent to the applicant;  
2691 g) RA issues credentials in a manner that confirms ability of the applicant to receive  
2692 telephone communications at telephone number or email at email address  
2693 associated with the applicant in records.  
2694 h) Any secret sent over an unprotected channel shall be reset upon first use and shall  
2695 be valid for a maximum lifetime of seven days.  
2696

2697 Additional checks should be performed so as to establish the uniqueness of the claimed  
2698 identity (see AL3\_ID\_SCV#010).

2699 Alternative checks may be performed where the enterprise can show that they lead to at  
2700 least the same degree of certitude (see AL3\_ID\_SCV#010)..

### 2701 5.3.2.5 Current Relationship Identity Proofing

2702 If the specific service offers identity proofing to applicants with whom it has a current  
2703 relationship, then it must comply with the criteria in this section.

2704 The enterprise or specified service must:

2705 *AL3\_ID\_CRV#010 Required evidence*

2706 Ensure that it has previously exchanged with the applicant a shared secret (e.g., a PIN or  
2707 password) that meets AL3 (or higher) entropy requirements<sup>5</sup>.

2708 *AL3\_ID\_CRV#020 Evidence checks*

2709 Ensure that it has:

- 2710 a) only issued the shared secret after originally establishing the applicant's identity:

---

<sup>5</sup> Refer to NIST SP 800-63 "Appendix A: Estimating Entropy and Strength" or similar recognized sources of such information.



- 2711           iii) with a degree of rigor equivalent to that required under either the AL3 (or  
2712           higher) requirements for in-person or remote public verification; or  
2713           iv) by complying with regulatory requirements effective within the applicable  
2714           jurisdiction which set forth explicit proofing requirements which include a  
2715           prior in-person appearance by the applicant and are defined as meeting AL3  
2716           (or higher) requirements;
- 2717           a) an ongoing business relationship sufficient to satisfy the enterprise of the  
2718           applicant's continued personal possession of the shared secret.

#### 2719   **5.3.2.6   Affiliation Identity Proofing**

2720   A specific service that offers identity proofing to applicants on the basis of some form of  
2721   affiliation must comply with the criteria in this section to establish that affiliation and  
2722   with the previously stated requirements to verify the individual's identity.

2723   The enterprise or specified service must:

2724   *AL3\_ID\_AFV#000   Meet preceding criteria*

2725   Meet all the criteria set out above, under §5.3.2.4, "[Remote Public Identity](#)  
2726   [Verification](#)".

2727   *AL3\_ID\_AFV#010   Required evidence*

2728   Ensure that the applicant possesses:

- 2729   a)    identification from the organization with which it is claiming affiliation;  
2730   b)    agreement from the organization that the applicant may be issued a credential  
2731        indicating that an affiliation exists.

2732   *AL3\_ID\_AFV#020   Evidence checks*

2733   Have in place and apply processes which ensure that the presented documents:

- 2734   a)    each appear to be a genuine document properly issued by the claimed issuing  
2735        authorities and valid at the time of application;  
2736   b)    refer to an existing organization with a contact address;  
2737   c)    indicate that the applicant has some form of recognizable affiliation with the  
2738        organization;  
2739   d)    appear to grant the applicant an entitlement to obtain a credential indicating an  
2740        affiliation with the organization.

2741

#### 2742   **5.3.2.7   Identity-proofing based on Recognized Credentials**

2743   Where the Applicant already possesses recognized original credentials the CSP may  
2744   choose to accept the verified identity of the Applicant as a substitute for identity proofing,  
2745   subject to the following specific provisions. All other requirements of Assurance Level 3  
2746   identity proofing must also be observed.

2747 *AL3\_ID\_IDC#010 Authenticate Original Credential*

2748 Prior to issuing any derived credential the original credential on which the identity-  
2749 proofing relies must be:

- 2750 a) authenticated by a source trusted by the CSP as being valid and un-revoked;
- 2751 b) issued at **Assurance Level 4**;
- 2752 c) issued in the same name as that which the Applicant is claiming;
- 2753 d) proven to be in the possession and under the control of the Applicant.

2754 **Guidance:** This is the equivalent of recording the details of id documents provided  
2755 during (e.g.) face-face id-proofing.

2756 *AL3\_ID\_IDC#020 Record Original Credential*

2757 Record the details of the original credential.

2758 *AL3\_ID\_IDC#030 Issue Derived Credential*

2759 Before issuing the derived credential ensure that:

- 2760 a) for in-person issuance, the claimant is the Applicant;
- 2761 b) for remote issuance, token activation requires proof of possession of both the  
2762 derived token and the original **Level 4** token.

2763

2764 **5.3.2.8 Secondary Identity-proofing**

2765 In each of the above cases, the enterprise or specified service must also meet the  
2766 following criteria:

2767 *AL3\_ID\_SCV#010 Secondary checks*

2768 Have in place additional measures (e.g., require additional documentary evidence, delay  
2769 completion while out-of-band checks are undertaken) to deal with any anomalous  
2770 circumstance that can reasonably be anticipated (e.g., a legitimate and recent change of  
2771 address that has yet to be established as the address of record).

2772 **5.3.2.9 Identity-proofing Records**

2773 The specific service must retain records of the identity proofing (verification) that it  
2774 undertakes and provide them to qualifying parties when so required.

2775 The enterprise or specified service must:

2776 *AL3\_ID\_VRC#010 Verification Records for Personal Applicants*

2777 Log, taking account of all applicable legislative and policy obligations, a record of the  
2778 facts of the verification process **and the identity of the registrar**, including a reference  
2779 relating to the verification processes and the date and time of verification.

2780 **Guidance:** The facts of the verification process should include the specific record  
2781 information (source, unique reference, value/content) used in establishing the applicant's

2782 identity, and will be determined by the specific processes used and documents accepted  
2783 by the CSP. The CSP need not retain these records itself if it uses a third-party service  
2784 which retains such records securely and to which the CSP has access when required, in  
2785 which case it must retain a record of the identity of the third-party service providing the  
2786 verification service or the location at which the (in-house) verification was performed.

2787 *AL3\_ID\_VRC#020 Verification Records for Affiliated Applicants*

2788 In addition to the foregoing, log, taking account of all applicable legislative and policy  
2789 obligations, a record of the additional facts of the verification process [omitted]. At a  
2790 minimum, records of identity information must include:

- 2791 a) the 'full name;
- 2792 b) the Subject's<sup>6</sup> current address of record;
- 2793 c) the Subject's current telephone or email address of record;
- 2794 d) the Subject's acknowledgement of issuing the Subject with a credential;
- 2795 e) type, issuing authority, and reference number(s) of all documents checked in the  
2796 identity proofing process;
- 2797 **f) where required, a telephone or email address for related contact and/or**  
2798 **delivery of credentials/notifications.**

2799 *AL3\_ID\_VRC#025 Provide Subject Identity Records*

2800 If required, provide to qualifying parties records of identity proofing to the extent  
2801 permitted by applicable legislation and/or agreed by the Subscriber.

2802 *AL3\_ID\_VRC#030 Record Retention*

2803 Either retain, securely, the record of the verification/revocation process for the duration of  
2804 the Subject account plus a further period sufficient to allow fulfillment of any period  
2805 required legally, contractually or by any other form of binding agreement or obligation ,  
2806 or submit the same record to a client CSP that has undertaken to retain the record for the  
2807 requisite period or longer.

2808 *AL3\_CM\_IDP#040 Revision to Subject information*

2809 Provide a means for Subjects to securely amend their stored information after  
2810 registration, either by re-proving their identity as in the initial registration process or by  
2811 using their credentials to authenticate their revision. **Successful revision must, where**  
2812 **necessary, instigate the re-issuance of the credential.**

2813

---

<sup>6</sup> At this stage, the Subject is the entity acting in the role of Applicant, in anticipation of being issued a credential in which they shall be identified as the 'Subject' of that credential.

2814 **5.3.2.10 Credential Creation**

2815 These criteria define the requirements for creation of credentials whose highest use is  
2816 AL3. Any credentials/tokens that comply with the criteria stipulated at AL4 are also  
2817 acceptable at AL3 and below.

2818 Note, however, that a token and credential type required by a higher AL but created  
2819 according to these criteria may not necessarily provide that higher level of assurance for  
2820 the claimed identity of the Subject. Authentication can only be provided at the assurance  
2821 level at which the identity is proven.

2822 An enterprise and its specified service must:

2823 *AL3\_CM\_CRN#010 Authenticated Request*

2824 Only accept a request to generate a credential and bind it to an identity if the source of the  
2825 request, i.e., Registration Authority, can be authenticated as being authorized to perform  
2826 identity proofing at AL3 or higher.

2827 *AL3\_CM\_CRN#020 Unique identity*

2828 Ensure that the identity which relates to a specific applicant is unique within the specified  
2829 service, including identities previously used and that are now cancelled other than its re-  
2830 assignment to the same applicant.

2831 **Guidance:** This requirement is intended to prevent identities that may exist in a Relying  
2832 Party's access control lists from possibly representing a different physical person.

2833 Cf. AL3\_CM\_POL#020 which expresses a very similar requirement. Although  
2834 presenting repetition for a single provider, if the identity-proofing functions and  
2835 credential management functions are provided by separate CSPs, each needs to fulfill this  
2836 requirement.

2837 *AL3\_CM\_CRN#030 Credential uniqueness*

2838 Allow the Subject to select a credential (e.g., UserID) that is verified to be unique within  
2839 the specified service's community and assigned uniquely to a single identity Subject.

2840 *AL3\_CM\_CRN#035 Convey credential*

2841 Be capable of conveying the unique identity information associated with a credential to  
2842 Verifiers and Relying Parties.

2843 *AL3\_CM\_CRN#040 Token strength*

2844 **Not use PIN/password tokens.**

2845 *AL3\_CM\_CRN#050 One-time password strength*

2846 Only allow one-time password tokens that:

- 2847 a) **depend on a symmetric key stored on a personal hardware device evaluated**  
2848 **against FIPS 140-2 [FIPS140-2] Level 1 or higher, or equivalent, as**  
2849 **established by a recognized national technical authority;**  
2850 b) **permit at least 10<sup>6</sup> possible password values;**

2851 **c) require password or biometric activation by the Subject.**

2852 *AL3\_CM\_CRN#055 No stipulation*

2853 *AL3\_CM\_CRN#060 Software cryptographic token strength*

2854 Ensure that software cryptographic keys stored on general-purpose devices:

2855 a) are protected by a key and cryptographic protocol that are evaluated against  
2856 FIPS 14-2 [FIPS140-2] Level 1, or equivalent, as established by a recognized  
2857 national technical authority;

2858 **b) require password or biometric activation by the Subject or employ a**  
2859 **password protocol when being used for authentication;**

2860 **c) erase any unencrypted copy of the authentication key after each**  
2861 **authentication.**

2862 *AL3\_CM\_CRN#070 Hardware token strength*

2863 Ensure that hardware tokens used to store cryptographic keys:

2864 a) employ a cryptographic module that is evaluated against FIPS 140-2 [FIPS140-2]  
2865 Level 1 or higher, or equivalent, as established by a recognized national technical  
2866 authority;

2867 **b) require password or biometric activation by the Subject or also employ a**  
2868 **password when being used for authentication;**

2869 **c) erase any unencrypted copy of the authentication key after each**  
2870 **authentication.**

2871 *AL3\_CM\_CRN#075 No stipulation*

2872 *AL3\_CM\_CRN#080 Binding of key*

2873 **If the specified service generates the Subject's key pair, that the key generation**  
2874 **process securely and uniquely binds that process to the certificate generation and**  
2875 **maintains at all times the secrecy of the private key, until it is accepted by the**  
2876 **Subject.**

2877 *AL3\_CM\_CRN#090 Nature of Subject*

2878 Record the nature of the Subject of the credential (which must correspond to the manner  
2879 of identity proofing performed), i.e., private person, a named person acting on behalf of a  
2880 corporation or other legal entity, corporation or legal entity, or corporate machine entity,  
2881 in a manner that can be unequivocally associated with the credential and the identity that  
2882 it asserts.

