

1

2 Identity Assurance Framework: 3 Service Assessment Criteria

4 **Version:** 5.0
5 **Date:** 2016-08-15
6 **Status:** **Final Recommendation**

7
8 **Approval:** 2016-09-08

9 **Editor:** Richard G. Wilsher
10 Zyigma LLC

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

12 Abstract

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

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

26

27 **Notice**

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

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

47 Copyright: The content of this document is copyright of Kantara Initiative, Inc..
48 © 2016 Kantara Initiative, Inc.

49
50

51		Contents	
52			
53	1	INTRODUCTION	5
54	1.1	Changes in this revision	5
55	2	ASSURANCE LEVELS.....	7
56	3	SERVICE ASSESSMENT CRITERIA - GENERAL.....	8
57	3.1	Context and Scope	8
58	3.2	Criteria Applicability	8
59	3.3	Status and Readership	9
60	3.4	Criteria Descriptions	9
61	3.5	Terminology	11
62	4	COMMON ORGANIZATIONAL SERVICE ASSESSMENT CRITERIA	12
63	4.1	Assurance Level 1	12
64	4.1.1	Enterprise and Service Maturity	12
65	4.1.2	Notices and User information	13
66	4.1.3	No stipulation.....	14
67	4.1.4	No stipulation.....	14
68	4.1.5	No stipulation.....	14
69	4.1.6	No stipulation.....	14
70	4.1.7	Secure Communications	14
71	4.2	Assurance Level 2.....	15
72	4.2.1	Enterprise and Service Maturity	15
73	4.2.2	Notices and User Information/Agreements	16
74	4.2.3	Information Security Management	18
75	4.2.4	Security-relevant Event (Audit) Records.....	20
76	4.2.5	Operational infrastructure	20
77	4.2.6	External Services and Components	21
78	4.2.7	Secure Communications	21
79	4.3	Assurance Level 3.....	24
80	4.3.1	Enterprise and Service Maturity	24
81	4.3.2	Notices and User Information	25
82	4.3.3	Information Security Management	27
83	4.3.4	Security-Relevant Event (Audit) Records	29
84	4.3.5	Operational Infrastructure.....	30
85	4.3.6	External Services and Components	31
86	4.3.7	Secure Communications	31
87	4.4	Assurance Level 4.....	34
88	4.4.1	Enterprise and Service Maturity	34
89	4.4.2	Notices and Subscriber Information/Agreements.....	35
90	4.4.3	Information Security Management	37
91	4.4.4	Security-Related (Audit) Records.....	39
92	4.4.5	Operational Infrastructure.....	40
93	4.4.6	External Services and Components	41

94	4.4.7	Secure Communications	41
95	4.5	Compliance Tables.....	; Error! Marcador no definido.
96	5	OPERATIONAL SERVICE ASSESSMENT CRITERIA	43
97	5.1	Assurance Level 1.....	43
98	5.1.1	Part A - Credential Operating Environment	43
99	5.1.2	Part B - Credential Issuing.....	45
100	5.1.3	Part C - Credential Renewal and Re-issuing.....	49
101	5.1.4	Part D - Credential Revocation.....	49
102	5.1.5	Part E - Credential Status Management.....	50
103	5.1.6	Part F - Credential Verification/Authentication.....	50
104	5.2	Assurance Level 2.....	54
105	5.2.1	Part A - Credential Operating Environment	54
106	5.2.2	Part B - Credential Issuing.....	57
107	5.2.3	Part C - Credential Renewal and Re-issuing.....	68
108	5.2.4	Part D - Credential Revocation.....	69
109	5.2.5	Part E - Credential Status Management.....	72
110	5.2.6	Part F - Credential Verification/Authentication.....	72
111	5.3	Assurance Level 3.....	77
112	5.3.1	Part A - Credential Operating Environment	77
113	5.3.2	Part B - Credential Issuing.....	81
114	5.3.3	Part C - Credential Renewal and Re-issuing.....	92
115	5.3.4	Part D - Credential Revocation.....	93
116	5.3.5	Part E - Credential Status Management.....	96
117	5.3.6	Part F - Credential Verification/Authentication.....	97
118	5.4	Assurance Level 4.....	101
119	5.4.1	Part A - Credential Operating Environment	101
120	5.4.2	Part B - Credential Issuing.....	105
121	5.4.3	Part C - Credential Renewal and Re-issuing.....	114
122	5.4.4	Part D - Credential Revocation.....	115
123	5.4.5	Part E - Credential Status Management.....	119
124	5.4.6	Part F - Credential Verification/Authentication.....	119
125	5.5	Compliance Tables.....	; Error! Marcador no definido.
126	6	REFERENCES	125
127	7	REVISION HISTORY	128
128			

129 **1 INTRODUCTION**

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

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

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

148 Assurance Levels (ALs) are the levels of trust associated with a credential as measured by
149 the associated technology, processes, and policy and practice statements controlling the
150 operational environment. The IAF defers to the guidance provided by the U.S. National
151 Institute of Standards and Technology (NIST) Special Publication 800-63 version 2
152 [[NIST800-63](#)] which outlines four levels of assurance, ranging in confidence level from
153 low to very high. Use of ALs is determined by the level of confidence or trust (i.e.
154 assurance) necessary to mitigate risk in the transaction.

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

162 **1.1 Changes in this revision**

163 Consistent reference to 'assessment' used, removing use of 'evaluation', when referring
164 to determining CSPs' conformity to the criteria herein.

165 Replacement of references to FIPS 140-2 with like to ISO/IEC 19790:2012.

- 166 Consistent reference to validation, not evaluation, when referring to any program which
167 determining that cryptographic modules adhere to ISO/IEC 19790:2012.
- 168 Removal of all conformance tables, since others are available in better formats.

169 **2 ASSURANCE LEVELS**

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

175 **3 SERVICE ASSESSMENT CRITERIA - GENERAL**

176 **3.1 Context and Scope**

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

183 **1) Organizational Criteria:**

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

186 **2) Operational Criteria:**

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

190 **3.2 Criteria Applicability**

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

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

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

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

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

206 3.3 Status and Readership

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

212 The description of criteria in this document is required reading for all organizations
213 wishing to become Kantara-Approved credential services, and also for those wishing to
214 become Kantara-Accredited Assessors. It is also recommended reading for those
215 involved in the governance and day-to-day administration of the Identity Assurance
216 Framework.

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

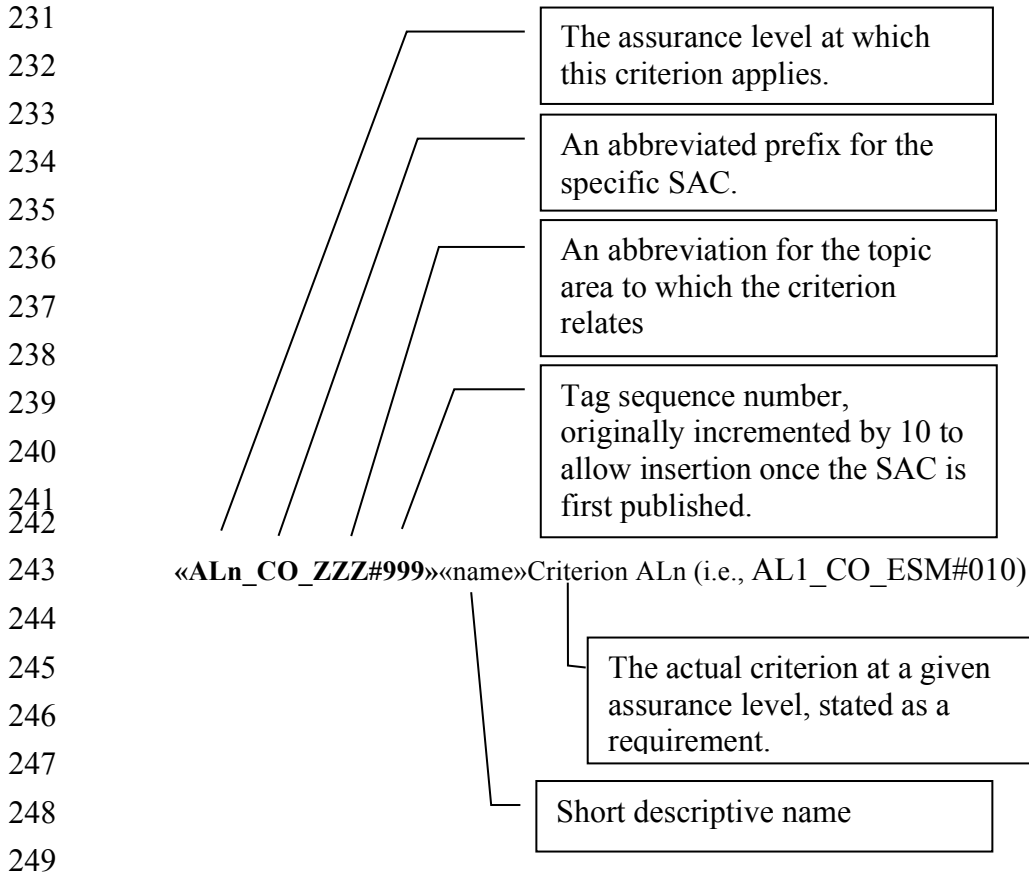
220 3.4 Criteria Descriptions

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

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

229

230 The criteria are described as follows:



250 When a given criterion changes (i.e. becomes more rigorous) at higher Assurance Levels
251 the new or revised text is **shown in bold** or **[Omitted]** is indicated where text has been
252 removed. With the obvious exception of AL1, when a criterion is first introduced it is
253 also shown in bold.

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

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

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

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

267 3.5 Terminology

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

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

273 4 COMMON ORGANIZATIONAL 274 SERVICE ASSESSMENT CRITERIA

275 The Service Assessment Criteria in this section establish the general business and
276 organizational requirements for conformity of services and service providers at all
277 Assurance Levels (AL) – refer to Section 2. These criteria are generally referred to
278 elsewhere within IAWG documentation as CO-SAC and can be identified by their tag
279 “ALn_CO_ xxxx”.

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

282 4.1 Assurance Level 1

283 4.1.1 Enterprise and Service Maturity

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

287 An enterprise and its specified service must:

288 *ALI_CO_ESM#010 Established enterprise*

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

291 *ALI_CO_ESM#020 Withdrawn*

292 Withdrawn

293 *ALI_CO_ESM#030 Legal & Contractual compliance*

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

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

301 *ALI_CO_ESM#040 No stipulation*

302 *ALI_CO_ESM#050 Data Retention and Protection*

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

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

309 *ALI_CO_ESM#055 Termination provisions*

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

315 **Guidance:** Termination covers the cessation of the business activities, the service
316 provider itself ceasing business operations altogether, change of ownership of the service-
317 providing business, and other similar events which change the status and/or operations of
318 the service provider in any way which interrupts the continued provision of the specific
319 service.

320 **4.1.2 Notices and User information**

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

323 An enterprise and its specified service must:

324 *ALI_CO_NUI#010 General Service Definition*

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

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

330 *ALI_CO_NUI#020 Service Definition inclusions*

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

333 a) a Privacy Policy.

334

335 *ALI_CO_NUI#030 Due notification*

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

339 *ALI_CO_NUI#040 User Acceptance*

340 Require Subscribers and Subjects to:

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

347 *ALI_CO_NUI#050 Record of User Acceptance*

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

352 **4.1.3 No stipulation**

353 **4.1.4 No stipulation**

354 **4.1.5 No stipulation**

355 **4.1.6 No stipulation**

356 **4.1.7 Secure Communications**

357 *ALI_CO_SCO#010 No stipulation*

358 *ALI_CO_SCO#015 No stipulation*

359 *ALI_CO_SCO#016 No stipulation*

360 *ALI_CO_SCO#020 Limited access to shared secrets*

361 Ensure that:

- 362 a) access to shared secrets shall be subject to discretionary controls which permit
363 access to those roles/applications needing such access;
364 b) stored shared secrets are not held in their plaintext form unless given adequate
365 physical or logical protection;
366 c) any plaintext passwords or secrets are not transmitted across any public or
367 unsecured network.

368

369 **4.2 Assurance Level 2**

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

373 **4.2.1 Enterprise and Service Maturity**

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

376 An enterprise and its specified service must:

377 *AL2_CO_ESM#010 Established enterprise*

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

380 *AL2_CO_ESM#020 Withdrawn*

381 Withdrawn

382 *AL2_CO_ESM#030 Legal & Contractual compliance*

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

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

393 *AL2_CO_ESM#040 Financial Provisions*

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

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

404 *AL2_CO_ESM#050 Data Retention and Protection*

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

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

415 *AL2_CO_ESM#055 Termination provisions*

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

421 **Guidance:** Termination covers the cessation of the business activities, the service
422 provider itself ceasing business operations altogether, change of ownership of the service-
423 providing business, and other similar events which change the status and/or operations of
424 the service provider in any way which interrupts the continued provision of the specific
425 service.

426 **4.2.2 Notices and User Information/Agreements**

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

430 An enterprise and its specified service must:

431 *AL2_CO_NUI#010 General Service Definition*

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

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

438 *AL2_CO_NUI#020 Service Definition inclusions*

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

- 441 a) Privacy, Identity Proofing & Verification, Renewal/Re-issuance, and
442 Revocation and Termination Policies;
443 b) the country in or legal jurisdiction under which the service is operated;
444 c) if different from the above, the legal jurisdiction under which Subscriber and
445 any relying party agreements are entered into;
446 d) applicable legislation with which the service complies;
447 e) obligations incumbent upon the CSP;
448 f) obligations incumbent upon each class of user of the service, e.g. Relying
449 Parties, Subscribers and Subjects;
450 g) notifications and guidance for relying parties, especially in respect of actions
451 they are expected to take should they choose to rely upon the service;
452 h) statement of warranties;
453 i) statement of liabilities toward Subscribers, Subjects and Relying Parties;
454 j) procedures for notification of changes to terms and conditions;
455 k) steps the CSP will take in the event that it chooses or is obliged to terminate
456 the service;
457 l) availability of the specified service *per se* and of its help desk facility.

458 *AL2_CO_NUI#025 AL2 Configuration Specification*

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

462 *AL2_CO_NUI#030 Due notification*

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

468 *AL2_CO_NUI#040 User Acceptance*

469 Require Subscribers and Subjects to:

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

476 *AL2_CO_NUI#050 Record of User Acceptance*

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

481 *AL2_CO_NUI#060 Withdrawn*

482 Withdrawn.

483 *AL2_CO_NUI#070 Change of Subscriber Information*

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

488 *AL2_CO_NUI#080 Withdrawn*

489 Withdrawn.

490 **4.2.3 Information Security Management**

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

496 An enterprise and its specified service must:

497 *AL2_CO_ISM#010 Documented policies and procedures*

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

502 *AL2_CO_ISM#020 Policy Management and Responsibility*

503 **Have a clearly defined managerial role, at a senior level, in which full responsibility**
504 **for the business's security policies is vested and from which review, approval, and**
505 **promulgation of policy and related procedures is applied and managed. The latest**
506 **approved versions of these policies must be applied at all times.**

507 *AL2_CO_ISM#030 Risk Management*

508 **Demonstrate a risk management methodology that adequately identifies and**
509 **mitigates risks related to the specified service and its user community.**

510 *AL2_CO_ISM#040 Continuity of Operations Plan*

511 **Have and keep updated a Continuity of Operations Plan that covers disaster**
512 **recovery and the resilience of the specified service.**

513 *AL2_CO_ISM#050 Configuration Management*

514 **Demonstrate that there is in place a configuration management system that at least**
515 **includes:**

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

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

519 *AL2_CO_ISM#060 Quality Management*

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

522 *AL2_CO_ISM#070 System Installation and Operation Controls*

523 **Apply controls during system development, procurement installation, and operation**
524 **that protect the security and integrity of the system environment, hardware,**
525 **software, and communications.**

526 *AL2_CO_ISM#080 Internal Service Audit*

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

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

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

542 *AL2_CO_ISM#090 Withdrawn*

543 Withdrawn.

544 *AL2_CO_ISM#100 Audit Records*

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

551 *AL2_CO_ISM#110 Withdrawn*

552 Withdrawn.

553 4.2.4 Security-relevant Event (Audit) Records

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

556 An enterprise and its specified service must:

557 *AL2_CO_SER#010 Security event logging*

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

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

566 4.2.5 Operational infrastructure

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

570 An enterprise and its specified service must:

571 *AL2_CO_OPN#010 Withdrawn*

572 Withdrawn.

573 *AL2_CO_OPN#020 Defined security roles*

574 **Define, by means of a job description, the roles and responsibilities for each service-**
575 **related security-relevant task, relating it to specific procedures, (which shall be set**
576 **out in the ISMS, or other IT security management methodology recognized by a**
577 **government or professional body) and other service-related job descriptions and**
578 **applicable policies, processes and procedures** {source [5415] KI.10.2.2.1#24}. **Where the**
579 **role is security-critical or where special privileges or shared duties exist, these must**
580 **be specifically identified as such, including the applicable access privileges relating**
581 **to logical and physical parts of the service's operations.**