2883 *AL3\_CM\_CRN#095 No stipulation*

2884 No stipulation

2885

2886 **5.3.2.11 Subject Key Pair Generation**

2887 An enterprise and its specified service must:

2888 *AL3\_CM\_SKP#010 Key generation by Specified Service*

2889 **If the specified service generates the Subject's keys:**

- 2890 a) **use a FIPS 140-2 [FIPS140-2] compliant algorithm, or equivalent, as**
- 2891 **established by a recognized national technical authority, that is recognized as**
- 2892 **being fit for the purposes of the service;**
- 2893 b) **only create keys of a key length and for use with a FIPS 140-2 [FIPS140-2]**
- 2894 **compliant public key algorithm, or equivalent, as established by a recognized**
- 2895 **national technical authority, recognized as being fit for the purposes of the**
- 2896 **service;**
- 2897 c) **generate and store the keys securely until delivery to and acceptance by the**
- 2898 **Subject;**
- 2899 d) **deliver the Subject's private key in a manner that ensures that the privacy of**
- 2900 **the key is not compromised and only the Subject has access to the private**
- 2901 **key.**

2902 *AL3\_CM\_SKP#020 Key generation by Subject*

2903 **If the Subject generates and presents its own keys, obtain the Subject's written**

2904 **confirmation that it has:**

- 2905 a) **used a FIPS 140-2 [FIPS140-2] compliant algorithm, or equivalent, as**
- 2906 **established by a recognized national technical authority, that is recognized as**
- 2907 **being fit for the purposes of the service;**
- 2908 b) **created keys of a key length and for use with a FIPS 140-2 [FIPS140-2]**
- 2909 **compliant public key algorithm, or equivalent, as established by a recognized**
- 2910 **national technical authority, recognized as being fit for the purposes of the**
- 2911 **service.**
- 2912

2913 **5.3.2.12 Credential Delivery**

2914 An enterprise and its specified service must:

2915 *AL3\_CM\_CRD#010, Notify Subject of Credential Issuance*

2916 **Notify the Subject of the credential's issuance and, if necessary, confirm Subject's contact**

2917 **information by:**

- 2918 a) **sending notice to the address of record confirmed during identity proofing, and**
- 2919 **either:**
- 2920 **i) issuing the credential(s) in a manner that confirms the address of**
- 2921 **record supplied by the applicant during identity proofing, or;**
- 2922 **ii) issuing the credential(s) in a manner that confirms the ability of the**
- 2923 **applicant to receive telephone communications at a phone number**

2924 **supplied by the applicant during identity proofing, while recording**  
2925 **the applicant's voice.**

2926 *AL3\_CM\_CRD#015 Confirm Applicant's identity (in person)*

2927 Prior to delivering the credential, require the Applicant to identify themselves in person in  
2928 any new transaction (beyond the first transaction or encounter) by either:

2929 (a) using a temporary secret which was established during **the** prior transaction or  
2930 encounter (**whilst ensuring that such temporary secrets are used only**  
2931 **once**), or sent to the Applicant's phone number, email address, or physical  
2932 address of record, or;

2933 (b) matching a biometric sample against a reference sample that was recorded  
2934 during a prior encounter.

2935 *AL3\_CM\_CRD#016 Confirm Applicant's identity (remotely)*

2936 Prior to delivering the credential, require the Applicant to identify themselves in any new  
2937 electronic transaction (beyond the first transaction or encounter) by presenting a  
2938 temporary secret which was established during a prior transaction or encounter, or sent to  
2939 the Applicant's phone number, email address, or physical address of record.

2940 *AL3\_CM\_CRD#017 Protected Issuance of Permanent Secrets (in person)*

2941 **Only issue permanent secrets if the CSP has:**

2942 (a) **loaded the secret itself onto the physical device, which was either:**

2943 **i) issued in-person to the Applicant, or;**

2944 **ii) delivered in a manner that confirms the address of record.**

2945 *AL3\_CM\_CRD#018 Protected Issuance of Permanent Secrets (remotely)*

2946 **Only issue permanent secrets within a protected session.**

2947 *AL3\_CM\_CRD#020 Subject's acknowledgement*

2948 **Receive acknowledgement of receipt of the credential before it is activated and its**  
2949 **directory status record is published (and thereby the subscription becomes active or**  
2950 **re-activated, depending upon the circumstances of issue).**

2951

### 2952 **5.3.3 Part C - Credential Renewal and Re-issuing**

2953 These criteria apply to the renewal and re-issuing of credentials. They address  
2954 requirements levied by the use of various technologies to achieve Assurance Level 3.

#### 2955 **5.3.3.1 Renewal/Re-issuance Procedures**

2956 These criteria address general renewal and re-issuance functions, to be exercised as  
2957 specific controls in these circumstances while continuing to observe the general  
2958 requirements established for initial credential issuance.

2959 An enterprise and its specified service must:

2960 *AL3\_CM\_RNR#010 Changeable PIN/Password*

2961 Permit Subjects to change **the passwords used to activate their credentials.**

2962 *AL3\_CM\_RNR#020 Proof-of-possession on Renewal/Re-issuance*

2963 Subjects wishing to change their passwords must demonstrate that they are in possession  
2964 of the unexpired current token prior to the CSP proceeding to renew or re-issue it.

2965 *AL3\_CM\_RNR#030 Renewal/Re-issuance limitations*

2966 a) **No stipulation;**

2967 b) **No stipulation;**

2968 c) **No stipulation;**

2969 **d)** conduct all renewal / re-issuance interactions with the Subject over a protected  
2970 channel such as SSL/TLS.

2971 **Guidance:** Renewal is considered as an extension of usability, whereas re-issuance  
2972 requires a change.

2973 *AL3\_CM\_RNR#040 No stipulation*

2974 No stipulation.

2975 *AL3\_CM\_RNR#050 Record Retention*

2976 Retain, securely, the record of any renewal/re-issuance process for the duration of the  
2977 Subscriber's account plus a further period sufficient to allow fulfillment of any period  
2978 required legally, contractually or by any other form of binding agreement or obligation, or  
2979 submit same record to a client CSP that has undertaken to retain the record for the  
2980 requisite period or longer.

2981

## 2982 **5.3.4 Part D - Credential Revocation**

2983 These criteria deal with credential revocation and the determination of the legitimacy of a  
2984 revocation request.

### 2985 **5.3.4.1 Revocation Procedures**

2986 These criteria address general revocation functions, such as the processes involved and  
2987 the basic requirements for publication.

2988 An enterprise and its specified service must:

2989 *AL3\_CM\_RVP#010 Revocation procedures*

2990 a) State the conditions under which revocation of an issued credential may occur;

2991 b) State the processes by which a revocation request may be submitted;



- 2992 c) State the persons and organizations from which a revocation request will be  
2993 accepted;
- 2994 d) State the validation steps that will be applied to ensure the validity (identity) of  
2995 the Revocant, and;
- 2996 e) State the response time between a revocation request being accepted and the  
2997 publication of revised certificate status.
- 2998 *AL3\_CM\_RVP#020 Secure status notification*  
2999 Ensure that published credential status notification information can be relied upon in  
3000 terms of the enterprise being its origin (i.e., its authenticity) and its correctness (i.e., its  
3001 integrity).
- 3002 *AL3\_CM\_RVP#030 Revocation publication*  
3003 **[Omitted]** Ensure that published credential status notification is revised within **24** hours  
3004 of the receipt of a valid revocation request, such that any subsequent attempts to use that  
3005 credential in an authentication shall be unsuccessful. **The nature of the revocation**  
3006 **mechanism shall be in accord with the technologies supported by the service.**
- 3007 *AL3\_CM\_RVP#040 Verify Revocation Identity*  
3008 Establish that the identity for which a revocation request is received is one that was  
3009 issued by the specified service.
- 3010 *AL3\_CM\_RVP#050 Revocation Records*  
3011 Retain a record of any revocation of a credential that is related to a specific identity  
3012 previously verified, solely in connection to the stated credential. At a minimum, records  
3013 of revocation must include:
- 3014 a) the Revocant's full name;  
3015 b) the Revocant's authority to revoke (e.g., Subscriber or the Subject themselves,  
3016 someone acting with the Subscriber's or the Subject's power of attorney, the  
3017 credential issuer, law enforcement, or other legal due process);  
3018 c) the Credential Issuer's identity (if not directly responsible for the identity  
3019 proofing service); **[Omitted]**  
3020 d) the reason for revocation.
- 3021 *AL3\_CM\_RVP#060 Record Retention*  
3022 Retain, securely, the record of the revocation process for **a period which is in**  
3023 **compliance with:**
- 3024 **a) the records retention policy required by AL3\_CM\_CPP#020, and;**  
3025 **b) applicable legislation;**  
3026 **and which, in addition, must be not less than** the duration of the Subscriber's account  
3027 plus 7.5 years.  
3028

3029 **5.3.4.2 Verify Revocant's Identity**

3030 Revocation of a credential requires that the requestor and the nature of the request be  
3031 verified as rigorously as the original identity proofing. The enterprise should not act on a  
3032 request for revocation without first establishing the validity of the request (if it does not,  
3033 itself, determine the need for revocation).

3034 In order to do so, the enterprise and its specified service must:

3035 *AL3\_CM\_RVR#010 Verify revocation identity*

3036 Establish that the credential for which a revocation request is received is one that was  
3037 initially issued by the specified service, applying the same process and criteria as would  
3038 be applied to an original identity proofing ensuring that the Subject of the credential is  
3039 uniquely identified.

3040 *AL3\_CM\_RVR#020 Revocation reason*

3041 Establish the reason for the revocation request as being sound and well founded, in  
3042 combination with verification of the Revocant, according to *AL3\_ID\_RVR#030*,  
3043 *AL3\_ID\_RVR#040*, or *AL3\_ID\_RVR#050*.

3044 *AL3\_CM\_RVR#030 Verify Subscriber as Revocant*

3045 When the Subscriber or Subject seeks revocation of the Subject's credential:

- 3046 a) if in-person, require presentation of a primary Government Picture ID document  
3047 that shall be electronically verified by a record check against the provided identity  
3048 with the specified issuing authority's records;  
3049 b) if remote:  
3050 i. electronically verify a signature against records (if available), confirmed  
3051 with a call to a telephone number of record, or;  
3052 ii. as an electronic request, authenticate it as being from the same Subscriber  
3053 or Subject, supported by a credential at Assurance Level 3 or higher.

3054 *AL3\_CM\_RVR#040 Verify CSP as Revocant*

3055 Where a CSP seeks revocation of a Subject's credential, establish that the request is  
3056 either:

- 3057 a) from the specified service itself, with authorization as determined by established  
3058 procedures, or;  
3059 b) from the client Credential Issuer, by authentication of a formalized request over  
3060 the established secure communications network.

3061 *AL3\_CM\_RVR#050 Verify Legal Representative as Revocant*

3062 Where the request for revocation is made by a law enforcement officer or presentation of  
3063 a legal document:

- 3064 a) if in person, verify the identity of the person presenting the request, or;  
3065 b) if remote:

- 3066 i. in paper/facsimile form, verify the origin of the legal document by a  
3067 database check or by telephone with the issuing authority, or;  
3068 ii. as an electronic request, authenticate it as being from a recognized legal  
3069 office, supported by a credential at Assurance Level 3 or higher.  
3070

3071 **5.3.4.3 No stipulation**

3072 **5.3.4.4 Secure Revocation Request**

3073 This criterion applies when revocation requests must be communicated between remote  
3074 components of the service organization.

3075 An enterprise and its specified service must:

3076 *AL3\_CM\_SRR#010 Submit Request*

3077 Submit a request for the revocation to the Credential Issuer service (function), using a  
3078 secured network communication.

3079

3080 **5.3.5 Part E - Credential Status Management**

3081 These criteria deal with credential status management, such as the receipt of requests for  
3082 new status information arising from a new credential being issued or a revocation or other  
3083 change to the credential that requires notification. They also deal with the provision of  
3084 status information to requesting parties (Verifiers, Relying Parties, courts and others  
3085 having regulatory authority, etc.) having the right to access such information.

3086 **5.3.5.1 Status Maintenance**

3087 An enterprise and its specified service must:

3088 *AL3\_CM\_CSM#010 Maintain Status Record*

3089 Maintain a record of the status of all credentials issued.

3090 *AL3\_CM\_CSM#020 Validation of Status Change Requests*

3091 Authenticate all requestors seeking to have a change of status recorded and published and  
3092 validate the requested change before considering processing the request. Such validation  
3093 should include:

- 3094 a) the requesting source as one from which the specified service expects to receive  
3095 such requests;  
3096 b) if the request is not for a new status, the credential or identity as being one for  
3097 which a status is already held.

3098 *AL3\_CM\_CSM#030 Revision to Published Status*

3099 Process authenticated requests for revised status information and have the revised  
3100 information available for access within a period of 72 hours.

3101 *AL3\_CM\_CSM#040 Status Information Availability*

3102 Provide, with **99%** availability, a secure automated mechanism to allow relying parties to  
3103 determine credential status and authenticate the Claimant's identity.

3104 *AL3\_CM\_CSM#050 Inactive Credentials*

3105 Disable any credential that has not been successfully used for authentication during a  
3106 period of 18 months.

3107

### 3108 **5.3.6 Part F - Credential Verification/Authentication**

3109 These criteria apply to credential validation and identity authentication.

#### 3110 **5.3.6.1 Assertion Security**

3111 An enterprise and its specified service must:

3112 *AL3\_CM\_ASS#010 Validation and Assertion Security*

3113 Provide validation of credentials to a Relying Party using a protocol that:

- 3114 a) requires authentication of the specified service, itself, or of the validation source;  
3115 b) ensures the integrity of the authentication assertion.