582 *AL2_CO_OPN#030 Personnel recruitment*

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

586 *AL2_CO_OPN#040 Personnel skills*

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

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

592 *AL2_CO_OPN#050 Adequacy of Personnel resources*

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

595 *AL2_CO_OPN#060 Physical access control*

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

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

602 *AL2_CO_OPN#070 Logical access control*

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

605 **4.2.6 External Services and Components**

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

609 An enterprise and its specified service must:

610 *AL2_CO_ESC#010 Contracted policies and procedures*

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

616 *AL2_CO_ESC#020 Visibility of contracted parties*

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

622 **4.2.7 Secure Communications**

623 An enterprise and its specified service must:

624 *AL2_CO_SCO#010 Secure remote communications*

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

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

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

635 *AL2_CO_SCO#015 Verification / Authentication confirmation messages*

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

642 *AL2_CO_SCO#016 Withdrawn*

643 Now AL2_CM_RVP#045

644 *AL2_CO_SCO#020 Limited access to shared secrets*

645 Ensure that:

- 646 a) access to shared secrets shall be subject to discretionary controls that only permit
647 access by those roles/applications requiring such access;
648 b) stored shared secrets are not held in their plaintext form unless given adequate
649 physical or logical protection;
650 c) any plaintext passwords or secrets are not transmitted across any public or
651 unsecured network;
652 d) **any long-term (i.e., not session) shared secrets are revealed only to the**
653 **Subject or to the CSP’s direct agents (bearing in mind (a) above).**
654

655 **In addition, these roles should be defined and documented by the CSP in accordance**
656 **with AL2_CO_OPN#020 above.**

657 *AL2_CO_SCO#030 Logical protection of shared secrets*

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

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

- 663 **b) encryption using an Approved algorithm and modes, and the shared secret**
664 **decrypted only when immediately required for authentication, or;**
665 **c) any secure method allowed to protect shared secrets at Level 3 or 4.**
- 666

667 4.3 Assurance Level 3

668 Achieving AL3 requires meeting more stringent criteria in addition to all criteria required
669 to achieve AL2.

670 4.3.1 Enterprise and Service Maturity

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

673 An enterprise and its specified service must:

674 *AL3_CO_ESM#010 Established enterprise*

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

677 *AL3_CO_ESM#020 Withdrawn*

678 Withdrawn

679 *AL3_CO_ESM#030 Legal & Contractual compliance*

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

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

690 *AL3_CO_ESM#040 Financial Provisions*

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

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

701 *AL3_CO_ESM#050 Data Retention and Protection*

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

708 *AL3_CO_ESM#055 Termination provisions*

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

714 **Guidance:** Termination covers the cessation of the business activities, the service
715 provider itself ceasing business operations altogether, change of ownership of the service-
716 providing business, and other similar events which change the status and/or operations of
717 the service provider in any way which interrupts the continued provision of the specific
718 service.

719 *AL3_CO_ESM#060 Ownership*

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

723 *AL3_CO_ESM#070 Independent management and operations*

724 **Demonstrate that, for the purposes of providing the specified service, its**
725 **management and operational structures are distinct, autonomous, have discrete**
726 **legal accountability, and operate according to separate policies, procedures, and**
727 **controls.**

728 **4.3.2 Notices and User Information**

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

732 An enterprise and its specified service must:

733 *AL3_CO_NUI#010 General Service Definition*

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

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

740 *AL3_CO_NUI#020 Service Definition inclusions*

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

- 743 a) Privacy, Identity Proofing & Verification, Renewal/Re-issuance, and Revocation
744 and Termination Policies;)
- 745 b) the country in or the legal jurisdiction under which the service is operated;
- 746 c) if different to the above, the legal jurisdiction under which Subscriber and any
747 relying party agreements are entered into;
- 748 d) applicable legislation with which the service complies;
- 749 e) obligations incumbent upon the CSP;
- 750 f) obligations incumbent upon each class of user of the service, e.g. Relying Parties,
751 Subscribers and Subjects, ...;
- 752 g) notifications and guidance for relying parties, especially in respect of actions they
753 are expected to take should they choose to rely upon the service's product;
- 754 h) statement of warranties;
- 755 i) statement of liabilities toward both Subjects and Relying Parties;
- 756 j) procedures for notification of changes to terms and conditions;
- 757 k) steps the CSP will take in the event that it chooses or is obliged to terminate the
758 service;
- 759 l) availability of the specified service *per se* and of its help desk facility.

760 *AL3_CO_NUI#025 AL3 Configuration Specification*

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

764 *AL3_CO_NUI#030 Due notification*

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

770 *AL3_CO_NUI#040 User Acceptance*

771 Require Subscribers and Subjects to:

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

778 *AL3_CO_NUI#050 Record of User Acceptance*

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

783 *AL3_CO_NUI#060 Withdrawn*
784 Withdrawn.

785 *AL3_CO_NUI#070 Change of Subscriber Information*
786 Require and provide the mechanisms for Subscribers and Subjects to provide in a timely
787 manner full and correct amendments should any of their recorded information change, as
788 required under the terms of their use of the service, and only after the Subscriber's and/or
789 Subject's identity has been authenticated.

790 *AL3_CO_NUI#080 Withdrawn*
791 Withdrawn.

792 **4.3.3 Information Security Management**

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

798 An enterprise and its specified service must:

799 *AL3_CO_ISM#010 Documented policies and procedures*
800 Have documented all security-relevant administrative management and technical policies
801 and procedures. The enterprise must ensure that these are based upon recognized
802 standards, published references or organizational guidelines, are adequate for the
803 specified service, and are implemented in the manner intended.

804 *AL3_CO_ISM#020 Policy Management and Responsibility*
805 Have a clearly defined managerial role, at a senior level, where full responsibility for the
806 business' security policies is vested and from which review, approval, and promulgation
807 of policy and related procedures is applied and managed. The latest approved versions of
808 these policies must be applied at all times.

809 *AL3_CO_ISM#030 Risk Management*
810 Demonstrate a risk management methodology that adequately identifies and mitigates
811 risks related to the specified service and its user community **and must show that a risk**
812 **assessment review is performed at least once every six months, such as adherence to**
813 **CobIT or [IS27001] practices.**

814 *AL3_CO_ISM#040 Continuity of Operations Plan*

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

818 *AL3_CO_ISM#050 Configuration Management*

819 Demonstrate that there is in place a configuration management system that at least
820 includes:

- 821 a) version control for software system components;
- 822 b) timely identification and installation of all organizationally-approved patches for
823 any software used in the provisioning of the specified service;
- 824 c) **version control and managed distribution for all documentation associated**
825 **with the specification, management, and operation of the system, covering**
826 **both internal and publicly available materials.**

827 *AL3_CO_ISM#060 Quality Management*

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

830 *AL3_CO_ISM#070 System Installation and Operation Controls*

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

- 834 a) **the software and hardware development environments, for customized**
835 **components;**
- 836 b) **the procurement process for commercial off-the-shelf (COTS) components;**
- 837 c) **contracted consultancy/support services;**
- 838 d) **shipment of system components;**
- 839 e) **storage of system components;**
- 840 f) **installation environment security;**
- 841 g) **system configuration;**
- 842 h) **transfer to operational status.**

843 *AL3_CO_ISM#080 Internal Service Audit*

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

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

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

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

856 *AL3_CO_ISM#090 Withdrawn*
857 Withdrawn.

858 *AL3_CO_ISM#100 Audit Records*
859 Retain records of all audits, both internal and independent, for a period which, as a
860 minimum, fulfills its legal obligations and otherwise for greater periods either as it may
861 have committed to in its Service Definition or required by any other obligations it has
862 with/to a Subscriber or Subject, and which in any event is not less than 36 months. Such
863 records must be held securely and be protected against unauthorized access, loss,
864 alteration, public disclosure, or unapproved destruction.

865 *AL3_CO_ISM#110 Withdrawn*
866 Withdrawn.

867 *AL3_CO_ISM#120 Best Practice Security Management*
868 **Have in place an Information Security Management System (ISMS), or other IT**
869 **security management methodology recognized by a government or professional**
870 **body, that follows best practices as accepted by the information security industry**
871 **and that applies and is appropriate to the CSP in question. All requirements**
872 **expressed in preceding criteria in this section must *inter alia* fall wholly within the**
873 **scope of this ISMS or selected recognized alternative.**

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

877 **4.3.4 Security-Relevant Event (Audit) Records**

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

880 An enterprise and its specified service must:

881 *AL3_CO_SER#010 Security Event Logging*
882 Maintain a log of all relevant security events concerning the operation of the service,
883 together with an accurate record of the time at which the event occurred (time-stamp),
884 and retain such records with appropriate protection and controls to ensure successful
885 retrieval, accounting for Service Definition risk management requirements, applicable
886 legislation, and organizational policy.

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

890 4.3.5 Operational Infrastructure

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

894 An enterprise and its specified service must:

895 *AL3_CO_OPN#010* *Withdrawn*

896 *Withdrawn.*

897 *AL3_CO_OPN#020* *Defined security roles*

898 Define, by means of a job description, the roles and responsibilities for each service-
899 related security-relevant task, relating it to specific procedures (which shall be set out in
900 the ISMS, or other IT security management methodology recognized by a government or
901 professional body) and other service-related job descriptions and applicable policies,
902 processes and procedures. {source [5415] KI.10.2.2.1#24} Where the role is security-critical
903 or where special privileges or shared duties exist, these must be specifically identified as
904 such, including the applicable access privileges relating to logical and physical parts of
905 the service's operations.

906 *AL3_CO_OPN#025* *Acknowledgement of assigned security roles and responsibilities*

907 **Require those assigned to critical security roles to acknowledge, by signature (hand-**
908 **written or electronic), that they have read and understood the system documentation**
909 **applicable to their role(s) and that they accept the associated responsibilities.** {source
910 [5415] KI.10.2.2.1#24}

911 *AL3_CO_OPN#030* *Personnel recruitment*

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

917 *AL3_CO_OPN#040* *Personnel skills*

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

923 *AL3_CO_OPN#050* *Adequacy of Personnel resources*

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

926 *AL3_CO_OPN#060* *Physical access control*

927 Apply physical access control mechanisms to ensure that:

928 a) access to sensitive areas is restricted to authorized personnel;

- 929 b) all removable media and paper documents containing sensitive information as
930 plain-text are stored in secure containers;
931 c) a minimum of two persons is required to enable access to any cryptographic
932 modules;
933 d) there is 24/7 monitoring for unauthorized intrusions.

934 *AL3_CO_OPN#070 Logical access control*

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

937 **4.3.6 External Services and Components**

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

941 An enterprise and its specified service must:

942 *AL3_CO_ESC#010 Contracted policies and procedures*

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

948 *AL3_CO_ESC#020 Visibility of contracted parties*

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

954 **4.3.7 Secure Communications**

955 An enterprise and its specified service must:

956 *AL3_CO_SCO#010 Secure remote communications*

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

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

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

967 *AL3_CO_SCO#015 Verification / Authentication confirmation messages*

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

973 *AL3_CO_SCO#016 Withdrawn*

974 *AL3_CO_SCO#020 Limited access to shared secrets*

975 Ensure that:

- 976 a) access to shared secrets shall be subject to discretionary controls that permit
977 access to those roles/applications requiring such access;
- 978 b) stored shared secrets are **encrypted such that:**
- 979 i **the encryption key for the shared secret file is encrypted under a key**
980 **held in either an [IS19790] Level 2 (or higher) validated¹ hardware**
981 **cryptographic module or any [IS19790] Level 3 or 4 validated**
982 **cryptographic module, or equivalent, as established by a recognized**
983 **national technical authority, and decrypted only as immediately**
984 **required for an authentication operation;**
- 985 ii **they are protected as a key within the boundary of either an [IS19790]**
986 **Level 2 (or higher) validated hardware cryptographic module or any**
987 **[IS19790] Level 3 or 4 validated cryptographic module, or equivalent,**
988 **as established by a recognized national technical authority, and are**
989 **not exported from the module in plaintext;**
- 990 c) any long-term (i.e., not session) shared secrets are revealed only to the Subject
991 and the CSP’s direct agents (bearing in mind (a) above).

992
993 In addition, these roles should be defined and documented by the CSP in accordance with
994 AL3_CO_OPN#020 above.

995 *AL3_CO_SCO#030 Logical protection of shared secrets*

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

¹ Where jurisdictions have validation programs for cryptographic modules then validated components shall be used. Where no validation program exists within a jurisdiction cryptographic components should either have been validated under another program, such as one operating in their country of manufacture, or should be carry their manufacturer’s self-attestation of conformity to ISO/IEC 19790 or another standard recognized by a national technical authority. This footnote applies to all requirements for validated modules.

- 997 a) concatenation of the password to a salt and/or username which is then hashed
 - 998 with an Approved algorithm such that the computations used to conduct a
 - 999 dictionary or exhaustion attack on a stolen password file are not useful to attack
 - 1000 other similar password files, or;
 - 1001 b) encryption using an Approved algorithm and modes, and the shared secret
 - 1002 decrypted only when immediately required for authentication, or;
 - 1003 c) any secure method allowed to protect shared secrets at Level 3 or 4.
- 1004

1005 **4.4 Assurance Level 4**

1006 Achieving AL4 requires meeting even more stringent criteria in addition to the criteria
1007 required to achieve AL3.

1008 **4.4.1 Enterprise and Service Maturity**

1009 Criteria in this section address the establishment of the enterprise offering the service and
1010 its basic standing as a legal and operational business entity.

1011 An enterprise and its specified service must:

1012 *AL4_CO_ESM#010 Established enterprise*

1013 Be a valid legal entity and a person with legal authority to commit the organization must
1014 submit the signed assessment package.

1015 *AL4_CO_ESM#020 Withdrawn*

1016 Withdrawn

1017 *AL4_CO_ESM#030 Legal & Contractual compliance*

1018 Demonstrate that it understands and complies with any legal requirements incumbent on
1019 it in connection with operation and delivery of the specified service, accounting for all
1020 jurisdictions within which its services may be offered. Any specific contractual
1021 requirements shall also be identified.

1022 **Guidance:** Kantara Initiative, Inc. will not recognize a service which is not fully released
1023 for the provision of services to its intended user/client community. Systems, or parts
1024 thereof, which are not fully proven and released shall not be considered in an assessment
1025 and therefore should not be included within the scope of the assessment package. Parts of
1026 systems still under development, or even still being planned, are therefore ineligible for
1027 inclusion within the scope of assessment.

1028 *AL4_CO_ESM#040 Financial Provisions*

1029 Provide documentation of financial resources that allow for the continued operation of the
1030 service and demonstrate appropriate liability processes and procedures that satisfy the
1031 degree of liability exposure being carried.

1032 **Guidance:** The organization must show that it has a budgetary provision to operate the
1033 service for at least a twelve-month period, with a clear review of the budgetary planning
1034 within that period so as to keep the budgetary provisions extended. It must also show
1035 how it has determined the degree of liability protection required, in view of its exposure
1036 per 'service' and the number of users it has. This criterion helps ensure that Kantara
1037 Initiative, Inc. does not grant Recognition to services that are not likely to be sustainable
1038 over at least this minimum period of time.

1039 *AL4_CO_ESM#050 Data Retention and Protection*

1040 Specifically set out and demonstrate that it understands and complies with those legal and
1041 regulatory requirements incumbent upon it concerning the retention and destruction of
1042 private and identifiable information (personal and business) (i.e. its secure storage and
1043 protection against loss, accidental public exposure, and/or improper destruction) and the
1044 protection of private information (against unlawful or unauthorized access excepting that
1045 permitted by the information owner or required by due process).

1046 *AL4_CO_ESM#055 Termination provisions*

1047 Define the practices in place for the protection of Subjects' private and secret information
1048 related to their use of the service which must ensure the ongoing secure preservation and
1049 protection of legally required records and for the secure destruction and disposal of any
1050 such information whose retention is no longer legally required. Specific details of these
1051 practices must be made available.

1052 **Guidance:** Termination covers the cessation of the business activities, the service
1053 provider itself ceasing business operations altogether, change of ownership of the service-
1054 providing business, and other similar events which change the status and/or operations of
1055 the service provider in any way which interrupts the continued provision of the specific
1056 service.

1057 *AL4_CO_ESM#060 Ownership*

1058 If the enterprise named as the CSP is a part of a larger entity, the nature of the relationship
1059 with its parent organization, shall be disclosed to the assessors and, on their request, to
1060 customers.

1061 *AL4_CO_ESM#070 Independent Management and Operations*

1062 Demonstrate that, for the purposes of providing the specified service, its management and
1063 operational structures are distinct, autonomous, have discrete legal accountability, and
1064 operate according to separate policies, procedures, and controls.

1065 **4.4.2 Notices and Subscriber Information/Agreements**

1066 Criteria in this section address the publication of information describing the service and
1067 the manner of and any limitations upon its provision, and how users are required to accept
1068 those terms.

1069 An enterprise and its specified service must:

1070 *AL4_CO_NUI#010 General Service Definition*

1071 Make available to the intended user community a Service Definition that includes all
1072 applicable Terms, Conditions, and Fees, including any limitations of its usage, and
1073 definitions of any terms having specific intention or interpretation. Specific provisions
1074 are stated in further criteria in this section.

1075 **Guidance:** The intended user community encompasses potential and actual Subscribers,
1076 Subjects, and relying parties.

1077 *AL4_CO_NUI#020 Service Definition inclusions*

- 1078 Make available a Service Definition for the specified service containing clauses that
1079 provide the following information:
- 1080 a) Privacy, Identity Proofing & Verification, Renewal/Re-issuance, and Revocation
1081 and Termination Policies;
 - 1082 b) the country in or legal jurisdiction under which the service is operated;
 - 1083 c) if different to the above, the legal jurisdiction under which Subscriber and any
1084 relying party agreements are entered into;
 - 1085 d) applicable legislation with which the service complies;
 - 1086 e) obligations incumbent upon the CSP;
 - 1087 f) obligations incumbent upon each class of user of the service, e.g. Relying Parties,
1088 Subscribers and Subjects;
 - 1089 g) notifications and guidance for relying parties, especially in respect of actions they
1090 are expected to take should they choose to rely upon the service's product;
 - 1091 h) statement of warranties;
 - 1092 i) statement of liabilities toward both Subjects and Relying Parties;
 - 1093 j) procedures for notification of changes to terms and conditions;
 - 1094 k) steps the CSP will take in the event that it chooses or is obliged to terminate the
1095 service;
 - 1096 l) availability of the specified service per se and of its help desk facility.

1097 *AL4_CO_NUI#025 AL4 Configuration Specification*

1098 Make available a detailed specification (accounting for the service specification and
1099 architecture) which defines how a user of the service can configure it so as to be assured
1100 of receiving at least an **AL4** baseline service.

1101 *AL4_CO_NUI#030 Due Notification*

1102 Have in place and follow appropriate policy and procedures to ensure that it notifies
1103 Subscribers and Subjects in a timely and reliable fashion of any changes to the Service
1104 Definition and any applicable Terms, Conditions, Fees, and Privacy Policy for the
1105 specified service, and provide a clear means by which Subscribers and Subjects must
1106 indicate that they wish to accept the new terms or terminate their subscription.

1107 *AL4_CO_NUI#040 User Acceptance*

1108 Require Subscribers and Subjects to:

- 1109 a) indicate, prior to receiving service, that they have read and accept the terms of
1110 service as defined in the Service Definition, thereby indicating their properly-
1111 informed opt-in;
- 1112 b) at periodic intervals, determined by significant service provision events (e.g.
1113 issuance, re-issuance, renewal) and otherwise at least once every five years, re-
1114 affirm their understanding and observance of the terms of service;
- 1115 c) always provide full and correct responses to requests for information.

1116 *AL4_CO_NUI#050 Record of User Acceptance*

1117 Obtain a record (hard-copy or electronic) of the Subscriber's and Subject's acceptance of
1118 the terms and conditions of service, prior to initiating the service and thereafter reaffirm
1119 the agreement at periodic intervals, determined by significant service provision events
1120 (e.g. issuance, re-issuance, renewal) and otherwise at least once every five years.

1121 *AL4_CO_NUI#060 Withdrawn*
1122 Withdrawn.

1123 *AL4_CO_NUI#070 Change of Subscriber Information*
1124 *Require and provide the mechanisms for Subscribers and Subjects to provide in a timely*
1125 *manner full and correct amendments should any of their recorded information change, as*
1126 *required under the terms of their use of the service, and only after the Subscriber's and/or*
1127 *Subject's identity has been authenticated.*

1128 *AL4_CO_NUI#080 Withdrawn*
1129 Withdrawn.

1130 **4.4.3 Information Security Management**

1131 These criteria address the way in which the enterprise manages the security of its
1132 business, the specified service, and information it holds relating to its user community.

1133 This section focuses on the key components that comprise a well-established and
1134 effective Information Security Management System (ISMS), or other IT security
1135 management methodology recognized by a government or professional body.

1136 An enterprise and its specified service must:

1137 *AL4_CO_ISM#010 Documented policies and procedures*
1138 Have documented all security-relevant administrative, management, and technical
1139 policies and procedures. The enterprise must ensure that these are based upon recognized
1140 standards, published references, or organizational guidelines, are adequate for the
1141 specified service, and are implemented in the manner intended.

1142 *AL4_CO_ISM#020 Policy Management and Responsibility*
1143 Have a clearly defined managerial role, at a senior level, where full responsibility for the
1144 business' security policies is vested and from which review, approval, and promulgation
1145 of policy and related procedures is applied and managed. The latest approved versions of
1146 these policies must be applied at all times.

1147 *AL4_CO_ISM#030 Risk Management*
1148 Demonstrate a risk management methodology that adequately identifies and mitigates
1149 risks related to the specified service and its user community and must show that on-going
1150 risk assessment review is conducted as a part of the business' procedures, such as
1151 adherence to CobIT or [[IS27001](#)] methods.

1152 *AL4_CO_ISM#040 Continuity of Operations Plan*

1153 Have and keep updated a continuity of operations plan that covers disaster recovery and
1154 the resilience of the specified service and must show that **on-going review of this plan is**
1155 **conducted as a part of the business' procedures.**

1156 *AL4_CO_ISM#050 Configuration Management*

1157 Demonstrate that there is in place a configuration management system that at least
1158 includes:

- 1159 a) version control for software system components;
- 1160 b) timely identification and installation of all organizationally-approved patches for
1161 any software used in the provisioning of the specified service;
- 1162 c) version control and managed distribution for all documentation associated with
1163 the specification, management, and operation of the system, covering both
1164 internal and publicly available materials.

1165 *AL4_CO_ISM#060 Quality Management*

1166 Demonstrate that there is in place a quality management system that is appropriate for the
1167 specified service.

1168 *AL4_CO_ISM#070 System Installation and Operation Controls*

1169 Apply controls during system development, procurement, installation, and operation that
1170 protect the security and integrity of the system environment, hardware, software, and
1171 communications having particular regard to:

- 1172 a) the software and hardware development environments, for customized
1173 components;
- 1174 b) the procurement process for commercial off-the-shelf (COTS) components;
- 1175 c) contracted consultancy/support services;
- 1176 d) shipment of system components;
- 1177 e) storage of system components;
- 1178 f) installation environment security;
- 1179 g) system configuration;
- 1180 h) transfer to operational status.

1181 *AL4_CO_ISM#080 Internal Service Audit*

1182 Be subjected to a first-party audit at least once every 12 months for the effective
1183 provision of the specified service by internal audit functions of the enterprise responsible
1184 for the specified service, unless it can show that by reason of its organizational size or due
1185 to other justifiable operational restrictions it is unreasonable to be so audited.

1186 **Guidance:** 'First-party' audits are those undertaken by an independent part of the same
1187 organization which offers the service. The auditors cannot be involved in the
1188 specification, development or operation of the service.

1189 Management systems require that there be internal audit conducted as an inherent part of
1190 management review processes. Any third-party (i.e. independent) audit of the
1191 management system is intended to show that the internal management system controls are

1192 being appropriately applied, and for the purposes of fulfilling Kantara’s needs, a formal
1193 Kantara Assessment performed by an Accredited Assessor should be considered as such.

1194 *AL4_CO_ISM#090 Withdrawn*
1195 Withdrawn.

1196 *AL4_CO_ISM#100 Audit Records*
1197 Retain records of all audits, both internal and independent, for a period which, as a
1198 minimum, fulfills its legal obligations and otherwise for greater periods either as it may
1199 have committed to in its Service Definition or required by any other obligations it has
1200 with/to a Subscriber or Subject, and which in any event is not less than 36 months. Such
1201 records must be held securely and be protected against unauthorized access loss,
1202 alteration, public disclosure, or unapproved destruction.

1203 *AL4_CO_ISM#110 Withdrawn*
1204 Withdrawn.

1205 *AL4_CO_ISM#120 Best Practice Security Management*
1206 Have in place a **certified** Information Security Management System (ISMS), or other IT
1207 security management methodology recognized by a government or professional body, that
1208 **has been assessed and found to be in compliance with the requirements of**
1209 **ISO/IEC 27001 [IS27001] and which applies and is appropriate to the CSP in**
1210 **question.** All requirements expressed in preceding criteria in this section must *inter alia*
1211 fall wholly within the scope of this ISMS, or the selected recognized alternative.

1212 **4.4.4 Security-Related (Audit) Records**

1213 The criteria in this section are concerned with the need to provide an auditable log of all
1214 events that are pertinent to the correct and secure operation of the service.

1215 An enterprise and its specified service must:

1216 *AL4_CO_SER#010 Security Event Logging*
1217 Maintain a log of all relevant security events concerning the operation of the service,
1218 together with a **precise** record of the time at which the event occurred (time-stamp)
1219 **provided by a trusted time-source** and retain such records with appropriate protection
1220 and controls to ensure successful retrieval, accounting for service definition, risk
1221 management requirements, applicable legislation, and organizational policy.

1222 **Guidance:** The trusted time source could be an external trusted service or a network time
1223 server or other hardware timing device. The time source must be not only precise but
1224 authenticatable as well.

1225 **4.4.5 Operational Infrastructure**

1226 The criteria in this section address the infrastructure within which the delivery of the
1227 specified service takes place. It puts particular emphasis upon the personnel involved,
1228 and their selection, training, and duties.

1229 An enterprise and its specified service must:

1230 *AL4_CO_OPN#010* *Withdrawn*

1231 *Withdrawn.*

1232 *AL4_CO_OPN#020* *Defined Security Roles*

1233 Define, by means of a job description, the roles and responsibilities for each service-
1234 related security-relevant task, relating it to specific procedures (which shall be set out in
1235 the ISMS, or other IT security management methodology recognized by a government or
1236 professional body) and other service-related job descriptions and applicable policies,
1237 processes and procedures {source [5415] KI.10.2.2.1#24}. Where the role is security-critical or
1238 where special privileges or shared duties exist, these must be specifically identified as
1239 such, including the applicable access privileges relating to logical and physical parts of
1240 the service's operations.

1241 *AL4_CO_OPN#025* *Acknowledgement of assigned security roles and responsibilities*

1242 Require those assigned to critical security roles to acknowledge, by signature (hand-
1243 written or electronic), that they have read and understood the system documentation
1244 applicable to their role(s) and that they accept the associated responsibilities. {source [5415]
1245 KI.10.2.2.1#24}

1246 *AL4_CO_OPN#030* *Personnel Recruitment*

1247 Demonstrate that it has defined practices for the selection, vetting, and contracting of all
1248 service-related personnel, both direct employees and those whose services are provided
1249 by third parties. Full records of all searches and supporting evidence of qualifications and
1250 past employment must be kept for the duration of the individual's employment plus the
1251 longest lifespan of any credential issued under the Service Policy.

1252 *AL4_CO_OPN#040* *Personnel skills*

1253 Ensure that employees are sufficiently trained, qualified, experienced, and current for the
1254 roles they fulfill. Such measures must be accomplished either by recruitment practices or
1255 through a specific training program. Where employees are undergoing on-the-job
1256 training, they must only do so under the guidance of a mentor possessing the defined
1257 service experiences for the training being provided.

1258 *AL4_CO_OPN#050* *Adequacy of Personnel resources*

1259 Have sufficient staff to adequately operate and resource the specified service according to
1260 its policies and procedures.

1261 *AL4_CO_OPN#060* *Physical access control*

1262 Apply physical access control mechanisms to ensure that:

1263 a) access to sensitive areas is restricted to authorized personnel;

- 1264 b) all removable media and paper documents containing sensitive information as
1265 plain-text are stored in secure containers;
1266 c) a minimum of two persons are required to enable access to any cryptographic
1267 modules;
1268 d) there is 24/7 monitoring for unauthorized intrusions.

1269 *AL4_CO_OPN#070 Logical access control*

1270 Employ logical access control mechanisms that ensure access to sensitive system
1271 functions and controls is restricted to authorized personnel.

1272 **4.4.6 External Services and Components**

1273 This section addresses the relationships and obligations upon contracted parties both to
1274 apply the policies and procedures of the enterprise and also to be available for assessment
1275 as critical parts of the overall service provision.

1276 An enterprise and its specified service must:

1277 *AL4_CO_ESC#010 Contracted Policies and Procedures*

1278 Where the enterprise uses external suppliers for specific packaged components of the
1279 service or for resources which are integrated with its own operations and under its
1280 control, ensure that those parties are engaged through reliable and appropriate contractual
1281 arrangements which stipulate which critical policies, procedures, and practices sub-
1282 contractors are required to fulfill.

1283 *AL4_CO_ESC#020 Visibility of Contracted Parties*

1284 Where the enterprise uses external suppliers for specific packaged components of the
1285 service or for resources which are integrated with its own operations and under its
1286 control, ensure that the suppliers' compliance with contractually-stipulated policies and
1287 procedures, and thus with the IAF Service Assessment Criteria, can be independently
1288 verified, and subsequently monitored if necessary.

1289 **4.4.7 Secure Communications**

1290 An enterprise and its specified service must:

1291 *AL4_CO_SCO#010 Secure remote communications*

1292 If the specific service components are located remotely from and communicate over a
1293 public or unsecured network with other service components or other CSPs it services, or
1294 parties requiring access to the CSP's services, each transaction must be cryptographically
1295 protected using an encryption method approved by a recognized national technical
1296 authority or other generally-recognized authoritative body, by either:

- 1297 a) implementing mutually-authenticated protected sessions; or
1298 b) time-stamped or sequenced messages signed by their source and encrypted for their
1299 recipient.

1300 **Guidance:** The reference to “parties requiring access to the CSP’s services” is intended
1301 to cover SP 800-63-2’s reference to RPs (see cross-mapped EZP 63-2 clause).

1302 *AL4_CO_SCO#015 Verification / Authentication confirmation messages*

1303 Ensure that any verification or confirmation of authentication messages, which assert
1304 either that a weakly bound credential is valid or that a strongly bound credential has not
1305 been subsequently revoked, is logically bound to the credential and that the message, the
1306 logical binding, and the credential are all transmitted within a single integrity-protected
1307 session between the service and the Verifier / Relying Party.

1308 *AL4_CO_SCO#016 No stipulation*

1309 *AL4_CO_SCO#020 Limited access to shared secrets*

1310 Ensure that:

- 1311 a) access to shared secrets shall be subject to discretionary controls which permit
1312 access to those roles/applications which need such access;
- 1313 b) stored shared secrets are encrypted such that:
- 1314 i the encryption key for the shared secret file is encrypted under a key held
1315 in an [IS19790] Level 2 (or higher) validated hardware cryptographic
1316 module, or equivalent, as established by a recognized national technical
1317 authority, or any [IS19790] Level 3 or 4 validated cryptographic module,
1318 or equivalent, as established by a recognized national technical authority,
1319 and decrypted only as immediately required for an authentication
1320 operation;
- 1321 ii they are protected as a key within the boundary of an [IS19790] Level 2
1322 (or higher) validated hardware cryptographic module, or equivalent, as
1323 established by a recognized national technical authority, or any [IS19790]
1324 Level 3 or 4 cryptographic module, or equivalent, as established by a
1325 recognized national technical authority, and are not exported from the
1326 module in plaintext;
- 1327 **iii they are split by an "n from m" cryptographic secret-sharing method;**
- 1328 c) any long-term (i.e., not session) shared secrets are revealed only to the Subject
1329 and the CSP's direct agents (bearing in mind (a) above).

1330 In addition, these roles should be defined and documented by the CSP in accordance with
1331 AL4_CO_OPN#020 above.

1332 **5 OPERATIONAL SERVICE ASSESSMENT CRITERIA**

1333 The Service Assessment Criteria in this section establish requirements for the operational
1334 conformity of credential management services and their providers at all Assurance Levels
1335 (AL) – refer to Section 2. These criteria are generally referred to elsewhere within IAF
1336 documentation as OP-SAC.

1337 Previous editions of this document have these criteria set out in two distinct sections and
1338 have used the terms CM-SAC and ID-SAC: the OP-SAC is the combination of those two
1339 previous SAC sections, with optimizations necessary for their integration. To ensure
1340 backwards compatibility with assessments already performed against previous editions of
1341 this document the criteria within the OP-SAC continue to be identified either by a tag
1342 “ALn_ID_ xxxx” or “ALn_CM_ xxxx”.

1343 Within each Assurance Level the criteria are divided into six Parts. Each part deals with a
1344 specific functional aspect of the overall credential management process, including
1345 identity proofing services (see Parts B, at each Assurance Level).