3116 *AL3\_CM\_ASS#015 No False Authentication*

3117 Employ techniques which ensure that system failures do not result in 'false positive  
3118 authentication' errors.

3119 *AL3\_CM\_ASS#018 Ensure token validity*

3120 **Ensure that tokens are either still valid or have been issued within the last 24 hours.**

3121 **Guidance:** The 24-hour period allows for the fact that if a freshly-issued credential is  
3122 then revoked, notice of the revocation may take 24 hours to be publicised (per  
3123 *AL3\_CM\_RVP#030*).

3124 *AL3\_CM\_ASS#020 Post Authentication*

3125 *Not* authenticate credentials that have been revoked unless the time of the transaction for  
3126 which verification is sought precedes the time of revocation of the credential.

3127 **Guidance:** The purpose in this criterion is that, if a verification is intended to refer to the  
3128 status of a credential at a specific historical point in time, e.g. to determine whether the  
3129 Claimant was entitled to act as a signatory in a specific capacity at the time of the  
3130 transaction, this may be done. It is implicit in this thinking that both the request and the  
3131 response indicate the historical nature of the query and response; otherwise the default  
3132 time is 'now'. If no such service is offered then this criterion may simply be  
3133 'Inapplicable', for that reason.

3134 *AL3\_CM\_ASS#030 Proof of Possession*

3135 Use an authentication protocol that requires the claimant to prove possession and control  
3136 of the authentication token.

3137 *AL3\_CM\_ASS#035 No stipulation*

3138 *AL3\_CM\_ASS#040 Assertion Lifetime*

3139 **For non-cryptographic credentials**, generate assertions so as to indicate and effect their  
3140 expiration 12 hours after their creation; **otherwise, notify the relying party of how often**  
3141 **the revocation status sources are updated.**

#### 3142 **5.3.6.2 Authenticator-generated challenges**

3143 An enterprise and its specified service must:

3144 *AL3\_CM\_AGC#010 Entropy level*

3145 Create authentication secrets to be used during the authentication exchange (i.e. with out-  
3146 of-band or cryptographic device tokens) with a degree of entropy appropriate to the token  
3147 type in question.

#### 3148 **5.3.6.3 Multi-factor authentication**

3149 An enterprise and its specified service must:

3150 *AL3\_CM\_MFA#010 Permitted multi-factor tokens*

3151 Require two tokens which, when used in combination within a single authentication  
3152 exchange, are acknowledged as providing an equivalence of AL3, as determined by a  
3153 recognized national technical authority.

#### 3154 **5.3.6.4 Verifier's assertion schema**

3155 Note: Since assertions and related schema can be complex and may be modeled directly  
3156 on the needs and preferences of the participants, the details of such schema fall outside  
3157 the scope of the SAC's herein, which are expressed observing, insofar as is feasible, a  
3158 technology-agnostic policy. The following criteria, therefore, are perhaps more open to  
3159 variable conformity through their final implementation than are others in this document.

3160 These criteria are derived directly from NIST SP 800-63-2 and have been expressed in as  
3161 generic a manner as they can be.

3162 *Editor's note: I have avoided reference to the RP here – I am concerned as to what the*  
3163 *SAC requires services to do, not who might be using their products. SAC do not refer to*  
3164 *RPs.*

3165 An enterprise and its specified service must:

3166 *AL3\_CM\_VAS#010 Approved cryptography*

- 3167 Apply assertion protocols which use cryptographic techniques approved by a national  
3168 authority or other generally-recognized authoritative body.
- 3169 *AL3\_CM\_VAS#020 No stipulation*  
3170 No stipulation.
- 3171 *AL3\_CM\_VAS#030 Assertion assurance level*  
3172 Create assertions which, either explicitly or implicitly (using a mutually-agreed  
3173 mechanism), indicate the assurance level at which the initial authentication of the Subject  
3174 was made.
- 3175 *AL3\_CM\_VAS#040 No pseudonyms*  
3176 Create assertions which indicate **only verified Subscriber names** in the credential  
3177 subject to verification.
- 3178 *AL3\_CM\_VAS#050 Specify recipient*  
3179 Create assertions which identify the intended recipient of the verification such that the  
3180 recipient may validate that it is intended for them.
- 3181 *AL3\_CM\_VAS#060 No assertion manufacture/modification*  
3182 Ensure that it is impractical to manufacture an assertion or assertion reference by **Signing**  
3183 **the assertion and** using at least one of the following techniques:
- 3184 a) Signing the assertion;
- 3185 b) Encrypting the assertion using a secret key shared with the RP;
- 3186 c) Creating an assertion reference which has a minimum of 64 bits of entropy;
- 3187 d) Sending the assertion over a protected channel during a mutually-authenticated  
3188 session.
- 3189 *AL3\_CM\_VAS#070 Assertion protections*  
3190 Provide protection of assertion-related data such that:
- 3191 a) both assertions and assertion references are protected against capture and re-use;
- 3192 b) assertions are also protected against redirection;
- 3193 c) assertions, assertion references and session cookies used for authentication  
3194 purposes, including any which are re-directed, are protected against session  
3195 hijacking, for at least the duration of their validity (see AL3\_CM\_VAS#110).
- 3196 *AL3\_CM\_VAS#080 Single-use assertions*  
3197 Limit to a single transaction the use of assertions which do not support proof of  
3198 ownership.
- 3199 *AL3\_CM\_VAS#090 Single-use assertion references*  
3200 Limit to a single transaction the use of assertion references.

- 3201 *AL3\_CM\_VAS#100 Bind reference to assertion*  
3202 Provide a strong binding between the assertion reference and the corresponding assertion,  
3203 based on integrity-protected (or signed) communications over which the Verifier has been  
3204 authenticated.
- 3205 *AL3\_CM\_VAS#110 Assertion expiration*  
3206 Set assertions to expire such that:
- 3207 a) those used outside of the internet domain of the Verifier become invalid 5 minutes  
3208 after their creation; or
  - 3209 b) those used within a single internet domain become invalid **30 minutes** after their  
3210 creation (including assertions contained in or referenced by cookies).
- 3211 *AL3\_CM\_VAS#120 SSO provisions*  
3212 **If SSO is supported, provide a re-authentication of the Subject so long as:**
- 3213 a) **the Subject has been successfully authenticated within the last 12 hours;**
  - 3214 b) **the Subject continues to be able to demonstrate that they were the party that**  
3215 **was previously authenticated;**
  - 3216 c) **it can be ensured that the Subscriber has not been inactive for more than 30**  
3217 **minutes.**
- 3218 **Guidance:** The conditional nature of this criterion is dictated by the phrasing used in  
3219 NIST SP 800-63 which states ‘*may*’.
- 3220

## 3221 5.4 Assurance Level 4

### 3222 5.4.1 Part A - Credential Operating Environment

3223 These criteria describe requirements for the overall operational environment in which  
3224 credential lifecycle management is conducted. The Common Organizational criteria  
3225 describe broad requirements. The criteria in this Part describe operational  
3226 implementation specifics.

3227 These criteria apply exclusively to cryptographic technology deployed through a Public  
3228 Key Infrastructure. This technology requires hardware tokens protected by password or  
3229 biometric controls. No other forms of credential are permitted at AL4.

3230 The following four criteria are **MANDATORY** for all Services, Full or Component, and  
3231 are individually marked as such:

3232 AL4\_CM\_CPP#020, AL4\_CM\_CPP#030, AL4\_CM\_CTR#030, AL4\_CM\_SER#010.

#### 3233 5.4.1.1 Certification Policy and Practices

3234 These criteria apply to the policy and practices under which certificates are managed.

3235 An enterprise and its specified service must:

3236 *ALA\_CM\_CPP#010 No stipulation*

3237 *ALA\_CM\_CPP#020 Certificate Policy/Certification Practice Statement*

3238 **MANDATORY.**

3239 **Include in its Service Definition its full Certificate Policy and the corresponding**  
3240 **Certification and Practice Statement. The Certificate Policy and Certification**  
3241 **Practice Statement must conform to IETF RFC 3647 (2003-11) [RFC 3647] in their**  
3242 **content and scope or be demonstrably consistent with the content or scope of that**  
3243 **RFC. At a minimum, the Certificate Policy must specify:**

- 3244 a) **applicable OIDs for each certificate type issued;**
- 3245 b) **how users may subscribe to the service/apply for certificates, and how**  
3246 **certificates will be issued to them;**
- 3247 c) **if users present their own keys, how they will be required to demonstrate**  
3248 **possession of the private key;**
- 3249 d) **if users' keys are generated for them, how the private keys will be delivered**  
3250 **to them;**
- 3251 e) **how Subjects acknowledge receipt of tokens and credentials and what**  
3252 **obligations they accept in so doing (including whether they consent to**  
3253 **publication of their details in certificate status directories);**
- 3254 f) **how certificates may be renewed, re-keyed, modified, revoked, and**  
3255 **suspended, including how requestors are authenticated or their identity**  
3256 **proven;**



3257 **g) what actions a Subject must take to terminate their subscription.**

3258 *ALA\_CM\_CPP#030 Management Authority*

3259 **MANDATORY.**

3260 Have a nominated or appointed high-level management body with authority and  
3261 responsibility for approving the Certificate Policy and Certification Practice Statement,  
3262 including ultimate responsibility for their proper implementation.

3263 *ALA\_CM\_CPP#040 Discretionary Access Control*

3264 **Apply discretionary access controls that limit access to trusted administrators and to**  
3265 **those applications that require access.**

3266 **Guidance:** This requirement was previously AL3\_CM\_STS#010 b) (part a) having been  
3267 withdrawn, which left part b) somewhat out of context.

3268

#### 3269 **5.4.1.2 Security Controls**

3270 An enterprise and its specified service must:

3271 *ALA\_CM\_CTR#010 Withdrawn*

3272 *ALA\_CM\_CTR#020 Protocol threat risk assessment and controls*

3273 Account for at least the following protocol threats in its risk assessment and apply  
3274 controls that reduce them to acceptable risk levels:

- 3275 a) password guessing, **showing that there is sufficient entropy;**
- 3276 b) message replay, showing that it is impractical;
- 3277 c) eavesdropping, showing that it is impractical;
- 3278 d) relying party (verifier) impersonation, showing that it is impractical;
- 3279 e) man-in-the-middle attack, showing that it is impractical;

3280

3281 **f) session hijacking, showing that it is impractical.**

3282 The above list shall not be considered to be a complete list of threats to be addressed by  
3283 the risk assessment.

3284 *ALA\_CM\_CTR#025 No stipulation*

3285 *ALA\_CM\_CTR#028 No Stipulation*

3286 *ALA\_CM\_CTR#030 System threat risk assessment and controls*

3287 **MANDATORY.**

3288 Account for the following system threats in its risk assessment and apply controls that  
3289 reduce them to acceptable risk levels:

- 3290 a) the introduction of malicious code;

- 3291 b) compromised authentication arising from insider action;
- 3292 c) out-of-band attacks by both users and system operators (e.g., shoulder-surfing);
- 3293 d) spoofing of system elements/applications;
- 3294 e) malfeasance on the part of Subscribers and Subjects;
- 3295 f) intrusions leading to information theft.

3296 The above list shall not be considered to be a complete list of threats to be addressed by  
3297 the risk assessment.

3298 *ALA\_CM\_CTR#040 Specified Service's Key Management*

3299 Specify and observe procedures and processes for the generation, storage, and destruction  
3300 of its own cryptographic keys used for securing the specific service's assertions and other  
3301 publicized information. At a minimum, these should address:

- 3302 a) the physical security of the environment;
- 3303 b) access control procedures limiting access to the minimum number of authorized  
3304 personnel;
- 3305 c) public-key publication mechanisms;
- 3306 d) application of controls deemed necessary as a result of the service's risk  
3307 assessment;
- 3308 e) destruction of expired or compromised private keys in a manner that prohibits  
3309 their retrieval, or their archival in a manner which prohibits their reuse;
- 3310 f) applicable cryptographic module security requirements, quoting FIPS 140-2  
3311 [FIPS140-2] or equivalent, as established by a recognized national technical  
3312 authority.