1346 Full Service Provision requires conformity to all of the following operational criteria at
1347 the chosen Assurance Level. This may be demonstrated either by the Full Service
1348 Provider fulfilling all of these criteria itself or by its service being a composition of
1349 Service Components which must, collectively, fulfill all of these criteria, under the overall
1350 management of the Full Service Provider. Providers of Service Components may
1351 conform to a defined sub-set of these criteria (although, within Part A at each Assurance
1352 Level, there is a small number of criteria which are mandatory for Component Services,
1353 which are marked as such).

1354 The procedures and processes required to create a secure environment for management of
1355 credentials and the particular technologies that are considered strong enough to meet the
1356 assurance requirements differ considerably from level to level.

1357 **5.1 Assurance Level 1**

1358 **5.1.1 Part A - Credential Operating Environment**

1359 These criteria describe requirements for the overall operational environment in which
1360 credential lifecycle management is conducted. The Common Organizational criteria
1361 describe broad requirements. The criteria in this Part describe operational
1362 implementation specifics

1363 These criteria apply to PINs and passwords, as well as SAML assertions.

1364 The criterion AL1_CM_CTR#030 is marked as **MANDATORY** for all Component
1365 Services.

1366 **5.1.1.1 Not used**

1367 No stipulation.

1368 **5.1.1.2 Security Controls**

1369 An enterprise and its specified service must:

1370 *ALI_CM_CTR#010 Withdrawn*

1371 *ALI_CM_CTR#020 Protocol threat risk assessment and controls*

1372 Account for at least the following protocol threats and apply appropriate controls:

- 1373 a) password guessing, such that there are at least 14 bits of entropy to resist an on-
1374 line guessing attack against a selected user/password;
1375 b) message replay.

1376 **Guidance:** Organizations should consider potential protocol threats identified in other
1377 sources, e.g. ISO/IEC 29115:2013 “*Information technology -- Security techniques –*
1378 *Entity authentication assurance framework*”. Kantara IAF-5415 provides a mapping
1379 between IS29115 and the SAC.

1380 *ALI_CM_CTR#025 No stipulation*

1381 *ALI_CM_CTR#028 No stipulation*

1382 *ALI_CM_CTR#030 System threat risk assessment and controls*

1383 **MANDATORY.**

1384 Account for the following system threats and apply appropriate controls:

- 1385 a) the introduction of malicious code;
1386 b) compromised authentication arising from insider action;
1387 c) out-of-band attacks by other users and system operators (e.g., the ubiquitous
1388 shoulder-surfing);
1389 d) spoofing of system elements/applications;
1390 e) malfeasance on the part of Subscribers and Subjects.

1391 **Guidance:** the risk assessment should address these threats from any perspective in
1392 which they might adversely affect the operation of the service, whether they be from
1393 within the organization (e.g. in its development environment, the hosting environment) or
1394 without (e.g. network attacks, hackers).

1395 **5.1.1.3 Storage of Long-term Secrets**

1396 *ALI_CM_STS#010 Withdrawn*

1397 Withdrawn (AL1_CO_SCO#020 (a) & (b) enforce this requirement)

1398 **5.1.1.4 No stipulation**

1399 **5.1.1.5 Subject Options**

1400 *ALI_CM_OPN#010 Withdrawn*
1401 Withdrawn – see AL1_CM_RNR#010.

1402 **5.1.2 Part B - Credential Issuing**

1403 These criteria apply to the verification of the identity of the Subject of a credential and
1404 with token strength and credential delivery mechanisms. They address requirements
1405 levied by the use of various technologies to achieve Assurance Level 1.

1406 **5.1.2.1 Identity Proofing Policy**

1407 The specific service must show that it applies identity proofing policies and procedures
1408 and that it retains appropriate records of identity proofing activities and evidence.

1409 The enterprise and its specified service must:

1410 *ALI_ID_POL#010 Unique service identity*
1411 Ensure that a unique identity is attributed to the specific service, such that credentials
1412 issued by it can be distinguishable from those issued by other services, including services
1413 operated by the same enterprise.

1414 *ALI_ID_POL#020 Unique Subject identity*
1415 Ensure that each applicant’s identity is unique within the service’s community of Subjects
1416 and uniquely associable with tokens and/or credentials issued to that identity.

1417 **5.1.2.2 Identity Verification**

1418 The enterprise or specific service:

1419 *ALI_ID_IDV#000 Identity Proofing classes*

- 1420 a) must include in its Service Definition at least one of the following classes of
1421 identity proofing service, and;
- 1422 b) may offer any additional classes of identity proofing service it chooses, subject to
1423 the nature and the entitlement of the CSP concerned;
- 1424 c) must fulfill the applicable assessment criteria according to its choice of identity
1425 proofing service, i.e. conform to at least one of the criteria sets defined in:
- 1426 i) **§;Error! No se encuentra el origen de la referencia.**, “In-Person Public
1427 Identity Proofing”;
- 1428 ii) **§;Error! No se encuentra el origen de la referencia.**, “Remote Public

1428 ii) **§;Error! No se encuentra el origen de la referencia.**, “Remote Public
1429 Identity Proofing”.

1430 **5.1.2.3 In-Person Public Identity Verification**

1431 If the specific service offers in-person identity proofing to applicants with whom it has no
1432 previous relationship, then it must comply with the criteria in this section.

1433 An enterprise or specified service must:

1434 *ALI_ID_IPV#010 Required evidence*

1435 Accept a self-assertion of identity.

1436 *ALI_ID_IPV#020 Evidence checks*

1437 Accept self-attestation of evidence.

1438 **5.1.2.4 Remote Public Identity Verification**

1439 If the specific service offers remote identity proofing to applicants with whom it has no
1440 previous relationship, then it must comply with the criteria in this section.

1441 An enterprise or specified service must:

1442 *ALI_ID_RPV#010 Required evidence*

1443 Require the applicant to provide a contact telephone number or email address.

1444 *ALI_ID_RPV#020 Evidence checks*

1445 Verify the provided information by either:

1446 a) confirming the request by calling the number;

1447 b) successfully sending a confirmatory email and receiving a positive
1448 acknowledgement.

1449 **5.1.2.5 No stipulation**

1450 **5.1.2.6 No stipulation**

1451 **5.1.2.7 Issuing Derived Credentials**

1452 Where the Applicant already possesses recognized original credentials the CSP may
1453 choose to accept the verified identity of the Applicant as a substitute for identity proofing,
1454 subject to the following specific provisions. All other requirements of Assurance Level 1
1455 identity proofing must also be observed.

1456 *ALI_ID_IDC#010 Authenticate Original Credential*

1457 Prior to issuing any derived credential the original credential on which the identity-
1458 proofing relies must be proven to be in the possession and under the control of the
1459 Applicant.

1460 **Guidance:** This is the equivalent of recording the details of identity-proofing documents
1461 provided during (e.g.) face-face id-proofing. It is not required that the original credential
1462 be issued by a Kantara-Approved CSP.

1463 **5.1.2.8 Secondary Identity Verification**

1464 In each of the above cases, an enterprise or specified service must:

1465 *ALI_ID_SCV#010 Secondary checks*

1466 Have in place additional measures (e.g., require additional documentary evidence, delay
1467 completion while out-of-band checks are undertaken) to deal with:

1468 a) any reasonably anomalous circumstances that can be reasonably anticipated (e.g.,
1469 a legitimate and recent change of address that has yet to be established as the
1470 address of record);

1471 b) any use of processes and/or technologies which may not fully meet the preceding
1472 applicable requirements but which are deemed to be comparable and thus able to
1473 support AL1.

1474 **5.1.2.9 Identity-proofing Records**

1475 *ALI_ID_VRC#010 No stipulation*

1476 *ALI_ID_VRC#020 No stipulation*

1477 *ALI_ID_VRC#025 Provide Subject Identity Records*

1478 If required, provide to qualifying parties a unique identity for each Subscriber and their
1479 associated tokens and credentials to the extent permitted by applicable legislation and/or
1480 agreed by the Subscriber.

1481 **Guidance:** the qualifier ‘if required’ is intended to account for circumstances where
1482 conditions such as whether a contract or a federation policy permits or is required or
1483 jurisdiction / legal injunction demand such provision. A qualifying party is any party to
1484 which provision of such info can justified according to circumstance: by contract/policy;
1485 with Subject’s agreement; with due authority (Court Order, e.g.). The CSP needs to make
1486 the case, according to their service’s characteristics and operating environment.

1487 *ALI_ID_VRC#030 No stipulation*

1488 *ALI_CM_IDP#010 Revision to Subject Information*

1489 Provide a means for Subjects to amend their stored information after registration.

1490 **Guidance:** The necessity for re-issuance will be determined by, *inter alia*, policy, the
1491 technology and practices in use, the nature of change (e.g. registration data not bound into
1492 the credential) and the nature of the proofing processes.

1493 *ALI_CM_IDP#020 Authenticate Subject Information Changes*

1494 Permit only changes which are supported by appropriate and sufficient authentication of
1495 the legitimacy of change according, to its type.

1496 **Guidance:** The requirement to authenticate the legitimacy of a change will depend upon
1497 what is retained by the CSP and what is being changed: whereas a change of address may
1498 require less demanding authentication than may a change of name, a change of date-of-
1499 birth would be very unlikely and therefore would require substantial supporting
1500 authentication.

1501 **5.1.2.10 Credential Creation**

1502 These criteria address the requirements for creation of credentials that can only be used at
1503 AL1. Any credentials/tokens that comply with the criteria stipulated for AL2 and higher
1504 are acceptable at AL1.

1505 An enterprise and its specified service must:

1506 *ALI_CM_CRN#010 Authenticated Request*

1507 Only accept a request to generate a credential and bind it to an identity if the source of the
1508 request can be authenticated as being authorized to perform identity proofing at AL1 or
1509 higher.

1510 *ALI_CM_CRN#020 No stipulation*

1511 *ALI_CM_CRN#030 Credential uniqueness*

1512 Allow the Subject to select a credential (e.g., UserID) that is verified to be unique within
1513 the specified service's community and assigned uniquely to a single identity Subject.

1514 **Default names shall not be permitted.** {source [5415] KI.10.3.2.1#04}

1515 *ALI_CM_CRN#035 Convey credential*

1516 Be capable of conveying the unique identity information associated with a credential to
1517 Verifiers and Relying Parties.

1518 *ALI_CM_CRN#040 Token strength*

1519 Ensure that the single-factor token associated with the credential has one of the following
1520 sets of characteristics:

- 1521 a) For a memorized secret, apply a rule-set such that there shall be a minimum of 14
1522 bits of entropy in the pin or pass-phrase. **Default values shall not be permitted;**
- 1523 b) For a knowledge-based question, apply a rule-set such that there shall be:
- 1524 i) a minimum of 14 bits of entropy in the pin or pass-phrase OR;

- 1525 ii) a set of knowledge-based questions created by the user OR;
1526 iii) a set of knowledge-based questions selected by the user from a service-
1527 generated list of at least five questions.
1528

1529 Null or empty answers in any case above shall not be permitted.

1530 **5.1.2.11 No stipulation**

1531 **5.1.2.12 No stipulation**

1532 **5.1.3 Part C - Credential Renewal and Re-issuing**

1533 These criteria apply to the renewal and re-issuing of credentials. They address
1534 requirements levied by the use of various technologies to achieve the appropriate
1535 Assurance Level 1.

1536 **5.1.3.1 Renewal/Re-issuance Procedures**

1537 These criteria address general renewal and re-issuance functions, to be exercised as
1538 specific controls in these circumstances while continuing to observe the general
1539 requirements established for initial credential issuance.

1540 An enterprise and its specified service must:

1541 *ALI_CM_RNR#010 Changeable PIN/Password*

1542 Permit Subjects to change their PINs/passwords.

1543 *ALI_CM_RNR#020 Proof-of-possession on Renewal/Re-issuance*

1544 Subjects wishing to change their passwords must demonstrate that they are in possession
1545 of the unexpired current token prior to the CSP proceeding to renew or re-issue it. {source
1546 [5415] KI.10.2.2.1#29}

1547 **5.1.4 Part D - Credential Revocation**

1548 These criteria deal with credential revocation and the determination of the legitimacy of a
1549 revocation request.

1550 An enterprise and its specified service must:

1551 **5.1.4.1 No stipulation**

1552 **5.1.4.2 No stipulation**

1553 **5.1.4.3 No stipulation**

1554 **5.1.4.4 Secure Revocation Request**

1555 This criterion applies when revocation requests between remote components of a service
1556 are made over a secured communication.

1557 An enterprise and its specified service must:

1558 *ALI_CM_SRR#010 Submit Request*

1559 Submit a request for revocation to the Credential Issuer service (function), using a
1560 secured network communication, if necessary.

1561

1562 **5.1.5 Part E - Credential Status Management**

1563 These criteria deal with credential status management, such as the receipt of requests for
1564 new status information arising from a new credential being issued or a revocation or other
1565 change to the credential that requires notification. They also deal with the provision of
1566 status information to requesting parties (Verifiers, Relying Parties, courts and others
1567 having regulatory authority, etc.) having the right to access such information.

1568 **5.1.5.1 Status Maintenance**

1569 An enterprise and its specified service must:

1570 *ALI_CM_CSM#010 Maintain Status Record*

1571 Maintain a record of the status of all credentials issued.

1572 *ALI_CM_CSM#020 No stipulation*

1573 *ALI_CM_CSM#030 No stipulation*

1574 *ALI_CM_CSM#040 Status Information Availability*

1575 Provide, with 95% availability, a secure automated mechanism to allow relying parties to
1576 determine credential status and authenticate the Claimant's identity.

1577 **5.1.6 Part F - Credential Verification/Authentication**

1578 These criteria apply to credential validation and identity authentication.

1579 **5.1.6.1 Assertion Security**

1580 An enterprise and its specified service must:

1581 *ALI_CM_ASS#010 Validation and Assertion Security*

1582 Provide validation of credentials to a Relying Party using a protocol that:

- 1583 a) requires authentication of the specified service or of the validation source;
- 1584 b) ensures the integrity of the authentication assertion;
- 1585 c) protects assertions against manufacture, modification and substitution, and
- 1586 secondary authenticators from manufacture;

1587 and which, specifically:

- 1588 d) creates assertions which are specific to a single transaction;
- 1589 e) where assertion references are used, generates a new reference whenever a new
- 1590 assertion is created;
- 1591 f) when an assertion is provided indirectly, either signs the assertion or sends it via a
- 1592 protected channel, using a strong binding mechanism between the secondary
- 1593 authenticator and the referenced assertion;
- 1594 g) requires the secondary authenticator to:
 - 1595 i) be signed when provided directly to Relying Party, or;
 - 1596 ii) have a minimum of 64 bits of entropy when provision is indirect (i.e.
 - 1597 through the credential user).

1598 *ALI_CM_ASS#015 No stipulation*

1599 *ALI_CM_ASS#018 No stipulation*

1600 *ALI_CM_ASS#020 No Post Authentication*

1601 Not authenticate credentials that have been revoked.

1602 *ALI_CM_ASS#030 Proof of Possession*

1603 Use an authentication protocol that requires the claimant to prove possession and control

1604 of the authentication token.

1605 *ALI_CM_ASS#035 Limit authentication attempts*

1606 Limit the number of failed authentication attempts to no more than 100 in any 30-day

1607 period.

1608 *ALI_CM_ASS#040 Assertion Lifetime*

1609 Set assertions to expire such that:

- 1610 a) those used outside of the internet domain of the Verifier become invalid 5 minutes
- 1611 after their creation; or
- 1612 b) those used within a single internet domain become invalid 12 hours after their
- 1613 creation (including assertions contained in or referenced by cookies).

1614 **5.1.6.2 Authenticator-generated challenges**

1615 No stipulation.

1616 **5.1.6.3 Multi-factor authentication**

1617 No stipulation.

1618 **5.1.6.4 Verifier's assertion schema**

1619 Note: Since assertions and related schema can be complex and may be modeled directly
1620 on the needs and preferences of the participants, the details of such schema fall outside
1621 the scope of the SAC's herein, which are expressed observing, insofar as is feasible, a
1622 technology-agnostic policy. The following criteria, therefore, are perhaps more open to
1623 variable conformity through their final implementation than are others in this document.

1624 These criteria are derived directly from NIST SP 800-63-2 and have been expressed in as
1625 generic a manner as they can be.

1626 An enterprise and its specified service must:

1627 *ALI_CM_VAS#010 No stipulation*

1628 No stipulation.

1629 *ALI_CM_VAS#020 No stipulation*

1630 No stipulation.

1631 *ALI_CM_VAS#030 Assertion assurance level*

1632 Create assertions which, either explicitly or implicitly (using a mutually-agreed
1633 mechanism), indicate the assurance level at which the initial authentication of the Subject
1634 was made.

1635 *ALI_CM_VAS#040 No stipulation*

1636 No stipulation.

1637 *ALI_CM_VAS#050 No stipulation*

1638 No stipulation.

1639 *ALI_CM_VAS#060 No assertion manufacture/modification*

1640 Ensure that it is impractical to manufacture an assertion or assertion reference by using at
1641 least one of the following techniques:

1642 a) Signing the assertion;

1643 b) Encrypting the assertion using a secret key shared with the RP;

1644 c) Creating an assertion reference which has a minimum of 64 bits of entropy;

- 1645 d) Sending the assertion over a protected channel during a mutually-authenticated
1646 session.
- 1647 *ALI_CM_VAS#070 No stipulation*
1648 No stipulation.
- 1649 *ALI_CM_VAS#080 Single-use assertions*
1650 Limit to a single transaction the use of assertions which do not support proof of
1651 ownership.
- 1652 *ALI_CM_VAS#090 Single-use assertion references*
1653 Limit to a single transaction the use of assertion references.
- 1654 *ALI_CM_VAS#100 Bind reference to assertion*
1655 Provide a strong binding between the assertion reference and the corresponding assertion,
1656 based on integrity-protected (or signed) communications over which the Verifier has been
1657 authenticated.
- 1658

1659 5.2 Assurance Level 2

1660 **5.2.1 Part A - Credential Operating Environment**

1661 These criteria describe requirements for the overall operational environment in which
1662 credential lifecycle management is conducted. The Common Organizational criteria
1663 describe broad requirements. The criteria in this Part describe operational
1664 implementation specifics.

1665 These criteria apply to passwords, as well as acceptable SAML assertions.

1666 The following three criteria are **MANDATORY** for all Services, Full or Component, and
1667 are individually marked as such:

1668 AL2_CM_CPP#010, AL2_CM_CPP#030, AL2_CM_CTR#030.

1669 **5.2.1.1 Credential Policy and Practices**

1670 These criteria apply to the policy and practices under which credentials are managed.

1671 An enterprise and its specified service must:

1672 *AL2_CM_CPP#010 Credential Policy and Practice Statement*

1673 **MANDATORY.**

1674 **Document and apply both the Credential Policy against which it issues credentials**
1675 **and the corresponding Credential Practices it applies in their management. At a**
1676 **minimum, the Credential Policy and Practice Statement must specify:**

- 1677 a) if applicable, any OIDs related to the Practice and Policy Statement;
- 1678 b) how users may subscribe to the service/apply for credentials and how users'
1679 credentials will be delivered to them;
- 1680 c) how Subjects acknowledge receipt of tokens and credentials, what obligations
1681 they accept in so doing (including whether they consent to publication of
1682 their details in credential status directories) and the measures the CSP takes
1683 to initialize and personalize the credentials; {source: [5415] KI.10.2.2.1#01}
- 1684 d) how credentials may be renewed, modified, revoked, and suspended,
1685 including how requestors are authenticated or their identity re-proven;
- 1686 e) what actions a Subject must take to terminate a subscription;
- 1687 f) how records are retained and archived.

1688 *AL2_CM_CPP#015 Credential Policy reference*

1689 **MANDATORY.**

1690 **Include in its Service Definition, either directly or by accessible reference, the policy**
1691 **against which it issues credentials. {source [5415] KI.10.2.2.1#20}**

1692 *AL2_CM_CPP#020 No stipulation*

1693 *AL2_CM_CPP#030 Management Authority*

1694 **MANDATORY.**

1695 **Have a nominated management body with authority and responsibility for**
1696 **approving the Credential Policy and Practice Statement and for its implementation.**

1697 **5.2.1.2 Security Controls**

1698 An enterprise and its specified service must:

1699 *AL2_CM_CTR#010 Withdrawn*

1700 *AL2_CM_CTR#020 Protocol threat risk assessment and controls*

1701 Account for at least the following protocol threats **in its risk assessment** and apply
1702 **[omitted] controls that reduce them to acceptable risk levels:**

- 1703 a) password guessing, such that there are at least 24 bits of entropy to resist an on-
1704 line guessing attack against a selected user/password;
- 1705 b) message replay, **showing that it is impractical;**
- 1706 c) **eavesdropping, showing that it is impractical;**
- 1707 d) **no stipulation;**
- 1708 e) **man-in-the-middle attack;**
- 1709 f) **session hijacking.**

1710 **Guidance:** Organizations should consider potential protocol threats identified in other
1711 sources, e.g. ISO/IEC 29115:2013 “Information technology -- Security techniques –
1712 Entity authentication assurance framework”.

1713 *AL2_CM_CTR#025 Authentication protocols*

1714 **Apply only authentication protocols which, through a comparative risk assessment**
1715 **which takes into account the target Assurance Level, are shown to have resistance to**
1716 **attack at least as strong as that provided by commonly-recognized protocols such as:**

- 1717 a) **tunneling;**
- 1718 b) **zero knowledge-based;**
- 1719 c) **signed SAML [Omitted].**

1720 **Guidance:** Whilst many authentication protocols are well-established and may be
1721 mandated or strongly-recommended by specific jurisdictions or sectors (e.g. standards
1722 published by national SDOs or applicable to government-specific usage) this criterion
1723 gives flexibility to advanced and innovative authentication protocols for which adequate
1724 strength can be shown to be provided by the protocol applied with the specific service.

1725 *AL2_CM_CTR#028 One-time passwords*

1726 **Use only one-time passwords which:**

- 1727 a) **are generated using an approved block-cipher or hash function to combine a**
1728 **symmetric key, stored on the device, with a nonce; or**

- 1729 b) **derive the nonce from a date and time, or a counter, which is generated on**
1730 **the device; or**
1731 c) **have a limited lifetime, in the order of minutes.**

1732 *AL2_CM_CTR#030 System threat risk assessment and controls*

1733 **MANDATORY.**

1734 Account for the following system threats **in its risk assessment** and apply **[omitted]**
1735 controls **that reduce them to acceptable risk levels:**

- 1736 a) the introduction of malicious code;
1737 b) compromised authentication arising from insider action;
1738 c) out-of-band attacks by both users and system operators (e.g., the ubiquitous
1739 shoulder-surfing);
1740 d) spoofing of system elements/applications;
1741 e) malfeasance on the part of Subscribers and Subjects;
1742 f) **intrusions leading to information theft.**

1743 **Guidance:** the risk assessment should address these threats from any perspective in
1744 which they might adversely affect the operation of the service, whether they be from
1745 within the organization (e.g. in its development environment, the hosting environment) or
1746 without (e.g. network attacks, hackers).

1747 *AL2_CM_CTR#040 Specified Service's Key Management*

1748 **Specify and observe procedures and processes for the generation, storage, and**
1749 **destruction of its own cryptographic keys used for securing the specific service's**
1750 **assertions and other publicized information. At a minimum, these should address:**

- 1751 a) **the physical security of the environment;**
1752 b) **access control procedures limiting access to the minimum number of**
1753 **authorized personnel;**
1754 c) **public-key publication mechanisms;**
1755 d) **application of controls deemed necessary as a result of the service's risk**
1756 **assessment;**
1757 e) **destruction of expired or compromised private keys in a manner that**
1758 **prohibits their retrieval, or their archival in a manner that prohibits their**
1759 **reuse;**
1760 f) **applicable cryptographic module security requirements, quoting [IS19790]**
1761 **or equivalent, as established by a recognized national technical authority.**

1762 **5.2.1.3 Storage of Long-term Secrets**

1763 *AL2_CM_STS#010 Withdrawn*

1764 Withdrawn (AL2_CO_SCO#020 (a) & (b) enforce this requirement).

1765 **5.2.1.4 No stipulation**

1766 **5.2.1.5 No stipulation**

1767 *AL2_CM_OPN#010 Withdrawn*

1768 Withdrawn – see AL2_CM_RNR#010.

1769 **5.2.2 Part B - Credential Issuing**

1770 These criteria apply to the verification of the identity of the Subject of a credential and
1771 with token strength and credential delivery mechanisms. They address requirements
1772 levied by the use of various technologies to achieve Assurance Level 2.

1773 **5.2.2.1 Identity Proofing Policy**

1774 The specific service must show that it applies identity proofing policies and procedures
1775 and that it retains appropriate records of identity proofing activities and evidence.

1776 The enterprise and its specified service must:

1777 *AL2_ID_POL#010 Unique service identity*

1778 Ensure that a unique identity is attributed to the specific service, such that credentials
1779 issued by it can be distinguishable from those issued by other services, including services
1780 operated by the same enterprise.

1781 *AL2_ID_POL#020 Unique Subject identity*

1782 Ensure that each applicant's identity is unique within the service's community of Subjects
1783 and uniquely associable with tokens and/or credentials issued to that identity.

1784 **Guidance:** Cf. AL2_CM_CRN#020 which expresses a very similar requirement.

1785 Although presenting repetition for a single provider, if the identity-proofing functions and
1786 credential management functions are provided by separate CSPs, each needs to fulfill this
1787 requirement.

1788 *AL2_ID_POL#030 Published Proofing Policy*

1789 **Make available the Identity Proofing Policy under which it verifies the identity of**
1790 **applicants² in form, language, and media accessible to the declared community of**
1791 **Users.**

1792 *AL2_ID_POL#040 Adherence to Proofing Policy*

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

1793 **Perform all identity proofing strictly in accordance with its published Identity**
1794 **Proofing Policy.**

1795 **5.2.2.2 Identity Verification**

1796 The enterprise or specific service:

1797 *AL2_ID_IDV#000 Identity Proofing classes*

- 1798 a) must include in its Service Definition at least one of the following classes of
1799 identity proofing service, and;
- 1800 b) may offer any additional classes of identity proofing service it chooses, Subject to
1801 the nature and the entitlement of the CSP concerned;
- 1802 c) must fulfill the applicable assessment criteria according to its choice of identity
1803 proofing service, i.e. conform to at least one of the criteria sets defined in:
- 1804 i) §0, “[In-Person Public Identity Verification](#)”;
- 1805 ii) §5.2.2.4, “[Remote Public Identity Verification](#)”;
- 1806 iii) §5.2.2.5, “[Current Relationship Identity Verification](#)”;
- 1807 iv) §5.2.2.6, “[Affiliation Identity Verification](#)”;
- 1808 **although, in any of the above cases, the criteria defined in §5.2.2.7 may be**
1809 **substituted for identity proofing where the Applicant already possesses a**
1810 **recognized credential at Level 3 or 4.**

1811 *AL2_ID_IDV#010 - Identity Verification Measures*

1812 **For each identity proofing service offered (see above [i.e. AL2_ID_IDV#000]) justify**
1813 **the identity verification measures applied by describing how these meet or exceed**
1814 **the requirements of applicable policies, regulations, adopted standards and other**
1815 **relevant conditions in order to maintain a level of rigour consistent with the**
1816 **applicable Assurance Level.**

1817 **Guidance:** Although strict requirements for identity proofing and verification can be
1818 defined, a real-world approach must account for instances where there is not 100%
1819 certitude. To cope with this CSPs need to have a set of prescribed (through policy – see
1820 AL2_ID_POL#030) and applied measures (see AL2_ID_POL#040) which observe
1821 policy, identify the measures taken according to the degree of certitude determined by
1822 each step in the verification process and what additional measures are taken. The CSP
1823 must present a case which shows that their solution is sufficient to ensure that the basic
1824 requirements of the applicable AL are met or exceeded.

1825 Note that in each set of proofing service criteria below there are criteria with specific
1826 requirements for evidence checks and an additional criterion for ‘secondary’ checks, all of
1827 which have an interplay with these overall requirements to have a policy and practice

1828 statement and to demonstrate processes which sustain confidence that AL2 is being
1829 achieved.

1830 Even though a CSP may use the services of a component service for the performance of
1831 the identity-proofing within its own service, it still needs to ensure that its policy is both
1832 justified and upheld. Where another service provider is used appropriate stipulations in
1833 contracts should be established, but any internal adherence to (e.g.) 'POL#040 should be
1834 determined by the fact that the component service is already Kantara Approved.

1835 **5.2.2.3 In-Person Public Identity Proofing**

1836 If the specific service offers in-person identity proofing to applicants with whom it has no
1837 previous relationship, then it must comply with the criteria in this section.

1838 The enterprise or specified service must:

1839 *AL2_ID_IPV#010 Required evidence*

1840 **Ensure that the applicant is in possession of a primary Government Picture ID
1841 document that bears a photographic image of the holder.**

1842 *AL2_ID_IPV#020 Evidence checks*

1843 **Have in place and apply processes which ensure that the presented document:**

- 1844 a) **appears to be a genuine document properly issued by the claimed issuing
1845 authority and valid at the time of application;**
1846 b) **bears a photographic image of the holder that matches that of the applicant;**
1847 c) **provides all reasonable certainty that the identity exists and that it uniquely
1848 identifies the applicant.**

1849 **5.2.2.4 Remote Public Identity Proofing**

1850 If the specific service offers remote identity proofing to applicants with whom it has no
1851 previous relationship, then it must comply with the criteria in this section.

1852 An enterprise or specified service must:

1853 *AL2_ID_RPV#010 Required evidence*

1854 **Ensure that the applicant submits the references of and attests to current possession
1855 of a primary Government [omitted] ID document, and one of:**

- 1856 a) **a second Government ID;**
1857 b) **an employee or student ID number;**
1858 c) **a financial account number (e.g., checking account, savings account, loan or
1859 credit card);**
1860 d) **a utility service account number (e.g., electricity, gas, or water) for an address
1861 matching that in the primary document; or**
1862 e) **a telephone service account.**

1863 **Ensure that the applicant provides additional verifiable personal information that at**
1864 **a minimum must include:**

- 1865 **f) a name that matches the referenced ID;**
- 1866 **g) date (year, month and day) of birth and;**
- 1867 **h) current address [omitted];**
- 1868 **i) for a telephone service account, the demonstrable ability to send or receive**
1869 **messages at the phone number.**

1870 **Additional information may be requested so as to ensure a unique identity, and**
1871 **alternative information may be sought where the enterprise can show that it leads to**
1872 **at least the same degree of certitude when verified.**

1873 *AL2_ID_RPV#020 Evidence checks*

1874 **Perform inspection and analysis of records against the provided identity references**
1875 **with the specified issuing authorities/institutions or through similar databases,**
1876 **according to the inspection rules set by the issuing authorities:**

- 1877 **a) the existence of such records with matching name and reference numbers;**
- 1878 **b) corroboration of date (year, month and day) of birth, current contact**
1879 **information of record, and other personal information sufficient to ensure a**
1880 **unique identity;**
- 1881 **c) for a utility account, dynamic verification of personal information previously**
1882 **provided by or likely to be known only by the applicant;**
- 1883 **d) for a telephone service account, confirmation that the phone number**
1884 **supplied by the applicant is associated in Records with the Applicant's name**
1885 **and address of record and by having the applicant demonstrate that they are**
1886 **able to send or receive messages at the phone number.**

1887 **Confirm contact information of record by at least one of the following means,**
1888 **ensuring that any secret sent over an unprotected channel shall be reset upon first**
1889 **use and shall be valid for a maximum lifetime of seven days:**

- 1890 **e) RA sends notice to an address of record confirmed in the records check and**
1891 **receives a mailed or telephonic reply from applicant;**
- 1892 **f) RA issues credentials in a manner that confirms the address of record**
1893 **supplied by the applicant, for example by requiring applicant to enter on-line**
1894 **some information from a notice sent to the applicant;**
- 1895 **g) RA issues credentials in a manner that confirms ability of the applicant to**
1896 **receive telephone communications at telephone number or email at email**
1897 **address associated with the applicant in records.**
- 1898 **h) [Omitted]**

1899 **Additional checks may be performed so as to establish the uniqueness of the claimed**
1900 **identity (see AL2_ID_SCV#010).**

1901 **Alternative checks may be performed where the enterprise can show that they lead**
1902 **to a comparable degree of certitude (see AL2_ID_SCV#010).**

1903 **5.2.2.5 Current Relationship Identity Proofing**

1904 If the specific service offers identity proofing to applicants with whom it has a current
1905 relationship, then it must comply with the criteria in this section.

1906 The enterprise or specified service must:

1907 *AL2_ID_CRV#010 Required evidence*

1908 **Ensure that it has previously exchanged with the applicant a shared secret (e.g., a**
1909 **PIN or password) that meets AL2 (or higher) entropy requirements³.**

1910 *AL2_ID_CRV#020 Evidence checks*

1911 **Ensure that it has:**

- 1912 **a) only issued the shared secret after originally establishing the applicant’s**
1913 **identity:**
- 1914 **i) with a degree of rigor equivalent to that required under either the AL2**
1915 **(or higher) requirements for in-person or remote public verification;**
1916 **or**
 - 1917 **ii) by complying with regulatory requirements effective within the**
1918 **applicable jurisdiction which set forth explicit proofing requirements**
1919 **which include a prior in-person appearance by the applicant and are**
1920 **defined as meeting AL2 (or higher) requirements;**
- 1921 **b) an ongoing business relationship sufficient to satisfy the enterprise of the**
1922 **applicant’s continued personal possession of the shared secret.**

1923 **5.2.2.6 Affiliation Identity Proofing**

1924 If the specific service offers identity proofing to applicants on the basis of some form of
1925 affiliation, then it must comply with the criteria in this section for the purposes of
1926 establishing that affiliation, in addition to the previously stated requirements for the
1927 verification of the individual’s identity.