3313

3314 **5.4.1.3 Storage of Long-term Secrets**

3315 The enterprise and its specified service must meet the following criteria:

3316 *ALA\_CM\_STS#010 Withdrawn*

3317 Withdrawn (ALA\_CO\_SCO#020 (a) & (b) enforce this requirement part a) and  
3318 ALA\_CM\_CPP#040 now enforces part b))

3319 *ALA\_CM\_STS#020 Stored Secret Encryption*

3320 Encrypt such [omitted] secret files so that:

- 3321 a) the encryption key for the [omitted] secret file is encrypted under a key held in a  
3322 FIPS 140-2 [FIPS140-2] Level 2 or higher validated hardware cryptographic  
3323 module or any FIPS 140-2 Level 3 or 4 cryptographic module, or equivalent, as  
3324 established by a recognized national technical authority;
- 3325 b) the [omitted] secret file is decrypted only as immediately required for a key  
3326 recovery operation;
- 3327 c) [omitted] secrets are protected as a key within the boundary of a FIPS 140-2  
3328 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2  
3329 Level 3 or 4 cryptographic module and are not exported from the module in

- 3330 plaintext, or equivalent, as established by a recognized national technical  
3331 authority;  
3332 d) escrowed secrets are split by an "*n from m*" cryptographic secret **storing** method.  
3333

#### 3334 **5.4.1.4 Security-relevant Event (Audit) Records**

3335 These criteria describe the need to provide an auditable log of all events that are pertinent  
3336 to the correct and secure operation of the service. The common organizational criteria  
3337 relating to the recording of all security-related events must also be considered carefully.  
3338 These criteria carry implications for credential management operations.

3339 In the specific context of a certificate management service, an enterprise and its specified  
3340 service must:

3341 *ALA\_CM\_SER#010 Security event logs*

3342 **MANDATORY**, to the extent that the sub-items relate to the scope of service.

3343 Ensure that such audit records include:

- 3344 a) the identity of the point of registration (irrespective of whether internal or  
3345 outsourced);  
3346 b) generation of the Subject's keys or evidence that the Subject was in possession of  
3347 both parts of the key-pair;  
3348 c) generation of the Subject's certificate;  
3349 d) dissemination of the Subject's certificate;  
3350 e) any revocation or suspension associated with the Subject's credential.  
3351

#### 3352 **5.4.1.5 Subject Options**

3353 *ALA\_CM\_OPN#010 Changeable PIN/Password*

3354 Withdrawn – see ALA\_CM\_RNR#010.

3355

### 3356 **5.4.2 Part B - Credential Issuing**

3357 These criteria apply to the verification of the identity of the Subject of a credential and  
3358 with token strength and credential delivery mechanisms. They address requirements  
3359 levied by the use of various technologies to achieve Assurance Level 4.

#### 3360 **5.4.2.1 Identity Proofing Policy**

3361 Identity proofing at Assurance Level 4 requires the physical presence of the applicant in  
3362 front of the registration officer with photo ID or other readily verifiable biometric identity  
3363 information, as well as the requirements set out by the following criteria.

3364 The specific service must show that it applies identity proofing policies and procedures  
3365 and that it retains appropriate records of identity proofing activities and evidence.

3366 An enterprise and its specified service must:

3367 *ALA\_CM\_IDP#010 Withdrawn*

3368 Withdrawn.

3369 *ALA\_CM\_IDP#020 Withdrawn*

3370 Withdrawn.

3371 *ALA\_CM\_IDP#030 Withdrawn*

3372 Withdrawn.

3373 *ALA\_ID\_POL#010 Unique service identity*

3374 Ensure that a unique identity is attributed to the specific service, such that credentials  
3375 issued by it can be distinguishable from those issued by other services, including services  
3376 operated by the same enterprise.

3377 *ALA\_ID\_POL#020 Unique Subject identity*

3378 Ensure that each applicant's identity is unique within the service's community of Subjects  
3379 and uniquely associable with tokens and/or credentials issued to that identity.

3380 **Guidance:** Cf. *ALA\_CM\_CRN#020* which expresses a very similar requirement.

3381 Although presenting repetition for a single provider, if the identity-proofing functions and  
3382 credential management functions are provided by separate CSPs, each needs to fulfill this  
3383 requirement.

3384 *ALA\_ID\_POL#030 Published Proofing Policy*

3385 Make available the Identity Proofing Policy under which it verifies the identity of  
3386 applicants<sup>7</sup> in form, language, and media accessible to the declared community of users.

3387 *ALA\_ID\_POL#040 Adherence to Proofing Policy*

3388 Perform all identity proofing strictly in accordance with its published Identity Proofing  
3389 Policy, through application of the procedures and processes set out in its Identity Proofing  
3390 Practice Statement (IdPPS).

3391

#### 3392 **5.4.2.2 Identity Verification**

3393 The enterprise or specific service may:

---

<sup>7</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.

3394 *ALA\_ID\_IDV#000 Identity Proofing classes*  
3395 **[Omitted] offer only face-to-face identity proofing service. Remote verification is not**  
3396 **allowed at this assurance level;**

3397 *ALA\_ID\_IDV#010 - Identity Verification Measures*

3398 **[Omitted]** Justify the identity verification measures described in its IdPPS (see  
3399 AL4\_ID\_POL#040) by describing how these meet or exceed the requirements of  
3400 applicable policies, regulations, adopted standards and other relevant conditions in order  
3401 to maintain a level of rigour consistent with the AL4.

3402 **Guidance:** Although strict requirements for identity proofing and verification can be  
3403 defined, a real-world approach must account for instances where there is not 100%  
3404 certitude. To cope with this CSPs need to have a set of prescribed (through policy – see  
3405 AL4\_ID\_POL#030) and applied measures (see AL4\_ID\_POL#040) which observe  
3406 policy, identify the measures taken according to the degree of certitude determined by  
3407 each step in the verification process and what additional measures are taken. The CSP  
3408 must present a case which shows that their solution is sufficient to ensure that the basic  
3409 requirements of the applicable AL are met or exceeded.

3410 Note that in each set of proofing service criteria below there are criteria with specific  
3411 requirements for evidence checks and an additional criterion for ‘secondary’ checks, all of  
3412 which have an interplay with these overall requirements to have a policy and practice  
3413 statement and to demonstrate processes which sustain confidence that AL3 is being  
3414 achieved.

3415

3416 The enterprise or specified service must:

#### 3417 **5.4.2.3 In-Person Public Identity Proofing**

3418 *ALA\_ID\_IPV#010 Required evidence*

3419 Ensure that the applicant is in possession of:

- 3420 a) a primary Government Picture ID document that bears a photographic image of  
3421 the **holder and either:**  
3422 i) **secondary Government Picture ID or an account number issued by a**  
3423 **regulated financial institution or;**  
3424 ii) **two items confirming name, and address or telephone number, such**  
3425 **as: utility bill, professional license or membership, or other evidence**  
3426 **of equivalent standing.**

3427 *ALA\_ID\_IPV#020 No stipulation*

3428 *ALA\_ID\_IPV#030 Evidence checks – primary ID*

3429 **Ensure that the presented document:**

- 3430 a) **appears to be a genuine document properly issued by the claimed issuing**  
3431 **authority and valid at the time of application;**  
3432 b) **bears a photographic image of the holder which matches that of the**  
3433 **applicant;**  
3434 c) **is electronically verified by a record check with the specified issuing**  
3435 **authority or through similar databases that:**  
3436 i) **establishes the existence of such records with matching name and**  
3437 **reference numbers;**  
3438 ii) **corroborates date of birth, current address of record, and other**  
3439 **personal information sufficient to ensure a unique identity;**  
3440 d) **provides all reasonable certainty, at AL4, that the identity exists and that it**  
3441 **uniquely identifies the applicant.**

3442 *AL4\_ID\_IPV#040 Evidence checks – secondary ID*

3443 **Ensure that the presented document meets the following conditions:**

- 3444 a) **If it is secondary Government Picture ID:**  
3445 i) **appears to be a genuine document properly issued by the claimed**  
3446 **issuing authority and valid at the time of application;**  
3447 ii) **bears a photographic image of the holder which matches that of the**  
3448 **applicant;**  
3449 iii) **states an address at which the applicant can be contacted.**  
3450 b) **If it is a financial institution account number, is verified by a record check**  
3451 **with the specified issuing authority or through similar databases that:**  
3452 i) **establishes the existence of such records with matching name and**  
3453 **reference numbers;**  
3454 ii) **corroborates date of birth, current address of record, and other**  
3455 **personal information sufficient to ensure a unique identity.**  
3456 c) **If it is two utility bills or equivalent documents:**  
3457 i) **each appears to be a genuine document properly issued by the**  
3458 **claimed issuing authority;**  
3459 ii) **corroborates current address of record or telephone number sufficient to**  
3460 **ensure a unique identity.**

3461 *AL4\_ID\_IPV#050 Applicant knowledge checks*

3462 **Where the applicant is unable to satisfy any of the above requirements, that the**  
3463 **applicant can provide a unique identifier, such as a Social Security Number (SSN),**  
3464 **that matches the claimed identity.**

3465

#### 3466 **5.4.2.4 Remote Public Identity Proofing**

3467 **Not permitted.**

3468 **5.4.2.5 Current Relationship Identity Proofing**

3469 **Not permitted**

3470 **5.4.2.6 Affiliation Identity Proofing**

3471 A specific service that offers identity proofing to applicants on the basis of some form of  
3472 affiliation must comply with the criteria in this section to establish that affiliation, in  
3473 addition to complying with the previously stated requirements for verifying the  
3474 individual's identity.

3475 The enterprise or specified service must:

3476 *ALA\_ID\_AFV#000 Meet preceding criteria*

3477 Meet all the criteria set out above, under §5.4.2.3, “[In-Person Public Identity](#)  
3478 [Verification](#)”.

3479 *ALA\_ID\_AFV#010 Required evidence*

3480 Ensure that the applicant possesses:

- 3481 a) identification from the organization with which it is claiming affiliation;  
3482 b) agreement from the organization that the applicant may be issued a credential  
3483 indicating that an affiliation exists.

3484 *ALA\_ID\_AFV#020 Evidence checks*

3485 Have in place and apply processes which ensure that the presented documents:

- 3486 a) each appear to be a genuine document properly issued by the claimed issuing  
3487 authorities and valid at the time of application;  
3488 b) refer to an existing organization with a contact address;  
3489 c) indicate that the applicant has some form of recognizable affiliation with the  
3490 organization;  
3491 d) appear to grant the applicant an entitlement to obtain a credential indicating an  
3492 affiliation with the organization.  
3493

3494 **5.4.2.7 Issuing Derived Credentials**

3495 Where the Applicant already possesses recognized original credentials the CSP may  
3496 choose to accept the verified identity of the Applicant as a substitute for identity proofing,  
3497 subject to the following specific provisions. All other identity proofing requirements  
3498 must also be observed.

3499 *ALA\_ID\_IDC#010 Authenticate Original Credential*

3500 Prior to issuing any derived credential the original credential on which the identity-  
3501 proofing relies must be:

- 3502 a) authenticated by a source trusted by the CSP as being valid and un-revoked;

- 3503 b) issued at Assurance Level 4;  
3504 c) issued in the same name as that which the Applicant is claiming;  
3505 d) proven to be in the possession and under the control of the Applicant, **who shall**  
3506 **be physically present.**

3507 *ALA\_ID\_IDC#020 Record Original Credential*  
3508 Record the details of the original credential, **the biometric sample related to the**  
3509 **original credential and the biometric sample captured when authenticating the**  
3510 **Applicant.**

3511 *ALA\_ID\_IDC#030 Issue Derived Credential*  
3512 **Only issue the derived credential in-person after performing biometric**  
3513 **authentication of the Applicant .**

3514

#### 3515 **5.4.2.8 Secondary Identity Verification**

3516 In each of the above cases, the enterprise or specified service must also meet the  
3517 following criteria:

3518 *ALA\_ID\_SCV#010 Secondary checks*  
3519 Have in place additional measures (e.g., require additional documentary evidence, delay  
3520 completion while out-of-band checks are undertaken) to deal with any anomalous  
3521 circumstances that can reasonably be anticipated (e.g., a legitimate and recent change of  
3522 address that has yet to be established as the address of record).

3523

#### 3524 **5.4.2.9 Identity-proofing Records**

3525 The specific service must retain records of the identity proofing (verification) that it  
3526 undertakes and provide them to qualifying parties when so required.

3527 The enterprise or specified service must:

3528 *ALA\_ID\_VRC#010 Verification Records for Personal Applicants*  
3529 Log, taking account of all applicable legislative and policy obligations, a record of the  
3530 facts of the verification process and the identity of the registrar, including a reference  
3531 relating to the verification processes and the date and time of verification **issued by a**  
3532 **trusted time-source.**

3533 **Guidance:** The facts of the verification process should include the specific record  
3534 information (source, unique reference, value/content) used in establishing the applicant's  
3535 identity, and will be determined by the specific processes used and documents accepted  
3536 by the CSP. The CSP need not retain these records itself if it uses a third-party service  
3537 which retains such records securely and to which the CSP has access when required, in



3538 which case it must retain a record of the identity of the third-party service providing the  
3539 verification service or the location at which the (in-house) verification was performed.