1928 The enterprise or specified service must:

1929 *AL2_ID_AJV#000 Meet preceding criteria*

1930 **Meet all the criteria set out above, under §5.2.2.5, “[Current Relationship](#)**
1931 **[Verification](#)”.**

1932 *AL2_ID_AJV#010 Required evidence*

1933 **Ensure that the applicant possesses:**

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

- 1934 a) **identification from the organization with which it is claiming affiliation;**
1935 b) **agreement from the organization that the applicant may be issued a**
1936 **credential indicating that an affiliation exists.**

1937 *AL2_ID_AJV#020 Evidence checks*

1938 **Have in place and apply processes which ensure that the presented documents:**

- 1939 a) **each appear to be a genuine document properly issued by the claimed issuing**
1940 **authorities and valid at the time of application;**
1941 b) **refer to an existing organization with a contact address;**
1942 c) **indicate that the applicant has some form of recognizable affiliation with the**
1943 **organization;**
1944 d) **appear to grant the applicant an entitlement to obtain a credential indicating**
1945 **its affiliation with the organization.**

1946 **5.2.2.7 Identity-proofing based on Recognized Credentials**

1947 Where the Applicant already possesses recognized original credentials the CSP may
1948 choose to accept the verified identity of the Applicant as a substitute for identity proofing,
1949 subject to the following specific provisions. All other requirements of **Assurance Level**
1950 **2** identity proofing must also be observed.

1951 *AL2_ID_IDC#010 Authenticate Original Credential*

1952 Prior to issuing any derived credential the original credential on which the identity-
1953 proofing relies must be:

- 1954 a) **authenticated by a source trusted by the CSP as being valid and un-revoked;**
1955 b) **issued at Assurance Level 3 or 4;**
1956 c) **issued in the same name as that which the Applicant is claiming;**
1957 d) **proven to be in the possession and under the control of the Applicant.**

1958 **Guidance:** This is the equivalent of recording the details of **identity-proofing** documents
1959 provided during (e.g.) face-face id-proofing. It is not required that the original credential
1960 be issued by a Kantara-Approved CSP.

1961 *AL2_ID_IDC#020 Record Original Credential*

1962 **Record the details of the original credential.**

1963 *AL2_ID_IDC#030 Issue Derived Credential*

1964 **Before issuing the derived credential ensure that:**

- 1965 a) **for in-person issuance, the claimant is the Applicant;**
1966 b) **for remote issuance, token activation requires proof of possession of both the**
1967 **derived token and the original Level 3 or Level 4 token.**

1968 **5.2.2.8 Secondary Identity-proofing**

1969 In each of the above cases, the enterprise or specified service must:

1970 *AL2_ID_SCV#010 Secondary checks*

1971 Have in place additional measures (e.g., require additional documentary evidence, delay
1972 completion while out-of-band checks are undertaken) to deal with:

1973 a) any reasonably anomalous circumstances that can be reasonably anticipated (e.g.,
1974 a legitimate and recent change of address that has yet to be established as the
1975 address of record);

1976 b) any use of processes and/or technologies which may not fully meet the preceding
1977 applicable requirements but which are deemed to be comparable and thus able to
1978 support **AL2**.

1979 **5.2.2.9 Identity-proofing Records**

1980 The specific service must retain records of the identity proofing (verification) that it
1981 undertakes and provide them to qualifying parties when so required.

1982 An enterprise or specified service must:

1983 *AL2_ID_VRC#010 Verification Records for Personal Applicants*

1984 **Log, taking account of all applicable legislative and policy obligations, a record of**
1985 **the facts of the verification process, including a reference relating to the verification**
1986 **processes, the date and time of verification and the identity of the registrar (person,**
1987 **or entity if remote or automatic) performing the proofing functions.**

1988 **Guidance:** The facts of the verification process should include the specific record
1989 information (source, unique reference, value/content) used in establishing the applicant's
1990 identity, and will be determined by the specific processes used and documents accepted
1991 by the CSP. The CSP need not retain these records itself if it uses a third-party service
1992 which retains such records securely and to which the CSP has access when required, in
1993 which case it must retain a record of the identity of the third-party service providing the
1994 verification service or the location at which the (in-house) verification was performed.

1995 *AL2_ID_VRC#020 Verification Records for Affiliated Applicants*

1996 **In addition to the foregoing, log, taking account of all applicable legislative and**
1997 **policy obligations, a record of the additional facts of the verification process**
1998 **[omitted].**

1999 **Guidance:** Although there is no specific stipulation as to what should be recorded the
2000 list below suggests facts which would typically be captured:

- 2001 a) the Subject's full name;
2002 b) the Subject's current telephone or email address of record;
2003 c) the Subscriber's acknowledgement for issuing the Subject with a credential;

2004 d) type, issuing authority, and reference number(s) of all documents checked in the
2005 identity proofing process.

2006 *AL2_ID_VRC#025 Provide Subject identity records*

2007 If required, provide to qualifying parties **records of identity proofing** to the extent
2008 permitted by applicable legislation and/or agreed by the Subscriber.

2009 **Guidance:** the qualifier ‘if required’ is intended to account for circumstances where
2010 conditions such as whether a contract or a federation policy permits or is required or
2011 jurisdiction / legal injunction demand such provision. A qualifying party is any party to
2012 which provision of such info can justified according to circumstance: by contract/policy;
2013 with Subject’s agreement; with due authority (Court Order, e.g.). The CSP needs to make
2014 the case, according to their service’s characteristics and operating environment.

2015 *AL2_ID_VRC#030 Record Retention*

2016 **Either retain, securely, the record of the verification process for the duration of the**
2017 **Subject account plus a further period sufficient to allow fulfillment of any period**
2018 **required legally, contractually or by any other form of binding agreement or**
2019 **obligation, or submit same record to a client CSP that has undertaken to retain the**
2020 **record for the requisite period or longer.**

2021 *AL2_CM_IDP#010 Revision to Subject information*

2022 Provide a means for Subjects to **securely** amend their stored information after
2023 registration, **either by re-proving their identity, as in the initial registration process,**
2024 **or by using their credentials to authenticate their revision. Successful revision must**
2025 **instigate the re-issuance of the credential when the data being revised are bound into**
2026 **the credential.**

2027 **Guidance:** The necessity for re-issuance will be determined by, *inter alia*, policy, the
2028 technology and practices in use, the nature of change (e.g. registration data not bound into
2029 the credential) and the nature of the proofing processes.

2030 *AL2_CM_IDP#020 Authenticate Subject Information Changes*

2031 Permit only changes which are supported by appropriate and sufficient authentication of
2032 the legitimacy of change according, to its type.

2033 **Guidance:** The requirement to authenticate the legitimacy of a change will depend upon
2034 what is retained by the CSP and what is being changed: whereas a change of address may
2035 require less demanding authentication than may a change of name, a change of date-of-
2036 birth would be very unlikely and therefore would require substantial supporting
2037 authentication.

2038 **5.2.2.10 Credential Creation**

2039 These criteria define the requirements for creation of credentials whose highest use is at
2040 AL2. Credentials/tokens that comply with the criteria stipulated at AL3 and higher are
2041 also acceptable at AL2 and below.

2042 Note, however, that a token and credential required by a higher AL but created according
2043 to these criteria may not necessarily provide that higher level of assurance for the claimed
2044 identity of the Subject. Authentication can only be provided at the assurance level at
2045 which the identity is proven.

2046 An enterprise and its specified service must:

2047 *AL2_CM_CRN#010 Authenticated Request*

2048 Only accept a request to generate a credential and bind it to an identity if the source of the
2049 request can be authenticated, **i.e., Registration Authority, as being authorized to**
2050 **perform identity proofing at AL2 or higher.**

2051 *AL2_CM_CRN#020 Unique identity*

2052 **Ensure that the identity which relates to a specific applicant is unique within the**
2053 **specified service, including identities previously used and that are now cancelled,**
2054 **other than its re-assignment to the same applicant.**

2055 **Guidance:** This requirement is intended to prevent identities that may exist in a Relying
2056 Party's access control list from possibly representing a different physical person.
2057 Cf. AL2_CM_POL#020 which expresses a very similar requirement. Although
2058 presenting repetition for a single provider, if the identity-proofing functions and
2059 credential management functions are provided by separate CSPs, each needs to fulfill this
2060 requirement.

2061 *AL2_CM_CRN#030 Credential uniqueness*

2062 Allow the Subject to select a credential (e.g., UserID) that is verified to be unique within
2063 the specified service's community and assigned uniquely to a single identity Subject.
2064 Default names shall not be permitted. {source [5415] KI.10.3.2.1#04}

2065 *AL2_CM_CRN#035 Convey credential*

2066 Be capable of conveying the unique identity information associated with a credential to
2067 Verifiers and Relying Parties.

2068 *AL2_CM_CRN#040 Token strength*

2069 Ensure that the single-factor token associated with the credential has one of the following
2070 sets of characteristics:

- 2071 a) For a memorized secret, apply a rule-set such that there shall be a minimum of **24**
2072 bits of entropy in the pin or pass-phrase. **Default values shall not be permitted;**
- 2073 b) For a knowledge-based question, apply a rule-set such that there shall be:
- 2074 i) a minimum of **20** bits of entropy in the pin or pass-phrase OR;
- 2075 ii) a set of knowledge-based questions created by the user OR;
- 2076 iii) a set of knowledge-based questions selected by the user from a service-generated
2077 list of at least **seven** questions.

- 2078
2079 Null or empty answers in either case above shall not be permitted.
- 2080 c) **For a look-up token, apply a rule-set such that there shall be a minimum of 20**
2081 **bits of entropy in the secret phrase(s);**
- 2082 d) **For an out-of-band token, ensure that the token is uniquely addressable and**
2083 **supports communication over a channel that is separate from the primary**
2084 **channel for e-authentication;**
- 2085 e) **For a one-time-password device, generate one-time passwords using an**
2086 **approved block cipher or hash function to combine a nonce and a symmetric**
2087 **key;**
- 2088 f) **Use a cryptographic device validated at [IS19790] Level 1 or higher or**
2089 **equivalent, as established by a recognized national technical authority.**
2090
- 2091 **[Omitted]**
- 2092 *AL2_CM_CRN#050 One-time password strength*
2093 **Only allow password tokens that have a resistance to online guessing attack against**
2094 **a selected user/password of at least 1 in 2¹⁴ (16,384), accounting for state-of-the-art**
2095 **attack strategies, and at least 10 bits of min-entropy** Error! Marcador no definido.
- 2096 *AL2_CM_CRN#055 One-time password lifetime*
2097 **Set the minimum valid lifetime for the one-time password to a value commensurate**
2098 **with service usage and in no case greater than fifteen minutes.**
- 2099 *AL2_CM_CRN#060 Software cryptographic token strength*
2100 **Ensure that software cryptographic keys stored on general-purpose devices are**
2101 **protected by a key and cryptographic protocol that are validated against [IS19790]**
2102 **Level 1, or equivalent, as established by a recognized national technical authority.**
- 2103 **[Omitted]**
- 2104 *AL2_CM_CRN#070 Hardware token strength*
2105 **Ensure that hardware tokens used to store cryptographic keys:**
- 2106 a) **employ a cryptographic module that is validated against [IS19790] Level 1 or**
2107 **higher, or equivalent, as established by a recognized national technical authority;**
- 2108 b) **are locked prior to their delivery, once personalization processes have been**
2109 **completed.** {source [5415] KI.10.2.2.1#07}
- 2110 *AL2_CM_CRN#075 No stipulation*
- 2111 *AL2_CM_CRN#080 Binding*
2112 **Ensure that the Subject is uniquely bound to the credential and remains so until the**
2113 **credential is securely delivered to the Subject.** {source [5415] KI.10.2.2.1#02}

2114 *AL2_CM_CRN#090 Nature of Subject*

2115 **Record the nature of the Subject of the credential (which must correspond to the**
2116 **manner of identity proofing performed), i.e., physical person, a named person acting**
2117 **on behalf of a corporation or other legal entity, corporation or legal entity, or**
2118 **corporate machine entity, in a manner that can be unequivocally associated with the**
2119 **credential and the identity that it asserts. [Omitted]**

2120 *AL2_CM_CRN#095 Pseudonym's Real Identity*

2121 **If the credential is based upon a pseudonym this must be indicated in the credential**
2122 **and a record of the real identity retained.**

2123 **5.2.2.11 Subject Key Pair Generation**

2124 No stipulation.

2125 **5.2.2.12 Credential Delivery**

2126 An enterprise and its specified service must:

2127 *AL2_CM_CRD#010 Notify Subject of Credential Issuance*

2128 **Notify the Subject of the credential's issuance and, if necessary, confirm the**
2129 **Subject's contact information by:**

- 2130 a) **sending notice to the address of record confirmed during identity proofing**
2131 **or;**
2132 b) **issuing the credential(s) in a manner that confirms the address of record**
2133 **supplied by the applicant during identity proofing or;**
2134 c) **issuing the credential(s) in a manner that confirms the ability of the applicant**
2135 **to receive telephone communications at a fixed-line telephone number or**
2136 **postal address supplied by the applicant during identity proofing.**

2137 **Guidance:** The nature of issuance could mean that the Subject is fully aware and
2138 therefore no notification is necessary. If any other such circumstances prevailed, the CSP
2139 should identify them.

2140 *AL2_CM_CRD#015 Confirm Applicant's identity (in person)*

2141 **Prior to delivering the credential, require the Applicant to identify themselves in**
2142 **person in any new transaction (beyond the first transaction or encounter) by either:**

- 2143 (a) **using a temporary secret which was established during a prior**
2144 **transaction or encounter, or sent to the Applicant's phone number, email**
2145 **address, or physical address of record, or;**
2146 (b) **matching a biometric sample against a reference sample that was**
2147 **recorded during a prior encounter.**

2148 *AL2_CM_CRD#016 Confirm Applicant's identity (remotely)*

2149 **Prior to activating the credential, require the Applicant to identify themselves in any**
2150 **new electronic transaction (beyond the first transaction or encounter) by presenting**
2151 **a temporary secret which was established during a prior transaction or encounter,**
2152 **or sent to the Applicant's phone number, email address, or physical address of**
2153 **record.**

2154 **Guidance:** Activation typically requires that the credential be delivered to the
2155 Applicant/Subject before activation occurs.

2156 *AL3_CM_CRD#030: Require activation of the credential within a time period specified*
2157 *in the Credential Policy*

2158 **5.2.3 Part C - Credential Renewal and Re-issuing**

2159 These criteria apply to the renewal and re-issuing of credentials. They address
2160 requirements levied by the use of various technologies to achieve Assurance Level 2.

2161 **5.2.3.1 Renewal/Re-issuance Procedures**

2162 These criteria address general renewal and re-issuance functions, to be exercised as
2163 specific controls in these circumstances while continuing to observe the general
2164 requirements established for initial credential issuance.

2165 An enterprise and its specified service must:

2166 *AL2_CM_RNR#010 Changeable PIN/Password*

2167 Permit Subjects to change their [omitted] passwords, **but employ reasonable practices**
2168 **with respect to password resets and repeated password failures.**

2169 *AL2_CM_RNR#020 Proof-of-possession on Renewal/Re-issuance*

2170 Subjects wishing to change their passwords must demonstrate that they are in possession
2171 of the unexpired current token prior to the CSP proceeding to renew or re-issue it.

2172 *AL2_CM_RNR#030 Renewal/Re-issuance limitations*

2173 **a) not renew but may re-issue Passwords;**

2174 **b) neither renew nor re-issue expired tokens;**

2175 **c) neither set to default nor re-use any token secrets;**

2176 **d) conduct all renewal / re-issuance interactions with the Subject over a**
2177 **protected channel such as SSL/TLS.**

2178 **Guidance:** Renewal is considered as an extension of usability, whereas re-issuance
2179 requires a change.

2180 *AL2_CM_RNR#040 No stipulation*

2181 **No stipulation.**

2182 *AL2_CM_RNR#050 Record Retention*

2183 **Retain, securely, the record of any renewal/re-issuance process for the duration of**
2184 **the Subscriber's account plus a further period sufficient to allow fulfillment of any**
2185 **period required legally, contractually or by any other form of binding agreement or**
2186 **obligation, or submit same record to a client CSP that has undertaken to retain the**
2187 **record for the requisite period or longer.**

2188 **5.2.4 Part D - Credential Revocation**

2189 These criteria deal with credential revocation and the determination of the legitimacy of a
2190 revocation request.

2191 **5.2.4.1 Revocation Procedures**

2192 These criteria address general revocation functions, such as the processes involved and
2193 the basic requirements for publication.

2194 An enterprise and its specified service must:

2195 *AL2_CM_RVP#010 Revocation procedures*

2196 a) **State the conditions under which revocation of an issued credential may**
2197 **occur;**

2198 b) **State the processes by which a revocation request may be submitted;**

2199 c) **State the persons and organizations from which a revocation request will be**
2200 **accepted;**

2201 d) **State the validation steps that will be applied to ensure the validity (identity)**
2202 **of the Revocant, and;**

2203 e) **State the response time between a revocation request being accepted and the**
2204 **publication of revised certificate status.**

2205 *AL2_CM_RVP#020 Secure status notification*

2206 **Ensure that published credential status notification information can be relied upon**
2207 **in terms of the enterprise of its origin (i.e., its authenticity) and its correctness (i.e.,**
2208 **its integrity).**

2209 *AL2_CM_RVP#030 Revocation publication*

2210 **Unless the credential will expire automatically within 72 hours:**

2211 **Ensure that published credential status notification is revised within 72 hours of the**
2212 **receipt of a valid revocation request, such that any subsequent attempts to use that**
2213 **credential in an authentication shall be unsuccessful.**

2214 *AL2_CM_RVP#040 Verify revocation identity*

2215 **Establish that the identity for which a revocation request is received is one that was**
2216 **issued by the specified service.**

2217 *AL2_CM_RVP#045 Notification of Revoked Credential*

2218 **When a verification / authentication request results in notification of a revoked**
2219 **credential one of the following measures shall be taken:**

- 2220 a) **the confirmation message shall be time-stamped, or;**
- 2221 b) **the session keys shall expire with an expiration time no longer than that of**
2222 **the applicable revocation list, or;**
- 2223 c) **the time-stamped message, binding, and credential shall all be signed by the**
2224 **service.**

2225 *AL2_CM_RVP#050 Revocation Records*

2226 **Retain a record of any revocation of a credential that is related to a specific identity**
2227 **previously verified, solely in connection to the stated credential. At a minimum,**
2228 **records of revocation must include:**

- 2229 a) **the Revocant's full name;**
- 2230 b) **the Revocant's authority to revoke (e.g., Subscriber, the Subject themselves,**
2231 **someone acting with the Subscriber's or the Subject's power of attorney, the**
2232 **credential issuer, law enforcement, or other legal due process);**
- 2233 c) **the Credential Issuer's identity (if not directly responsible for the identity**
2234 **proofing service);**
- 2235 d) **the identity associated with the credential (whether the Subject's name or a**
2236 **pseudonym);**
- 2237 e) **the reason for revocation.**

2238 *AL2_CM_RVP#060 Record Retention*

2239 **Retain securely, the record of the revocation process for a period which is the**
2240 **maximum of:**

- 2241 a) **the records retention policy required by AL2_CM_CPP#010; and**
- 2242 b) **applicable legislation, regulation, contract or standards.**

2243 **5.2.4.2 Verify Revocant's Identity**

2244 Revocation of a credential requires that the requestor and the nature of the request be
2245 verified as rigorously as the original identity proofing. The enterprise should not act on a
2246 request for revocation without first establishing the validity of the request (if it does not,
2247 itself, determine the need for revocation).

2248 In order to do so, the enterprise and its specified service must:

2249 *AL2_CM_RVR#010 Verify revocation identity*

2250 **Establish that the credential for which a revocation request is received was one that**
2251 **was issued by the specified service, applying the same process and criteria as would**
2252 **be applied to an original identity proofing.**

2253 *AL2_CM_RVR#020 Revocation reason*

2254 **Establish the reason for the revocation request as being sound and well founded, in**
2255 **combination with verification of the Revocant, according to AL2_ID_RVR#030,**
2256 **AL2_ID_RVR#040, or AL2_ID_RVR#050.**

2257 *AL2_CM_RVR#030 Verify Subscriber as Revocant*

2258 **When the Subscriber or Subject seeks revocation of the Subject's credential, the**
2259 **enterprise must:**

- 2260 a) **if in person, require presentation of a primary Government Picture ID**
2261 **document that shall be electronically verified by a record check against the**
2262 **provided identity with the specified issuing authority's records;**
2263 b) **if remote:**
2264 i. **electronically verify a signature against records (if available),**
2265 **confirmed with a call to a telephone number of record, or;**
2266 ii. **authenticate an electronic request as being from the same Subscriber or**
2267 **Subject, supported by a credential at Assurance Level 2 or higher.**

2268 *AL2_CM_RVR#040 CSP as Revocant*

2269 **Where a CSP seeks revocation of a Subject's credential, the enterprise must**
2270 **establish that the request is either:**

- 2271 a) **from the specified service itself, with authorization as determined by**
2272 **established procedures, or;**
2273 b) **from the client Credential Issuer, by authentication of a formalized request**
2274 **over the established secure communications network.**

2275 *AL2_CM_RVR#050 Verify Legal Representative as Revocant*

2276 **Where the request for revocation is made by a law enforcement officer or**
2277 **presentation of a legal document, the enterprise must:**

- 2278 a) **if in-person, verify the identity of the person presenting the request;**
2279 b) **if remote:**
2280 i. **in paper/facsimile form, verify the origin of the legal document by a**
2281 **database check or by telephone with the issuing authority, or;**
2282 ii. **as an electronic request, authenticate it as being from a recognized**
2283 **legal office, supported by a credential at Assurance Level 2 or higher.**

2284 **5.2.4.3 No stipulation**

2285 **5.2.4.4 Secure Revocation Request**

2286 This criterion applies when revocation requests must be communicated between remote
2287 components of the service organization.

2288 An enterprise and its specified service must:

2289 *AL2_CM_SRR#010 Submit Request*

2290 Submit a request for the revocation to the Credential Issuer service (function), using a
2291 secured network communication.

2292 **5.2.5 Part E - Credential Status Management**

2293 These criteria deal with credential status management, such as the receipt of requests for
2294 new status information arising from a new credential being issued or a revocation or other
2295 change to the credential that requires notification. They also deal with the provision of
2296 status information to requesting parties (Verifiers, Relying Parties, courts and others
2297 having regulatory authority, etc.) having the right to access such information.

2298 **5.2.5.1 Status Maintenance**

2299 An enterprise and its specified service must:

2300 *AL2_CM_CSM#010 Maintain Status Record*

2301 Maintain a record of the status of all credentials issued.

2302 *AL2_CM_CSM#020 Validation of Status Change Requests*

2303 **Authenticate all requestors seeking to have a change of status recorded and**
2304 **published and validate the requested change before considering processing the**
2305 **request. Such validation should include:**

2306 a) **the requesting source as one from which the specified service expects to**
2307 **receive such requests;**

2308 b) **if the request is not for a new status, the credential or identity as being one**
2309 **for which a status is already held.**

2310 *AL2_CM_CSM#030 Revision to Published Status*

2311 **Process authenticated requests for revised status information and have the revised**
2312 **information available for access within a period of 72 hours.**

2313 *AL2_CM_CSM#040 Status Information Availability*

2314 Provide, with 95% availability, a secure automated mechanism to allow relying parties to
2315 determine credential status and authenticate the Claimant's identity.

2316 *AL2_CM_CSM#050 Inactive Credentials*

2317 **Disable any credential that has not been successfully used for authentication during**
2318 **a period of 18 months.**

2319 **5.2.6 Part F - Credential Verification/Authentication**

2320 These criteria apply to credential validation and identity authentication.

2321 **5.2.6.1 Assertion Security**

2322 An enterprise and its specified service must:

2323 *AL2_CM_ASS#010 Validation and Assertion Security*

2324 Provide validation of credentials to a Relying Party using a protocol that:

- 2325 a) requires authentication of the specified service, itself, or of the validation source;
- 2326 b) ensures the integrity of the authentication assertion;
- 2327 c) protects assertions against manufacture, modification, **substitution and**
- 2328 **disclosure**, and secondary authenticators from manufacture, **capture and replay**;
- 2329 **d) uses approved cryptography techniques**;

2330 and which, specifically:

- 2331 e) creates assertions which are specific to a single transaction;
- 2332 f) where assertion references are used, generates a new reference whenever a new
- 2333 assertion is created;
- 2334 g) when an assertion is provided indirectly, either signs the assertion or sends it via a
- 2335 protected channel, using a strong binding mechanism between the secondary
- 2336 authenticator and the referenced assertion;
- 2337 **h) send assertions either via a channel mutually-authenticated with the Relying**
- 2338 **Party, or signed and encrypted for the Relying Party**;
- 2339 i) requires the secondary authenticator to:
 - 2340 i) be signed when provided directly to Relying Party, or;
 - 2341 ii) have a minimum of 64 bits of entropy when provision is indirect (i.e.
 - 2342 through the credential user);
 - 2343 **iii) be transmitted to the Subject through a protected channel which is**
 - 2344 **linked to the primary authentication process in such a way that**
 - 2345 **session hijacking attacks are resisted**;
 - 2346 **iv) not be subsequently transmitted over an unprotected channel or to an**
 - 2347 **unauthenticated party while it remains valid.**

2348 *AL2_CM_ASS#015 No False Authentication*

2349 **Employ techniques which ensure that system failures do not result in ‘false positive**

2350 **authentication’ errors.**

2351 *AL2_CM_ASS#018 No stipulation*

2352 *AL2_CM_ASS#020 No Post Authentication*

2353 **Not authenticate credentials that have been revoked unless the time of the transaction**

2354 **for which verification is sought precedes the time of revocation of the credential.**

2355 **Guidance:** The purpose in this criterion is that, if a verification is intended to refer to the

2356 status of a credential at a specific historical point in time, e.g. to determine whether the

2357 Claimant was entitled to act as a signatory in a specific capacity at the time of the

2358 transaction, this may be done. It is implicit in this thinking that both the request and the

2359 response indicate the historical nature of the query and response; otherwise the default

2360 time is ‘now’. If no such service is offered then this criterion may simply be
2361 ‘Inapplicable’, for that reason.

2362 *AL2_CM_ASS#030 Proof of Possession*

2363 Use an authentication protocol that requires the claimant to prove possession and control
2364 of the authentication token.

2365 *AL2_CM_ASS#035 Limit authentication attempts*

2366 **Unless the token authenticator has at least 64 bits of entropy**, limit the number of
2367 failed authentication attempts to no more than 100 in any 30-day period.

2368 *AL2_CM_ASS#040 Assertion Lifetime*

2369 Set assertions to expire such that:

- 2370 a) those used outside of the internet domain of the Verifier become invalid 5 minutes
2371 after their creation; or
2372 b) those used within a single internet domain become invalid 12 hours after their
2373 creation (including assertions contained in or referenced by cookies).

2374 **5.2.6.2 Authenticator-generated challenges**

2375 An enterprise and its specified service must:

2376 *AL2_CM_AGC#010 Entropy level*

2377 **Create authentication secrets to be used during the authentication exchange (i.e.**
2378 **with out-of-band or cryptographic device tokens) with a degree of entropy**
2379 **appropriate to the token type in question.**

2380 **5.2.6.3 Multi-factor authentication**

2381 An enterprise and its specified service must:

2382 *AL2_CM_MFA#010 Permitted multi-factor tokens*

2383 **Require two tokens which, when used in combination within a single authentication**
2384 **exchange, are acknowledged as providing an equivalence of AL2, as determined by a**
2385 **recognized national technical authority.**

2386 **5.2.6.4 Verifier’s assertion schema**

2387 Note: Since assertions and related schema can be complex and may be modeled directly
2388 on the needs and preferences of the participants, the details of such schema fall outside
2389 the scope of the SAC’s herein, which are expressed observing, insofar as is feasible, a
2390 technology-agnostic policy. The following criteria, therefore, are perhaps more open to
2391 variable conformity through their final implementation than are others in this document.

2392 These criteria are derived directly from NIST SP 800-63-2 and have been expressed in as
2393 generic a manner as they can be.

2394 *Editor's note: I have avoided reference to the RP here – I am concerned as to what the*
2395 *SAC requires services to do, not who might be using their products. SAC do not refer to*
2396 *RPs.*

2397 An enterprise and its specified service must:

2398 *AL2_CM_VAS#010 Approved cryptography*

2399 **Apply assertion protocols which use cryptographic techniques approved by a**
2400 **national authority or other generally-recognized authoritative body.**

2401 *AL2_CM_VAS#020 No stipulation*

2402 No stipulation.

2403 *AL2_CM_VAS#030 Assertion assurance level*

2404 Create assertions which, either explicitly or implicitly (using a mutually-agreed
2405 mechanism), indicate the assurance level at which the initial authentication of the Subject
2406 was made.

2407 *AL2_CM_VAS#040 Notify pseudonyms*

2408 **Create assertions which indicate whether the Subscriber name in the credential**
2409 **subject to verification is a pseudonym.**

2410 *AL2_CM_VAS#050 Specify recipient*

2411 **Create assertions which identify the intended recipient of the verification such that**
2412 **the recipient may validate that it is intended for them.**

2413 *AL2_CM_VAS#060 No assertion manufacture/modification*

2414 Ensure that it is impractical to manufacture an assertion or assertion reference by using at
2415 least one of the following techniques:

- 2416 a) Signing the assertion;
2417 b) Encrypting the assertion using a secret key shared with the RP;
2418 c) Creating an assertion reference which has a minimum of 64 bits of entropy;
2419 d) Sending the assertion over a protected channel during a mutually-authenticated
2420 session.

2421 *AL2_CM_VAS#070 Assertion protections*

2422 **Provide protection of assertion-related data such that:**

- 2423 a) **both assertions and assertion references are protected against capture and**
2424 **re-use;**
2425 b) **assertions are also protected against redirection;**
2426 c) **assertions, assertion references and session cookies used for authentication**
2427 **purposes, including any which are re-directed, are protected against session**
2428 **hijacking, for at least the duration of their validity (see AL2_CM_VAS#110).**

- 2429 *AL2_CM_VAS#080* *Single-use assertions*
2430 Limit to a single transaction the use of assertions which do not support proof of
2431 ownership.
- 2432 *AL2_CM_VAS#090* *Single-use assertion references*
2433 Limit to a single transaction the use of assertion references.
- 2434 *AL2_CM_VAS#100* *Bind reference to assertion*
2435 Provide a strong binding between the assertion reference and the corresponding assertion,
2436 based on integrity-protected (or signed) communications over which the Verifier has been
2437 authenticated.
- 2438

2439 **5.3 Assurance Level 3**

2440 **5.3.1 Part A - Credential Operating Environment**

2441 These criteria describe requirements for the overall operational environment in which
2442 credential lifecycle management is conducted. The Common Organizational criteria
2443 describe broad requirements. The criteria in this Part describe operational
2444 implementation specifics.

2445 These criteria apply to one-time password devices and soft crypto applications protected
2446 by passwords or biometric controls, as well as cryptographically-signed SAML
2447 assertions.

2448 The following four criteria are **MANDATORY** for all Services, Full or Component, and
2449 are individually marked as such:

2450 AL3_CM_CPP#010, AL3_CM_CPP#030, AL3_CM_CTR#030, AL3_CM_SER#010.

2451

2452 **5.3.1.1 Credential Policy and Practices**

2453 These criteria apply to the policy and practices under which credentials are managed.

2454 An enterprise and its specified service must:

2455 *AL3_CM_CPP#010 Credential Policy and Practice Statement*

2456 **MANDATORY.**

2457 Include in its Service Definition a full description of the policy against which it issues
2458 credentials and the corresponding practices it applies in their issuance. At a minimum,
2459 the Credential Policy and Practice Statement must specify:

- 2460 a) if applicable, any OIDs related to the Credential Policy and Practice Statement;
- 2461 b) how users may subscribe to the service/apply for credentials and how the users'
2462 credentials will be delivered to them;
- 2463 c) how Subscribers and/or Subjects acknowledge receipt of tokens and credentials
2464 and what obligations they accept in so doing (including whether they consent to
2465 publication of their details in credential status directories);
- 2466 d) how credentials may be renewed, modified, revoked, and suspended, including
2467 how requestors are authenticated or their identity proven;
- 2468 e) what actions a Subscriber or Subject must take to terminate a subscription;
- 2469 f) how records are retained and archived.

2470 *AL3_CM_CPP#015 Credential Policy reference*

2471 **MANDATORY.**

2472 Include in its Service Definition, either directly or by accessible reference, the policy
2473 against which it issues credentials. {source [5415] KI.10.2.2.1#22}

2474 *AL3_CM_CPP#020 No stipulation*

2475 *AL3_CM_CPP#030 Management Authority*

2476 **MANDATORY.**

2477 Have a nominated or appointed high-level management body with authority and
2478 responsibility for approving the Certificate Policy and Certification Practice Statement,
2479 including ultimate responsibility for their proper implementation.