3540 *ALA\_ID\_VRC#020 Verification Records for Affiliated Applicants*

3541 In addition to the foregoing, log, taking account of all applicable legislative and policy  
3542 obligations, a record of the additional facts of the verification process [omitted]. At a  
3543 minimum, records of identity information must include:

- 3544 a) the Subject's<sup>8</sup> full name;
- 3545 b) the Subject's current address of record;
- 3546 c) the Subject's current telephone or email address of record;
- 3547 d) the Subscriber's authorization for issuing the Subject a credential;
- 3548 e) type, issuing authority, and reference number(s) of all documents checked in the  
3549 identity proofing process;
- 3550 **f) a biometric record of each required representative of the affiliating**  
3551 **organization (e.g., a photograph, fingerprint, voice recording), as determined**  
3552 **by that organization's governance rules/charter.**

3553 *ALA\_ID\_VRC#025 Provide Subject identity records*

3554 If required, provide to qualifying parties records of identity proofing to the extent  
3555 permitted by applicable legislation and/or agreed by the Subscriber.

3556 *ALA\_ID\_VRC#030 Record Retention*

3557 Either retain, securely, the record of the verification/revocation process for the duration of  
3558 the Subject account plus a further period sufficient to allow fulfillment of any period  
3559 required legally, contractually or by any other form of binding agreement or obligation, or  
3560 submit the record to a client CSP that has undertaken to retain the record for the requisite  
3561 period or longer.

3562 *ALA\_CM\_IDP#040 Revision to Subscriber information*

3563 Provide a means for Subscribers and Subjects to securely amend their stored information  
3564 after registration, either by re-proving their identity as in the initial registration process or  
3565 by using their credentials to authenticate their revision. Successful revision must, where  
3566 necessary, instigate the re-issuance of the credential.

3567

#### 3568 **5.4.2.10 Credential Creation**

3569 These criteria define the requirements for creation of credentials whose highest use is  
3570 ALA.

---

<sup>8</sup> At this stage, the Subject is the entity acting in the role of Applicant, in anticipation of being issued a credential in which they shall be identified as the 'Subject' of that credential.

- 3571 Note, however, that a token and credential created according to these criteria may not  
3572 necessarily provide that level of assurance for the claimed identity of the Subject.  
3573 Authentication can only be provided at the assurance level at which the identity is proven.  
3574 An enterprise and its specified service must:
- 3575 *AL4\_CM\_CRN#010 Authenticated Request*  
3576 Only accept a request to generate a credential and bind it to an identity if the source of the  
3577 request, i.e., Registration Authority, can be authenticated as being authorized to perform  
3578 identity proofing at AL4.
- 3579 *AL4\_CM\_CRN#020 Unique identity*  
3580 Ensure that the identity which relates to a specific applicant is unique within the specified  
3581 service, including identities previously used and that are now cancelled, other than its re-  
3582 assignment to the same applicant.
- 3583 **Guidance:** This requirement is intended to prevent identities that may exist in a Relying  
3584 Party's access control lists from possibly representing a different physical person.
- 3585 Cf. AL4\_CM\_POL#020 which expresses a very similar requirement. Although  
3586 presenting repetition for a single provider, if the identity-proofing functions and  
3587 credential management functions are provided by separate CSPs, each needs to fulfill this  
3588 requirement.
- 3589 *AL4\_CM\_CRN#030 Credential uniqueness*  
3590 Allow the Subject to select a credential (e.g., UserID) that is verified to be unique within  
3591 the specified service's community and assigned uniquely to a single identity Subject.
- 3592 *AL4\_CM\_CRN#035 Convey credential*  
3593 Be capable of conveying the unique identity information associated with a credential to  
3594 Verifiers and Relying Parties.
- 3595 *AL4\_CM\_CRN#040 Token strength*  
3596 **Not use PIN/password tokens.**
- 3597 *AL4\_CM\_CRN#050 One-time password strength*  
3598 **Not use one-time password tokens.**
- 3599 *AL4\_CM\_CRN#055 No stipulation*
- 3600 *AL4\_CM\_CRN#060 Software cryptographic token strength*  
3601 **Not use software cryptographic tokens.**
- 3602 *AL4\_CM\_CRN#070 One-time password hardware token strength*  
3603 Ensure that hardware tokens used to store cryptographic keys:
- 3604 a) employ a cryptographic module that is validated against FIPS 140-2 [FIPS140-2]  
3605 Level 2 or higher, or equivalent, as determined by a recognized national technical  
3606 authority;
- 3607 b) require password or biometric activation by the Subject [omitted];

3608 c) **Generate a one-time password using an algorithm recognized by a national**  
3609 **technical authority.**

3610 *ALA\_CM\_CRN#075 Multi-factor hardware cryptographic token strength*

3611 **Ensure that hardware tokens used to store cryptographic keys:**

3612 a) **employ a cryptographic module that is validated against FIPS 140-2**  
3613 **[FIPS140-2] Level 2 or higher, or equivalent, as determined by a recognized**  
3614 **national technical authority;**

3615 b) **are evaluated against FIPS 140-2 Level 3 or higher, or equivalent, as**  
3616 **determined by a recognized national technical authority, for their physical**  
3617 **security;**

3618 c) **require password, PIN or biometric activation by the Subject when being**  
3619 **used for authentication;**

3620 d) **does not permit the export of authentication keys.**

3621 *ALA\_CM\_CRN#080 Binding of key*

3622 If the specified service generates the Subject's key pair, that the key generation process  
3623 securely and uniquely binds that process to the certificate generation and maintains at all  
3624 times the secrecy of the private key, until it is accepted by the Subject.

3625 *ALA\_CM\_CRN#090 Nature of Subject*

3626 Record the nature of the Subject of the credential **[omitted]**, i.e., private person, a named  
3627 person acting on behalf of a corporation or other legal entity, corporation or legal entity,  
3628 or corporate machine entity, in a manner that can be unequivocally associated with the  
3629 credential and the identity that it asserts.

3630 *ALA\_CM\_CRN#095 No stipulation*

3631 No stipulation

3632

#### 3633 **5.4.2.11 Subject Key Pair Generation**

3634 An enterprise and its specified service must:

3635 *ALA\_CM\_SKP#010 Key generation by Specified Service*

3636 If the specified service generates the Subject's keys:

3637 a) use a FIPS 140-2 **[FIPS140-2]** compliant algorithm, or equivalent, as established  
3638 by a recognized national technical authority, that is recognized as being fit for the  
3639 purposes of the service;

3640 b) only create keys of a key length and for use with a FIPS 140-2 **[FIPS140-2]**  
3641 compliant public key algorithm, or equivalent, as established by a recognized  
3642 national technical authority, recognized as being fit for the purposes of the  
3643 service;

- 3644 c) generate and store the keys securely until delivery to and acceptance by the  
3645 Subject;  
3646 d) deliver the Subject's private key in a manner that ensures that the privacy of the  
3647 key is not compromised and only the Subject has access to the private key.

3648 *ALA\_CM\_SKP#020 Key generation by Subject*

3649 If the Subject generates and presents its own keys, obtain the Subject's written  
3650 confirmation that it has:

- 3651 a) used a FIPS 140-2 [FIPS140-2] compliant algorithm, or equivalent, as established  
3652 by a recognized national technical authority, that is recognized as being fit for the  
3653 purposes of the service;  
3654 b) created keys of a key length and for use with a FIPS 140-2 [FIPS140-2] compliant  
3655 public key algorithm, or equivalent, as established by a recognized national  
3656 technical authority, recognized as being fit for the purposes of the service.  
3657

#### 3658 5.4.2.12 Credential Delivery

3659 An enterprise and its specified service must:

3660 *ALA\_CM\_CRD#010 Notify Subject of Credential Issuance*

3661 Notify the Subject of the credential's issuance and, if necessary, confirm Subject's contact  
3662 information by:

- 3663 a) sending notice to the address of record confirmed during identity proofing;  
3664 b) **unless the Subject presented with a private key, issuing the hardware token**  
3665 **to the Subject in a manner that confirms the address of record supplied by**  
3666 **the applicant during identity proofing;**  
3667 c) **issuing the certificate to the Subject over a separate channel in a manner that**  
3668 **confirms either the address of record or the email address supplied by the**  
3669 **applicant during identity proofing.**

3670 *ALA\_CM\_CRD#015 Confirm Applicant's identity (in person)*

3671 Prior to delivering the credential, require the Applicant to identify themselves in person in  
3672 any new transaction (beyond the first transaction or encounter) [deleted] through the use  
3673 of a biometric that was recorded during the first encounter.

3674 *ALA\_CM\_CRD#016 No stipulation*

3675 **No stipulation.**

3676 *ALA\_CM\_CRD#017 Protected Issuance of Permanent Secrets (in person)*

3677 Only issue permanent secrets if the CSP has:

- 3678 (b) loaded the secret itself onto the physical device, which was either:  
3679 i) issued in-person to the Applicant, or;  
3680 ii) delivered in a manner that confirms the address of record.

3681 *ALA\_CM\_CRD#018 No stipulation*  
3682 **No stipulation.**

3683 *ALA\_CM\_CRD#020 Subject's acknowledgement*  
3684 Receive acknowledgement of receipt of the **hardware token** before it is activated and **the**  
3685 **corresponding certificate and** its directory status record are published (and thereby the  
3686 subscription becomes active or re-activated, depending upon the circumstances of issue).  
3687

### 3688 **5.4.3 Part C - Credential Renewal and Re-issuing**

3689 These criteria apply to the renewal and re-issuing of credentials. They address  
3690 requirements levied by the use of various technologies to achieve Assurance Level 4.

#### 3691 **5.4.3.1 Renewal/Re-issuance Procedures**

3692 These criteria address general renewal and re-issuance functions, to be exercised as  
3693 specific controls in these circumstances while continuing to observe the general  
3694 requirements established for initial credential issuance.

3695 An enterprise and its specified service must:

3696 *ALA\_CM\_RNR#010 Changeable PIN/Password*  
3697 Permit Subjects to change the passwords used to activate their credentials.

3698 *ALA\_CM\_RNR#020 Proof-of-possession on Renewal/Re-issuance*  
3699 Subjects wishing to change their passwords must demonstrate that they are in possession  
3700 of the unexpired current token prior to the CSP proceeding to renew or re-issue it.

3701 *ALA\_CM\_RNR#030 Renewal/Re-issuance limitations*

3702 a) No stipulation;

3703 b) No stipulation;

3704 c) No stipulation;

3705 d) **cryptographically authenticate** all sensitive renewal / re-issuance interactions  
3706 with the Subject **using keys bound to the authentication process.**

3707 **Guidance:** Renewal is considered as an extension of usability, whereas re-issuance  
3708 requires a change.

3709 *ALA\_CM\_RNR#040 Authentication key life*

3710 **Expire after 24 hours all temporary or short-term keys derived during the**  
3711 **authentication process.**

3712 *ALA\_CM\_RNR#050 Record Retention*

3713 Retain, securely, the record of any renewal/re-issuance process for the duration of the  
3714 Subscriber's account plus a further period sufficient to allow fulfillment of any period  
3715 required legally, contractually or by any other form of binding agreement or obligation, or

3716 submit same record to a client CSP that has undertaken to retain the record for the  
3717 requisite period or longer.

3718

#### 3719 **5.4.4 Part D - Credential Revocation**

3720 These criteria deal with credential revocation and the determination of the legitimacy of a  
3721 revocation request.

##### 3722 **5.4.4.1 Revocation Procedures**

3723 These criteria address general revocation functions, such as the processes involved and  
3724 the basic requirements for publication.

3725 An enterprise and its specified service must:

3726 *ALA\_CM\_RVP#010 Revocation procedures*

3727 a) State the conditions under which revocation of an issued certificate may occur;

3728 b) State the processes by which a revocation request may be submitted;

3729 c) State the persons and organizations from which a revocation request will be  
3730 accepted;

3731 d) State the validation steps that will be applied to ensure the validity (identity) of  
3732 the Revocant, and;

3733 e) State the response time between a revocation request being accepted and the  
3734 publication of revised certificate status.

3735 *ALA\_CM\_RVP#020 Secure status notification*

3736 Ensure that published credential status notification information can be relied upon in  
3737 terms of the enterprise of its origin (i.e., its authenticity) and its correctness (i.e., its  
3738 integrity).

3739 *ALA\_CM\_RVP#030 Revocation publication*

3740 Ensure that published credential status notification is revised within **18** hours of the  
3741 receipt of a valid revocation request, such that any subsequent attempts to use that  
3742 credential in an authentication shall be unsuccessful. The nature of the revocation  
3743 mechanism shall be in accordance with the technologies supported by the service.

3744 *ALA\_CM\_RVP#040 Verify Revocation Identity*

3745 Establish that the identity for which a revocation request is received is one that was  
3746 issued by the specified service.

3747 *ALA\_CM\_RVP#050 Revocation Records*

3748 Retain a record of any revocation of a credential that is related to a specific identity  
3749 previously verified, solely in connection to the stated credential. At a minimum, records  
3750 of revocation must include:

- 3751 a) the Revocant's full name;
- 3752 b) the Revocant's authority to revoke (e.g., Subscriber or Subject themselves,
- 3753 someone acting with the Subscriber's or Subject's power of attorney, the
- 3754 credential issuer, law enforcement, or other legal due process);
- 3755 c) the Credential Issuer's identity (if not directly responsible for the identity
- 3756 proofing service); [Omitted]
- 3757 d) the reason for revocation.

3758 *ALA\_CM\_RVP#060 Record Retention*

3759 Retain, securely, the record of the revocation process for a period which is in compliance  
3760 with:

- 3761 c) the records retention policy required by AL2\_CM\_CPP#010, and;
  - 3762 d) applicable legislation;
- 3763 and which, in addition, must be not less than the duration of the Subscriber's account plus  
3764 **10.5** years.

3765

3766 **5.4.4.2 Verify Revocant's Identity**

3767 Revocation of a credential requires that the requestor and the nature of the request be  
3768 verified as rigorously as the original identity proofing. The enterprise should not act on a  
3769 request for revocation without first establishing the validity of the request (if it does not,  
3770 itself, determine the need for revocation).

3771 In order to do so, the enterprise and its specified service must:

3772 *ALA\_CM\_RVR#010 Verify revocation identity*

3773 Establish that the credential for which a revocation request is received is one that was  
3774 initially issued by the specified service, applying the same process and criteria as would  
3775 apply to an original identity proofing.

3776 *ALA\_CM\_RVR#020 Revocation reason*

3777 Establish the reason for the revocation request as being sound and well founded, in  
3778 combination with verification of the Revocant, according to AL4\_CM\_RVR#030,  
3779 AL4\_CM\_RVR#040, or AL4\_CM\_RVR#050.

3780 *ALA\_CM\_RVR#030 Verify Subscriber as Revocant*

3781 Where the Subscriber or Subject seeks revocation of the Subject's credential:

- 3782 a) if in person, require presentation of a primary Government Picture ID document
- 3783 that shall be [Omitted] verified by a record check against the provided identity
- 3784 with the specified issuing authority's records;
- 3785 b) if remote:
- 3786 i. verify a signature against records (if available), confirmed with a call to a
- 3787 telephone number of record, or;

- 3788 ii. as an electronic request, authenticate it as being from the same Subscriber  
3789 or Subject, supported by a **different** credential at **Assurance Level 4**.

3790 *ALA\_CM\_RVR#040 Verify CSP as Revocant*

3791 Where a CSP seeks revocation of a Subject's credential, establish that the request is  
3792 either:

- 3793 a) from the specified service itself, with authorization as determined by established  
3794 procedures, or;  
3795 b) from the client Credential Issuer, by authentication of a formalized request over  
3796 the established secure communications network.

3797 *ALA\_CM\_RVR#050 Verify Legal Representative as Revocant*

3798 Where the request for revocation is made by a law enforcement officer or presentation of  
3799 a legal document:

- 3800 a) if in-person, verify the identity of the person presenting the request, or;  
3801 b) if remote:  
3802 i. in paper/facsimile form, verify the origin of the legal document by a  
3803 database check or by telephone with the issuing authority;  
3804 ii. as an electronic request, authenticate it as being from a recognized legal  
3805 office, supported by a different credential at **Assurance Level 4**.

#### 3806 **5.4.4.3 Re-keying a credential**

3807 Re-keying of a credential requires that the requestor be verified as the Subject with as  
3808 much rigor as was applied to the original identity proofing. The enterprise should not act  
3809 on a request for re-key without first establishing that the requestor is identical to the  
3810 Subject.

3811 In order to do so, the enterprise and its specified service must:

3812 *ALA\_CM\_RKY#010 Verify Requestor as Subscriber*

3813 **Where the Subject seeks a re-key for the Subject's own credential:**

- 3814 a) **if in-person, require presentation of a primary Government Picture ID**  
3815 **document that shall be verified by a record check against the provided**  
3816 **identity with the specified issuing authority's records;**  
3817 b) **if remote:**  
3818 i. **verify a signature against records (if available), confirmed with a call**  
3819 **to a telephone number of record, or;**  
3820 ii. **authenticate an electronic request as being from the same Subject,**  
3821 **supported by a different credential at Assurance Level 4.**

3822 *ALA\_CM\_RKY#020 Re-key requests other than Subject*

3823 **Re-key requests from any parties other than the Subject must not be accepted.**



3824 **5.4.4.4 Secure Revocation/Re-key Request**

3825 This criterion applies when revocation **or re-key** requests must be communicated  
3826 between remote components of the service organization.

3827 The enterprise and its specified service must:

3828 *ALA\_CM\_SRR#010 Submit Request*

3829 Submit a request for the revocation to the Credential Issuer service (function), using a  
3830 secured network communication.

3831

3832 **5.4.5 Part E - Credential Status Management**

3833 These criteria deal with credential status management, such as the receipt of requests for  
3834 new status information arising from a new credential being issued or a revocation or other  
3835 change to the credential that requires notification. They also deal with the provision of  
3836 status information to requesting parties (Verifiers, Relying Parties, courts and others  
3837 having regulatory authority, etc.) having the right to access such information.

3838 **5.4.5.1 Status Maintenance**

3839 An enterprise and its specified service must:

3840 *ALA\_CM\_CSM#010 Maintain Status Record*

3841 Maintain a record of the status of all credentials issued.

3842 *ALA\_CM\_CSM#020 Validation of Status Change Requests*

3843 Authenticate all requestors seeking to have a change of status recorded and published and  
3844 validate the requested change before considering processing the request. Such validation  
3845 should include:

- 3846 a) the requesting source as one from which the specified service expects to receive  
3847 such requests;  
3848 b) if the request is not for a new status, the credential or identity as being one for  
3849 which a status is already held.

3850 *ALA\_CM\_CSM#030 Revision to Published Status*

3851 Process authenticated requests for revised status information and have the revised  
3852 information available for access within a period of 72 hours.

3853 *ALA\_CM\_CSM#040 Status Information Availability*

3854 Provide, with 99% availability, a secure automated mechanism to allow relying parties to  
3855 determine credential status and authenticate the Claimant's identity.

3856 *ALA\_CM\_CSM#050 Inactive Credentials*

3857 Disable any credential that has not been successfully used for authentication during a  
3858 period of 18 months.

3859

## 3860 **5.4.6 Part F - Credential Verification/Authentication**

3861 These criteria apply to credential validation and identity authentication.

### 3862 **5.4.6.1 Assertion Security**

3863 An enterprise and its specified service must:

3864 *ALA\_CM\_ASS#010 Validation and Assertion Security*

3865 Provide validation of credentials to a Relying Party using a protocol that:

- 3866 a) requires authentication of the specified service, itself, or of the validation source;
- 3867 b) ensures the integrity of the authentication assertion.

3868 *ALA\_CM\_ASS#015 No False Authentication*

3869 Employ techniques which ensure that system failures do not result in 'false positive  
3870 authentication' errors.

3871 *ALA\_CM\_ASS#018 Ensure token validity*

3872 Ensure that tokens are either still valid or have been issued within the last 24 hours.

3873 **Guidance:** The 24-hour period allows for the fact that if a freshly-issued credential is  
3874 then revoked, notice of the revocation may take 24 hours to be publicised (per  
3875 AL3\_CM\_RVP#030)..

3876 *ALA\_CM\_ASS#020 Post Authentication*

3877 *Not* authenticate credentials that have been revoked unless the time of the transaction for  
3878 which verification is sought precedes the time of revocation of the credential.

3879 **Guidance:** The purpose in this criterion is that, if a verification is intended to refer to the  
3880 status of a credential at a specific historical point in time, e.g. to determine whether the  
3881 Claimant was entitled to act as a signatory in a specific capacity at the time of the  
3882 transaction, this may be done. It is implicit in this thinking that both the request and the  
3883 response indicate the historical nature of the query and response; otherwise the default  
3884 time is 'now'. If no such service is offered then this criterion may simply be  
3885 'Inapplicable', for that reason.

3886 *ALA\_CM\_ASS#030 Proof of Possession*

3887 Use an authentication protocol that requires the claimant to prove possession and control  
3888 of the authentication token.

3889 *ALA\_CM\_ASS#035 No stipulation*

3890 *ALA\_CM\_ASS#040 Assertion Life-time*

3891 **[Omitted]** Notify the relying party of how often the revocation status sources are  
3892 updated.

3893 **5.4.6.2 Authenticator-generated challenges**

3894 An enterprise and its specified service must:

3895 *ALA\_CM\_AGC#010 Entropy level*

3896 Create authentication secrets to be used during the authentication exchange (i.e. with out-  
3897 of-band or cryptographic device tokens) with a degree of entropy appropriate to the token  
3898 type in question.

3899 *ALA\_CM\_AGC#020 Limit password validity*

3900 **Employ one-time passwords which expire within two minutes.**

3901 **5.4.6.3 Multi-factor authentication**

3902 An enterprise and its specified service must:

3903 *ALA\_CM\_MFA#010 Permitted multi-factor tokens*

3904 Require two tokens which, when used in combination within a single authentication  
3905 exchange, are acknowledged as providing an equivalence of AL4, as determined by a  
3906 recognized national technical authority.

3907 **5.4.6.4 Verifier's assertion schema**

3908 Note: Since assertions and related schema can be complex and may be modeled directly  
3909 on the needs and preferences of the participants, the details of such schema fall outside  
3910 the scope of the SAC's herein, which are expressed observing, insofar as is feasible, a  
3911 technology-agnostic policy. The following criteria, therefore, are perhaps more open to  
3912 variable conformity through their final implementation than are others in this document.

3913 These criteria are derived directly from NIST SP 800-63-2 and have been expressed in as  
3914 generic a manner as they can be.

3915 An enterprise and its specified service must:

3916 *ALA\_CM\_VAS#010 Approved cryptography*

3917 Apply assertion protocols which use cryptographic techniques approved by a national  
3918 authority or other generally-recognized authoritative body.

3919 *ALA\_CM\_VAS#020 No browser/bearer assertions*

3920 **Not issue browser / bearer assertions.**

3921 *ALA\_CM\_VAS#030 Assertion assurance level*

3922 Create assertions which, either explicitly or implicitly (using a mutually-agreed  
3923 mechanism), indicate the assurance level at which the initial authentication of the Subject  
3924 was made.

3925 *ALA\_CM\_VAS#040 No pseudonyms*

- 3926 Create assertions which indicate only verified Subscriber names in the credential subject  
3927 to verification.
- 3928 *ALA\_CM\_VAS#050 Specify recipient*  
3929 Create assertions which identify the intended recipient of the verification such that the  
3930 recipient may validate that it is intended for them.
- 3931 *ALA\_CM\_VAS#060 No assertion manufacture/modification*  
3932 Ensure that it is impractical to manufacture an assertion or assertion reference by Signing  
3933 the assertion and using at least one of the following techniques:
- 3934 a) [Omitted];  
3935 b) Encrypting the assertion using a secret key shared with the RP;  
3936 c) Creating an assertion reference which has a minimum of 64 bits of entropy;  
3937 d) Sending the assertion over a protected channel during a mutually-authenticated  
3938 session.
- 3939 *ALA\_CM\_VAS#070 Assertion protections*  
3940 Provide protection of assertion-related data such that:
- 3941 a) both assertions and assertion references are protected against capture and re-use;  
3942 b) assertions are also protected against redirection  
3943 c) assertions, assertion references and session cookies used for authentication  
3944 purposes, including any which are re-directed, are protected against session  
3945 hijacking, for at least the duration of their validity (see AL1\_CM\_VAS#110).
- 3946 *ALA\_CM\_VAS#080 Single-use assertions*  
3947 Limit to a single transaction the use of assertions which do not support proof of  
3948 ownership.
- 3949 *ALA\_CM\_VAS#090 Single-use assertion references*  
3950 Limit to a single transaction the use of assertion references.
- 3951 *ALA\_CM\_VAS#100 Bind reference to assertion*  
3952 Provide a strong binding between the assertion reference and the corresponding assertion,  
3953 based on integrity-protected (or signed) communications over which the Verifier has been  
3954 authenticated.
- 3955 *ALA\_CM\_VAS#110 Assertion expiration*  
3956 Set assertions to expire such that:
- 3957 a) those used outside of the internet domain of the Verifier become invalid 5 minutes  
3958 after their creation; or  
3959 b) those used within a single internet domain become invalid 30 minutes after their  
3960 creation (including assertions contained in or referenced by cookies).

3961 *ALA\_CM\_VAS#120 No stipulation*

3962 No stipulation.

3963

3964 **5.5 Compliance Tables**

3965 Use the following tables to correlate criteria for a particular Assurance Level (AL) and  
3966 the evidence offered to support compliance.

3967 Service providers preparing for an assessment can use the table appropriate to the AL at  
3968 which they are seeking approval to correlate evidence with criteria or to justify non-  
3969 applicability (e.g., "specific service types not offered").

3970 Assessors can use the tables to record the steps in their assessment and their  
3971 determination of compliance or failure.

3972 **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>	
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>	
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>	
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>	
AL1_ID_VRC#030	No stipulation	No conformity requirement
AL1_CM_IDP#040	<a href="#">Revision to Subscriber Information</a>	
AL1_CM_CRN#010	<a href="#">Authenticated Request</a>	
AL1_CM_CRN#020	No stipulation	No conformity requirement
AL1_CM_CRN#030	<a href="#">Credential uniqueness</a>	
AL1_CM_CRN#035	<a href="#">Convey credential</a>	
AL1_CM_CRN#040	<a href="#">Token strength</a>	
Part C – Credential Renewal and Re-issuing		
AL1_CM_RNR#010	<a href="#">Changeable PIN/Password</a>	
Part D – Credential Revocation		
AL1_CM_SRR#010	<a href="#">Submit Request</a>	
Part E – Credential Status Management		
AL1_CM_CSM#010	<a href="#">Maintain Status Record</a>	
AL1_CM_CSM#020	No stipulation	No conformity requirement
AL1_CM_CSM#030	No stipulation	No conformity requirement
AL1_CM_CSM#040	<a href="#">Status Information Availability</a>	
Part F – Credential Validation / Authentication		
AL1_CM_ASS#010	<a href="#">Validation and Assertion Security</a>	
AL1_CM_ASS#015	No stipulation	No conformity requirement
AL1_CM_ASS#018	No stipulation	No conformity requirement
AL1_CM_ASS#020	<a href="#">No Post Authentication</a>	
AL1_CM_ASS#030	<a href="#">Proof of Possession</a>	
AL1_CM_ASS#035	<a href="#">Limit authentication attempts</a>	
AL1_CM_ASS#040	<a href="#">Assertion Lifetime</a>	
AL1_CM_VAS#010	No stipulation	No conformity requirement
AL1_CM_VAS#020	No stipulation	No conformity requirement
AL1_CM_VAS#030	<a href="#">Assertion assurance level</a>	
AL1_CM_VAS#040	No stipulation	No conformity requirement
AL1_CM_VAS#050	No stipulation	No conformity requirement
AL1_CM_VAS#060	<a href="#">No assertion manufacture/modification</a>	
AL1_CM_VAS#070	No stipulation	No conformity requirement
AL1_CM_VAS#080	<a href="#">Single-use assertions</a>	
AL1_CM_VAS#090	<a href="#">Single-use assertion references</a>	
AL1_CM_VAS#100	<a href="#">Bind reference to assertion</a>	

ALI_CM_VAS#110	<a href="#">Assertion expiration</a>	
----------------	--------------------------------------	--

3973

3974



3975

**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>	
AL2_CM_CTR#025	<a href="#">Authentication protocols</a>	
AL2_CM_CTR#028	<a href="#">One-time passwords</a>	
AL2_CM_CTR#030	<a href="#">System threat risk assessment and controls</a>	
AL2_CM_CTR#040	<a href="#">Specified Service's Key Management</a>	
AL2_CM_STS#010	Withdrawn	No conformity requirement
AL2_CM_OPN#010	Withdrawn	No conformity requirement
Part B – Credential Issuing		
AL2_CM_IDP#010	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>	
AL2_ID_POL#030	<a href="#">Published Proofing Policy</a>	
AL2_ID_POL#040	<a href="#">Adherence to Proofing Policy</a>	
AL2_ID_IDV#000	<a href="#">Identity Proofing classes</a>	
AL2_ID_IDV#010	<a href="#">Identity Verification Measures</a>	
AL2_ID_IPV#010	<a href="#">Required evidence</a>	
AL2_ID_IPV#020	<a href="#">Evidence checks</a>	
AL2_ID_RPV#010	<a href="#">Required evidence</a>	
AL2_ID_RPV#020	<a href="#">Evidence checks</a>	
AL2_ID_CRV#010	<a href="#">Required evidence</a>	
AL2_ID_CRV#020	<a href="#">Evidence checks</a>	
AL2_ID_AFV#000	<a href="#">Meet preceding criteria</a>	
AL2_ID_AFV#010	<a href="#">Required evidence</a>	
AL2_ID_AFV#020	<a href="#">Evidence checks</a>	
AL2_ID_IDC#010	<a href="#">Authenticate Original Credential</a>	

AL2_ID_IDC#020	<a href="#">Record Original Credential</a>	
AL2_ID_IDC#030	<a href="#">Issue Derived Credential</a>	
AL2_ID_SCV#010	<a href="#">Secondary checks</a>	
AL2_ID_VRC#010	<a href="#">Verification Records for Personal Applicants</a>	
AL2_ID_VRC#020	<a href="#">Verification Records for Affiliated Applicants</a>	
AL2_ID_VRC#025	<a href="#">Provide Subject identity records</a>	
AL2_ID_VRC#030	<a href="#">Record Retention</a>	
AL2_CM_IDP#040	<a href="#">Revision to Subscriber information</a>	
AL2_CM_CRN#010	<a href="#">Authenticated Request</a>	
AL2_CM_CRN#020	<a href="#">Unique identity</a>	
AL2_CM_CRN#030	<a href="#">Credential uniqueness</a>	
AL2_CM_CRN#035	<a href="#">Convey credential</a>	
AL2_CM_CRN#040	<a href="#">Password strength</a>	
AL2_CM_CRN#050	<a href="#">One-time password strength</a>	
AL2_CM_CRN#055	<a href="#">One-time password lifetime</a>	
AL2_CM_CRN#060	<a href="#">Software cryptographic token strength</a>	
AL2_CM_CRN#070	<a href="#">Hardware token strength</a>	
AL2_CM_CRN#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>	
AL2_CM_CRD#010	<a href="#">Notify Subject of Credential Issuance</a>	
AL2_CM_CRD#015	<a href="#">Confirm Applicant's identity (in person)</a>	
AL2_CM_CRD#016	<a href="#">Confirm Applicant's identity (remotely)</a>	
Part C – Credential Renewal and Re-issuing		
AL2_CM_RNR#010	<a href="#">Changeable PIN/Password</a>	
AL2_CM_RNR#020	<a href="#">Proof-of-possession on Renewal/Re-issuance</a>	
AL2_CM_RNR#030	<a href="#">Renewal/Re-issuance limitations</a>	
AL2_CM_RNR#040	No stipulation	No conformity requirement
AL2_CM_RNR#050	<a href="#">Record Retention</a>	
Part D – Credential Revocation		
AL2_CM_RVP#010	<a href="#">Revocation procedures</a>	
AL2_CM_RVP#020	<a href="#">Secure status notification</a>	

AL2_CM_RVP#030	<a href="#">Revocation publication</a>	
AL2_CM_RVP#040	<a href="#">Verify revocation identity</a>	
AL2_CM_RVP#045	<a href="#">Notification of Revoked Credential</a>	
AL2_CM_RVP#050	<a href="#">Revocation Records</a>	
AL2_CM_RVP#060	<a href="#">Record Retention</a>	
AL2_CM_RVR#010	<a href="#">Verify revocation identity</a>	
AL2_CM_RVR#020	<a href="#">Revocation reason</a>	
AL2_CM_RVR#030	<a href="#">Verify Subscriber as Revocant</a>	
AL2_CM_RVR#040	<a href="#">CSP as Revocant</a>	
AL2_CM_RVR#050	<a href="#">Verify Legal Representative as Revocant</a>	
AL2_CM_SRR#010	<a href="#">Submit Request</a>	
Part E – Credential Status Management		
AL2_CM_CSM#010	<a href="#">Maintain Status Record</a>	
AL2_CM_CSM#020	<a href="#">Validation of Status Change Requests</a>	
AL2_CM_CSM#030	<a href="#">Revision to Published Status</a>	
AL2_CM_CSM#040	<a href="#">Status Information Availability</a>	
AL2_CM_CSM#050	<a href="#">Inactive Credentials</a>	
Part F – Credential Validation / Authentication		
AL2_CM_ASS#010	<a href="#">Validation and Assertion Security</a>	
AL2_CM_ASS#013	No stipulation	
AL2_CM_ASS#015	<a href="#">No False Authentication</a>	
AL2_CM_ASS#020	<a href="#">No Post Authentication</a>	
AL2_CM_ASS#030	<a href="#">Proof of Possession</a>	
AL2_CM_ASS#035	<a href="#">Limit authentication attempts</a>	
AL2_CM_ASS#040	<a href="#">Assertion Lifetime</a>	
AL2_CM_AGC#010	<a href="#">Entropy level</a>	
AL2_CM_MFA#010	<a href="#">Permitted multi-factor tokens</a>	
AL2_CM_VAS#010	<a href="#">Approved cryptography</a>	
AL2_CM_VAS#020	No stipulation	No conformity requirement
AL2_CM_VAS#030	<a href="#">Assertion assurance level</a>	
AL2_CM_VAS#040	<a href="#">Notify pseudonyms</a>	
AL2_CM_VAS#050	<a href="#">Specify recipient</a>	
AL2_CM_VAS#060	<a href="#">No assertion manufacture/modification</a>	
AL2_CM_VAS#070	<a href="#">Assertion protections</a>	
AL2_CM_VAS#080	<a href="#">Single-use assertions</a>	

AL2_CM_VAS#090	<a href="#">Single-use assertion references</a>	
AL2_CM_VAS#100	<a href="#">Bind reference to assertion</a>	
AL2_CM_VAS#110	<a href="#">Assertion expiration</a>	

3976

3977

3978

**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	No stipulation	No conformity requirement
AL3_CM_CTR#020	<a href="#">Protocol threat risk assessment and controls</a>	
AL3_CM_CTR#025	<a href="#">Permitted authentication protocols</a>	
AL3_CM_CTR#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_CM_IDP#010	Withdrawn	No conformity requirement
AL3_CM_IDP#020	Withdrawn	No conformity requirement
AL3_CM_IDP#030	Withdrawn	No conformity requirement
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>	
AL3_ID_RPV#020	<a href="#">Evidence checks</a>	
AL3_ID_CRV#010	<a href="#">Required evidence</a>	
AL3_ID_CRV#020	<a href="#">Evidence checks</a>	
AL3_ID_AFV#000	<a href="#">Meet preceding criteria</a>	
AL3_ID_AFV#010	<a href="#">Required evidence</a>	

AL3_ID_AFV#020	<a href="#">Evidence checks</a>	
AL3_ID_IDC#010	<a href="#">Authenticate Original Credential</a>	
AL3_ID_IDC#020	<a href="#">Record Original Credential</a>	
AL3_ID_IDC#030	<a href="#">Issue Derived Credential</a>	
AL3_ID_SCV#010	<a href="#">Secondary checks</a>	
AL3_ID_VRC#010	<a href="#">Verification Records for Personal Applicants</a>	
AL3_ID_VRC#020	<a href="#">Verification Records for Affiliated Applicants</a>	
AL3_ID_VRC#025	<a href="#">Provide Subject Identity Records</a>	
AL3_ID_VRC#030	<a href="#">Record Retention</a>	
AL3_CM_IDP#040	<a href="#">Revision to Subscriber information</a>	
AL3_CM_CRN#010	<a href="#">Authenticated Request</a>	
AL3_CM_CRN#020	<a href="#">Unique identity</a>	
AL3_CM_CRN#030	<a href="#">Credential uniqueness</a>	
AL3_CM_CRN#035	<a href="#">Convey credential</a>	
AL3_CM_CRN#040	<a href="#">PIN/Password strength</a>	
AL3_CM_CRN#050	<a href="#">One-time password strength</a>	
AL3_CM_CRN#055	No stipulation	No conformity requirement
AL3_CM_CRN#060	<a href="#">Software cryptographic token strength</a>	
AL3_CM_CRN#070	<a href="#">Hardware token strength</a>	
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>	
AL3_CM_CRD#015	<a href="#">Confirm Applicant's identity (in person)</a>	
AL3_CM_CRD#016	<a href="#">Confirm Applicant's identity (remotely)</a>	
AL3_CM_CRD#017	<a href="#">Protected Issuance of Permanent Secrets (in person)</a>	
AL3_CM_CRD#018	<a href="#">Protected Issuance of Permanent Secrets (remotely)</a>	
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>	
AL3_CM_RNR#030	<a href="#">Renewal/Re-issuance limitations</a>	
AL3_CM_RNR#040	No stipulation	No conformity requirement
AL3_CM_RNR#050	<a href="#">Record Retention</a>	
<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>	
AL3_CM_RVP#060	<a href="#">Record Retention</a>	
AL3_CM_RVR#010	<a href="#">Verify revocation identity</a>	
AL3_CM_RVR#020	<a href="#">Revocation reason</a>	
AL3_CM_RVR#030	<a href="#">Verify Subscriber as Revocant</a>	
AL3_CM_RVR#040	<a href="#">Verify CSP as Revocant</a>	
AL3_CM_RVR#050	<a href="#">Verify Legal Representative as Revocant</a>	
AL3_CM_SRR#010	<a href="#">Submit Request</a>	
<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>	
AL3_CM_ASS#015	<a href="#">No False Authentication</a>	
AL3_CM_ASS#018	<a href="#">Ensure token validity</a>	
AL3_CM_ASS#020	<a href="#">Post Authentication</a>	
AL3_CM_ASS#035	No stipulation	No conformity requirement
AL3_CM_ASS#030	<a href="#">Proof of Possession</a>	
AL3_CM_ASS#040	<a href="#">Assertion Lifetime</a>	
AL3_CM_AGC#010	<a href="#">Entropy level</a>	
AL3_CM_MFA#010	<a href="#">Permitted multi-factor tokens</a>	
AL3_CM_VAS#010	<a href="#">Approved cryptography</a>	
AL3_CM_VAS#020	No stipulation	No conformity requirement

---

AL3_CM_VAS#030	<a href="#">Assertion assurance level</a>	
AL3_CM_VAS#040	<a href="#">Notify pseudonyms</a>	
AL3_CM_VAS#050	<a href="#">Specify recipient</a>	
AL3_CM_VAS#060	<a href="#">No assertion manufacture/modification</a>	
AL3_CM_VAS#070	<a href="#">Assertion protections</a>	
AL3_CM_VAS#080	<a href="#">Single-use assertions</a>	
AL3_CM_VAS#090	<a href="#">Single-use assertion references</a>	
AL3_CM_VAS#100	<a href="#">Bind reference to assertion</a>	
AL3_CM_VAS#110	<a href="#">Assertion expiration</a>	
AL3_CM_VAS#120	<a href="#">SSO provisions</a>	

3979

3980



3981

**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>	
AL4_CM_CTR#010	Withdrawn	No conformity requirement
AL4_CM_CTR#020	<a href="#">Protocol threat risk assessment and controls</a>	
AL4_CM_CTR#025	No stipulation	No conformity requirement
AL4_CM_CTR#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
AL4_CM_STS#020	<a href="#">Stored Secret Encryption</a>	
AL4_CM_SER#010	<a href="#">Security event logs</a>	
AL4_CM_OPN#010	Withdrawn	No conformity requirement
Part B – Credential Issuing		
AL4_CM_IDP#010	Withdrawn	No conformity requirement
AL4_CM_IDP#020	Withdrawn	No conformity requirement
AL4_CM_IDP#030	Withdrawn	No conformity requirement
AL4_ID_POL#010	<a href="#">Unique service identity</a>	
AL4_ID_POL#020	<a href="#">Unique Subject identity</a>	
AL4_ID_POL#030	<a href="#">Published Proofing Policy</a>	
AL4_ID_POL#040	<a href="#">Adherence to Proofing Policy</a>	
AL4_ID_IDV#000	<a href="#">Identity Proofing classes</a>	
AL4_ID_IDV#010	<a href="#">Identity Verification Measures</a>	
AL4_ID_IPV#010	<a href="#">Required evidence</a>	
AL4_ID_IPV#020	No stipulation	No conformity requirement
AL4_ID_IPV#030	<a href="#">Evidence checks – primary ID</a>	
AL4_ID_IPV#040	<a href="#">Evidence checks – secondary ID</a>	
AL4_ID_IPV#050	<a href="#">Applicant knowledge checks</a>	

AL4_ID_AFV#000	<a href="#">Meet preceding criteria</a>	
AL4_ID_AFV#010	<a href="#">Required evidence</a>	
AL4_ID_AFV#020	<a href="#">Evidence checks</a>	
AL4_ID_IDC#010	<a href="#">Authenticate Original Credential</a>	
AL4_ID_IDC#020	<a href="#">Record Original Credential</a>	
AL4_ID_IDC#030	<a href="#">Issue Derived Credential</a>	
AL4_ID_SCV#010	<a href="#">Secondary checks</a>	
AL4_ID_VRC#010	<a href="#">Verification Records for Personal Applicants</a>	
AL4_ID_VRC#020	<a href="#">Verification Records for Affiliated Applicants</a>	
AL4_ID_VRC#025	<a href="#">Provide Subject identity records</a>	
AL4_ID_VRC#030	<a href="#">Record Retention</a>	
AL4_CM_IDP#040	<a href="#">Revision to Subscriber information</a>	
AL4_CM_CRN#010	<a href="#">Authenticated Request</a>	
AL4_CM_CRN#020	<a href="#">Unique identity</a>	
AL4_CM_CRN#030	<a href="#">Credential uniqueness</a>	
AL4_CM_CRN#035	<a href="#">Convey credential</a>	
AL4_CM_CRN#040	<a href="#">PIN/Password strength</a>	
AL4_CM_CRN#050	<a href="#">One-time password strength</a>	
AL4_CM_CRN#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>	
AL4_CM_CRN#075	<a href="#">Multi-factor hardware cryptographic token strength</a>	
AL4_CM_CRN#080	<a href="#">Binding of key</a>	
AL4_CM_CRN#090	<a href="#">Nature of Subject</a>	
AL4_CM_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>	
AL4_CM_CRD#015	<a href="#">Confirm Applicant's identity (in person)</a>	
AL4_CM_CRD#016	No stipulation	No conformity requirement
AL4_CM_CRD#017	<a href="#">Protected Issuance of Permanent Secrets (in person)</a>	
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>	
AL4_CM_RNR#030	<a href="#">Renewal/Re-issuance limitations</a>	
AL4_CM_RNR#040	No stipulation	No conformity requirement
AL4_CM_RNR#050	<a href="#">Record Retention</a>	
Part D – Credential Revocation		
AL4_CM_RVP#010	<a href="#">Revocation procedures</a>	
AL4_CM_RVP#020	<a href="#">Secure status notification</a>	
AL4_CM_RVP#030	<a href="#">Revocation publication</a>	
AL4_CM_RVP#040	<a href="#">Verify Revocation Identity</a>	
AL4_CM_RVP#050	<a href="#">Revocation Records</a>	
AL4_CM_RVP#060	<a href="#">Record Retention</a>	
AL4_CM_RVR#010	<a href="#">Verify revocation identity</a>	
AL4_CM_RVR#020	<a href="#">Revocation reason</a>	
AL4_CM_RVR#030	<a href="#">Verify Subscriber as Revocant</a>	
AL4_CM_RVR#040	<a href="#">Verify CSP as Revocant</a>	
AL4_CM_RVR#050	<a href="#">Verify Legal Representative as Revocant</a>	
AL4_CM_RKY#010	<a href="#">Verify Requestor as Subscriber</a>	
AL4_CM_RKY#020	<a href="#">Re-key requests other than Subject</a>	
AL4_CM_SRR#010	<a href="#">Submit Request</a>	
Part E – Credential Status Management		
AL4_CM_CSM#010	<a href="#">Maintain Status Record</a>	
AL4_CM_CSM#020	<a href="#">Validation of Status Change Requests</a>	
AL4_CM_CSM#030	<a href="#">Revision to Published Status</a>	
AL4_CM_CSM#040	<a href="#">Status Information Availability</a>	
AL4_CM_CSM#050	<a href="#">Inactive Credentials</a>	
Part F – Credential Validation / Authentication		
AL4_CM_ASS#010	<a href="#">Validation and Assertion Security</a>	
AL4_CM_ASS#015	<a href="#">No False Authentication</a>	
AL3_CM_ASS#018	<a href="#">Ensure token validity</a>	
AL4_CM_ASS#020	<a href="#">Post Authentication</a>	
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>	
AL4_CM_AGC#020	<a href="#">Limit password validity</a>	
AL4_CM_MFA#010	<a href="#">Permitted multi-factor tokens</a>	
AL4_CM_VAS#010	<a href="#">Approved cryptography</a>	
AL4_CM_VAS#020	No stipulation	No conformity requirement
AL4_CM_VAS#030	<a href="#">Assertion assurance level</a>	
AL4_CM_VAS#040	<a href="#">Notify pseudonyms</a>	
AL4_CM_VAS#050	<a href="#">Specify recipient</a>	
AL4_CM_VAS#060	<a href="#">No assertion manufacture/modification</a>	
AL4_CM_VAS#070	<a href="#">Assertion protections</a>	
AL4_CM_VAS#080	<a href="#">Single-use assertions</a>	
AL4_CM_VAS#090	<a href="#">Single-use assertion references</a>	
AL4_CM_VAS#100	<a href="#">Bind reference to assertion</a>	
AL4_CM_VAS#110	<a href="#">Assertion expiration</a>	
AL4_CM_VAS#120	No stipulation	No conformity requirement

## 3982 **6 REFERENCES**

---

3983

3984 [CAF] Louden, Chris, Spencer, Judy; Burr, Bill; Hawkins, Kevin; Temoshok, David;  
3985 Cornell, John; Wilsher, Richard G.; Timchak, Steve; Sill, Stephen; Silver, Dave; Harrison,  
3986 Von; eds., "E-Authentication Credential Assessment Framework (CAF)," E-  
3987 Authentication Initiative, Version 2.0.0 (March 16, 2005).  
3988 <http://www.cio.gov/eauthentication/documents/CAF.pdf>

3989

3990 [EAP CSAC 04011] "EAP working paper: Identity Proofing Service Assessment Criteria  
3991 (ID-SAC)," Electronic Authentication Partnership, Draft 0.1.3 (July 20, 2004)  
3992 [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)

3993

3994 [EAPTrustFramework] "Electronic Authentication Partnership Trust Framework"  
3995 Electronic Authentication Partnership, Version 1.0. (January 6, 2005)  
3996 [http://eap.projectliberty.org/docs/Trust\\_Framework\\_010605\\_final.pdf](http://eap.projectliberty.org/docs/Trust_Framework_010605_final.pdf)

3997

3998 [FIPS140-2] "Security Requirements for Cryptographic Modules" Federal Information  
3999 Processing Standards. (May 25, 2001) [http://csrc.nist.gov/publications/fips/fips140-](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)  
4000 [2/fips1402.pdf](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)

4001

4002 [IS27001] ISO/IEC 27001:2005 "Information technology - Security techniques -  
4003 Requirements for information security management systems" International Organization  
4004 for Standardization.  
4005 [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)

4006

4007 [M-04-04] Bolton, Joshua B., ed., "E-Authentication Guidance for Federal Agencies,"  
4008 Office of Management and Budget, (December 16, 2003).  
4009 <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>

4010

4011 [NIST800-63] Burr, William E.; Dodson, Donna F.; Polk, W. Timothy; eds., "Electronic  
4012 Authentication Guideline: : Recommendations of the National Institute of Standards and  
4013 Technology," Version 1.0.2, National Institute of Standards and Technology, (April,  
4014 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)

4015

4016 [RFC 3647] Chokhani, S.; Ford, W.; Sabett, R.; Merrill, C.; Wu, S.; eds., "Internet X.509  
4017 Public Key Infrastructure Certificate Policy and Certification Practices Framework," The  
4018 Internet Engineering Task Force (November, 2003). <http://www.ietf.org/rfc/rfc3647.txt>  
4019  
4020

- 4021 Revision History
- 4022 1. 2008-05-08 – Identity Assurance Framework Version 1.0 Initial Draft
- 4023 a. Released by Liberty Alliance
- 4024 b. Revision and scoping of Initial Draft release
- 4025 2. 2008-06-23 – Identity Assurance Framework Version 1.1 Final Draft
- 4026 a. Released by Liberty Alliance
- 4027 b. Inclusion of comments to Final Draft
- 4028 3. 2009-10-01 – Identity Assurance Framework Version 1.1 Final Draft
- 4029 a. Documents contributed to Kantara Initiative by Liberty Alliance
- 4030 4. 2010-04-dd – SAC Version 2.0
- 4031 a. Released by Kantara Initiative
- 4032 b. Significant scope build
- 4033 c. Original Identity Assurance Framework all inclusive document broken in
- 4034 to a set of documents with specific focus:
- 4035 i. Kantara IAF-1000-Overview
- 4036 ii. Kantara IAF-1100-Glossary
- 4037 iii. Kantara IAF-1200-Levels of Assurance
- 4038 iv. Kantara IAF-1300-Assurance Assessment Scheme
- 4039 v. Kantara IAF-1400-Service Assessment Criteria (this document)
- 4040 vi. Kantara IAF-1600-Assessor Qualifications and Requirements
- 4041 5. 2012-10-10 - SAC Version 3.0
- 4042 a. Revision to accommodate Full/Component Service Assessment and
- 4043 Approval.
- 4044 6. 2013-11-dd – SAC Version 4.0 (pending approval of
- 4045 a. Revision to map SAC against NIST SP 800-63-2;
- 4046 b. Alignment to revised Glossary;
- 4047 c. Further one-off changes to respond to tickets listed below.
- 4048

4049

## Tickets Resolved

4050

The following 'tickets' (Change Request/Fault Notifications) have been resolved with publication of this document:

4051

4052

Ticket #	Problem	Resolution
	ISM#090 required 3 <sup>rd</sup> -party assessment in addition to the independent KI Assessment.	Remove criterion at all ALs.

4053