2480

2481 **5.3.1.2 Security Controls**

2482 *AL3_CM_CTR#010 Withdrawn*

2483 *AL3_CM_CTR#020 Protocol threat risk assessment and controls*

2484 Account for at least the following protocol threats in its risk assessment and apply
2485 controls that reduce them to acceptable risk levels:

- 2486 a) password guessing, such that there are at least 24 bits of entropy to resist an on-
2487 line guessing attack against a selected user/password;
- 2488 b) message replay, showing that it is impractical;
- 2489 c) eavesdropping, showing that it is impractical;
- 2490 **d) relying party (verifier) impersonation, showing that it is impractical;**
- 2491 e) man-in-the-middle attack;
- 2492 **f) session hijacking, showing that it is impractical.**

2493 **The above list shall not be considered to be a complete list of threats to be addressed**
2494 **by the risk assessment.**

2495 **Guidance:** Organizations should consider potential protocol threats identified in other
2496 sources, e.g. ISO/IEC 29115:2013 “Information technology -- Security techniques –
2497 Entity authentication assurance framework”.

2498 *AL3_CM_CTR#025 Permitted authentication protocols*

2499 **For non-PKI credentials,** apply only authentication protocols which, through a
2500 comparative risk assessment which takes into account the target Assurance Level, are
2501 shown to have resistance to attack at least as strong as that provided by commonly-
2502 recognized protocols such as:

- 2503 d) tunneling;
- 2504 e) zero knowledge-based;
- 2505 f) signed SAML [Omitted].

2506 *AL3_CM_CTR#028 No Stipulation*

2507 *AL3_CM_CTR#030 System threat risk assessment and controls*

2508 **MANDATORY.**

2509 Account for the following system threats in its risk assessment and apply controls that
2510 reduce them to acceptable risk levels:

- 2511 a) the introduction of malicious code;
- 2512 b) compromised authentication arising from insider action;
- 2513 c) out-of-band attacks by both users and system operators (e.g., shoulder-surfing);
- 2514 d) spoofing of system elements/applications;
- 2515 e) malfeasance on the part of Subscribers and Subjects;
- 2516 f) intrusions leading to information theft.

2517 The above list shall not be considered to be a complete list of threats to be addressed by
2518 the risk assessment.

2519 **Guidance:** the risk assessment should address these threats from any perspective in
2520 which they might adversely affect the operation of the service, whether they be from
2521 within the organization (e.g. in its development environment, the hosting environment) or
2522 without (e.g. network attacks, hackers).

2523 *AL3_CM_CTR#040 Specified Service's Key Management*

2524 Specify and observe procedures and processes for the generation, storage, and destruction
2525 of its own cryptographic keys used for securing the specific service's assertions and other
2526 publicized information. At a minimum, these should address:

- 2527 a) the physical security of the environment;
- 2528 b) access control procedures limiting access to the minimum number of authorized
2529 personnel;
- 2530 c) public-key publication mechanisms;
- 2531 d) application of controls deemed necessary as a result of the service's risk
2532 assessment;
- 2533 e) destruction of expired or compromised private keys in a manner that prohibits
2534 their retrieval or their archival in a manner that prohibits their reuse;
- 2535 f) applicable cryptographic module security requirements, quoting [IS19790] or
2536 equivalent, as established by a recognized national technical authority.

2537 **5.3.1.3 Storage of Long-term Secrets**

2538 An enterprise and its specified service must:

2539 *AL3_CM_STS#010 Withdrawn*

2540 Withdrawn (AL3_CO_SCO#020 (a) & (b) enforce this requirement).

2541 *AL3_CM_STS#020 Stored Secret Encryption*

2542 **Encrypt such shared secret files so that:**

- 2543 a) the encryption key for the shared secret file is encrypted under a key held in
2544 an [IS19790] Level 2 or higher validated hardware or software cryptographic
2545 module or any [IS19790] Level 3 or 4 cryptographic module, or equivalent,
2546 as established by a recognized national technical authority;
2547 b) the shared secret file is decrypted only as immediately required for an
2548 authentication operation;
2549 c) shared secrets are protected as a key within the boundary of an [IS19790]
2550 Level 2 or higher validated hardware cryptographic module or any [IS19790]
2551 Level 3 or 4 cryptographic module and are not exported from the module in
2552 plain text, or equivalent, as established by a recognized national technical
2553 authority;
2554 d) shared secrets are split by an "n from m" cryptographic secret sharing
2555 method.

2556 5.3.1.4 Security-relevant Event (Audit) Records

2557 These criteria describe the need to provide an auditable log of all events that are pertinent
2558 to the correct and secure operation of the service. The common organizational criteria
2559 applying to provision of an auditable log of all security-related events pertinent to the
2560 correct and secure operation of the service must also be considered carefully. These
2561 criteria carry implications for credential management operations.

2562 In the specific context of a certificate management service, an enterprise and its specified
2563 service must:

2564 *AL3_CM_SER#010 Security event logs*

2565 **MANDATORY, to the extent that the sub-items relate to the scope of service.**

2566 **Ensure that such audit records include:**

- 2567 a) the identity of the point of registration (irrespective of whether internal or
2568 outsourced);
2569 b) generation of the Subject's keys or the evidence that the Subject was in
2570 possession of both parts of their own key-pair;
2571 c) generation of the Subject's certificate;
2572 d) dissemination of the Subject's certificate;
2573 e) any revocation or suspension associated with the Subject's certificate.

2574 5.3.1.5 Subject options

2575 *AL3_CM_OPN#010 Changeable PIN/Password*

2576 Withdrawn – see AL3_CM_RNR#010.

2577 **5.3.2 Part B - Credential Issuing**

2578 These criteria apply to the verification of the identity of the Subject of a credential and
2579 with token strength and credential delivery mechanisms. They address requirements
2580 levied by the use of various technologies to achieve Assurance Level 3.

2581 **5.3.2.1 Identity Proofing Policy**

2582 The specific service must show that it applies identity proofing policies and procedures
2583 and that it retains appropriate records of identity proofing activities and evidence.

2584 The enterprise and its specified service must:

2585 *AL3_ID_POL#010 Unique service identity*

2586 Ensure that a unique identity is attributed to the specific service, such that credentials
2587 issued by it can be distinguishable from those issued by other services, including services
2588 operated by the same enterprise.

2589 *AL3_ID_POL#020 Unique Subject identity*

2590 Ensure that each applicant's identity is unique within the service's community of Subjects
2591 and uniquely associable with tokens and/or credentials issued to that identity.

2592 **Guidance:** Cf. AL3_CM_CRN#020 which expresses a very similar requirement.

2593 Although presenting repetition for a single provider, if the identity-proofing functions and
2594 credential management functions are provided by separate CSPs, each needs to fulfill this
2595 requirement.

2596 *AL3_ID_POL#030 Published Proofing Policy*

2597 Make available the Identity Proofing Policy under which it verifies the identity of
2598 applicants⁴ in form, language, and media accessible to the declared community of Users.

2599 *AL3_ID_POL#040 Adherence to Proofing Policy*

2600 Perform all identity proofing strictly in accordance with its published Identity Proofing
2601 Policy, **through application of the procedures and processes set out in its Identity**
2602 **Proofing Practice Statement (IdPPS).**

2603 **5.3.2.2 Identity Proofing**

2604 The enterprise or specific service:

2605 *AL3_ID_IDV#000 Identity Proofing classes*

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

- 2606 a) must include in its Service Definition at least one of the following classes of
2607 identity proofing services, and;
- 2608 b) may offer any additional classes of identity proofing service it chooses, Subject to
2609 the nature and the entitlement of the CSP concerned;
- 2610 c) must fulfill the applicable assessment criteria according to its choice of identity
2611 proofing service, i.e. conform to at least one of the criteria sets defined in:
- 2612 i) §0, “[In-Person Public Identity Verification](#)”;
- 2613 ii) §5.3.2.4, “[Remote Public Identity Verification](#)”;
- 2614 iii) §5.3.2.5, “[Current Relationship Identity Verification](#)”;
- 2615 iv) §5.3.2.6, “[Affiliation Identity Verification](#)”.
- 2616 although, in any of the above cases, the criteria defined in §5.3.2.7 may be
2617 substituted for identity proofing where the Applicant already possesses a
2618 recognized credential at **Level 4**

2619 *AL3_ID_IDV#010 - Identity Verification Measures*

2620 For each identity proofing service offered (see above [*i.e.* AL3_IDV#000]) justify the
2621 identity verification measures **described in its IdPPS (see AL3_ID_POL#040)** by
2622 describing how these meet or exceed the requirements of applicable policies, regulations,
2623 adopted standards and other relevant conditions in order to maintain a level of rigour
2624 consistent with the AL3.

2625 **Guidance:** Although strict requirements for identity proofing and verification can be
2626 defined, a real-world approach must account for instances where there is not 100%
2627 certitude. To cope with this CSPs need to have a set of prescribed (through policy – see
2628 AL3_ID_POL#030) and applied measures (see AL3_ID_POL#040) which observe
2629 policy, identify the measures taken according to the degree of certitude determined by
2630 each step in the verification process and what additional measures are taken. The CSP
2631 must present a case which shows that their solution is sufficient to ensure that the basic
2632 requirements of the applicable AL are met or exceeded.

2633 Note that in each set of proofing service criteria below there are criteria with specific
2634 requirements for evidence checks and an additional criterion for ‘secondary’ checks, all of
2635 which have an interplay with these overall requirements to have a policy and practice
2636 statement and to demonstrate processes which sustain confidence that AL3 is being
2637 achieved.

2638 Even though a CSP may use the services of a component service for the performance of
2639 the identity-proofing within its own service, it still needs to ensure that its policy is both
2640 justified and upheld. Where another service provider is used appropriate stipulations in
2641 contracts should be established, but any internal adherence to (e.g.) POL#040 should be
2642 determined by the fact that the component service is already Kantara Approved.

2643 **5.3.2.3 In-Person Public Identity Proofing**

2644 A specific service that offers identity proofing to applicants with whom it has no previous
2645 relationship must comply with the criteria in this section.

2646 The enterprise or specified service must:

2647 *AL3_ID_IPV#010 Required evidence*

2648 Ensure that the applicant is in possession of a primary Government Picture ID document
2649 that bears a photographic image of the holder.

2650 *AL3_ID_IPV#020 Evidence checks*

2651 **Have in place and apply processes which ensure** that the presented document:

- 2652 a) appears to be a genuine document properly issued by the claimed issuing
2653 authority and valid at the time of application;
- 2654 b) bears a photographic image of the holder that matches that of the applicant;
- 2655 c) **is electronically verified by a record check with the specified issuing**
2656 **authority or through similar databases that:**
- 2657 i) **establishes the existence of such records with matching name and**
2658 **reference numbers;**
- 2659 ii) **corroborates date (year, month and day) of birth, current address of**
2660 **record, and other personal information sufficient to ensure a unique**
2661 **identity;**
- 2662 d) provides all reasonable certainty that the identity exists and that it uniquely
2663 identifies the applicant.

2664 **5.3.2.4 Remote Public Identity Proofing**

2665 A specific service that offers remote identity proofing to applicants with whom it has no
2666 previous relationship must comply with the criteria in this section.

2667 The enterprise or specified service must:

2668 *AL3_ID_RPV#010 Required evidence*

2669 Ensure that the applicant submits the references of and attests to current possession of a
2670 primary Government [omitted] ID document, and one of:

- 2671 a) a second Government ID;
- 2672 b) an employee or student ID number;
- 2673 c) a financial account number (e.g., checking account, savings account, loan, or
2674 credit card), or;
- 2675 d) a utility service account number (e.g., electricity, gas, or water) for an address
2676 matching that in the primary document.
- 2677 e) Omitted

2678 Ensure that the applicant provides additional verifiable personal information that at a
2679 minimum must include:

2680 f) a name that matches the referenced ID;

2681 g) date (year, month and day) of birth;

2682 h) current address [omitted].

2683 Additional information may be requested so as to ensure a unique identity, and alternative
2684 information may be sought where the enterprise can show that it leads to at least the same
2685 degree of certitude when verified.

2686 *AL3_ID_RPV#020 Evidence checks*

2687 **Electronically verify by a record check** against the provided identity references with the
2688 specified issuing authorities/institutions or through similar databases, according to the
2689 inspection rules set by the issuing authorities:

2690 a) the existence of such records with matching name and reference numbers;

2691 b) corroboration of date (year, month and day) of birth, contact information of record
2692 [omitted], and other personal information sufficient to ensure a unique identity;

2693 c) dynamic verification of personal information previously provided by or likely to
2694 be known only by the applicant

2695 d) for a telephone service account, confirmation that the phone number supplied by
2696 the applicant is associated in Records with the Applicant's name and address of
2697 record and by having the applicant demonstrate that they are able to send or
2698 receive messages at the phone number.

2699 Confirm contact information of record by at least one of the following means, ensuring
2700 that any secret sent over an unprotected channel shall be reset upon first use and shall be
2701 valid for a maximum lifetime of seven days:

2702 e) RA sends notice to an address of record confirmed in the records check and
2703 receives a mailed or telephonic reply from applicant;

2704 f) RA issues credentials in a manner that confirms the address of record supplied by
2705 the applicant, for example by requiring applicant to enter on-line some
2706 information from a notice sent to the applicant;

2707 g) RA issues credentials in a manner that confirms ability of the applicant to receive
2708 telephone communications at telephone number or email at email address
2709 associated with the applicant in records.

2710 h) **[Omitted]**

2711 Additional checks may be performed so as to establish the uniqueness of the claimed
2712 identity (see AL3_ID_SCV#010).

2713 Alternative checks may be performed where the enterprise can show that they lead to a
2714 comparable degree of certitude (see AL3_ID_SCV#010).

2715 **5.3.2.5 Current Relationship Identity Proofing**

2716 If the specific service offers identity proofing to applicants with whom it has a current
2717 relationship, then it must comply with the criteria in this section.

2718 The enterprise or specified service must:

2719 *AL3_ID_CRV#010 Required evidence*

2720 Ensure that it has previously exchanged with the applicant a shared secret (e.g., a PIN or
2721 password) that meets AL3 (or higher) entropy requirements⁵.

2722 *AL3_ID_CRV#020 Evidence checks*

2723 Ensure that it has:

- 2724 a) only issued the shared secret after originally establishing the applicant's identity:
2725 i) with a degree of rigor equivalent to that required under either the AL3 (or
2726 higher) requirements for in-person or remote public verification; or
2727 ii) by complying with regulatory requirements effective within the applicable
2728 jurisdiction which set forth explicit proofing requirements which include a
2729 prior in-person appearance by the applicant and are defined as meeting AL3
2730 (or higher) requirements;
2731 b) an ongoing business relationship sufficient to satisfy the enterprise of the
2732 applicant's continued personal possession of the shared secret.

2733 **5.3.2.6 Affiliation Identity Proofing**

2734 A specific service that offers identity proofing to applicants on the basis of some form of
2735 affiliation must comply with the criteria in this section to establish that affiliation and
2736 with the previously stated requirements to verify the individual's identity.

2737 The enterprise or specified service must:

2738 *AL3_ID_AJV#000 Meet preceding criteria*

2739 Meet all the criteria set out above, under §5.3.2.4, "[Remote Public Identity](#)
2740 [Verification](#)".

2741 *AL3_ID_AJV#010 Required evidence*

2742 Ensure that the applicant possesses:

- 2743 a) identification from the organization with which it is claiming affiliation;
2744 b) agreement from the organization that the applicant may be issued a credential
2745 indicating that an affiliation exists.

2746 *AL3_ID_AJV#020 Evidence checks*

2747 Have in place and apply processes which ensure that the presented documents:

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

- 2748 a) each appear to be a genuine document properly issued by the claimed issuing
2749 authorities and valid at the time of application;
2750 b) refer to an existing organization with a contact address;
2751 c) indicate that the applicant has some form of recognizable affiliation with the
2752 organization;
2753 d) appear to grant the applicant an entitlement to obtain a credential indicating an
2754 affiliation with the organization.

2755 **5.3.2.7 Identity-proofing based on Recognized Credentials**

2756 Where the Applicant already possesses recognized original credentials the CSP may
2757 choose to accept the verified identity of the Applicant as a substitute for identity proofing,
2758 subject to the following specific provisions. All other requirements of Assurance Level 3
2759 identity proofing must also be observed.

2760 *AL3_ID_IDC#010 Authenticate Original Credential*

2761 Prior to issuing any derived credential the original credential on which the identity-
2762 proofing relies must be:

- 2763 a) authenticated by a source trusted by the CSP as being valid and un-revoked;
2764 b) issued at **Assurance Level 4**;
2765 c) issued in the same name as that which the Applicant is claiming;
2766 d) proven to be in the possession and under the control of the Applicant.

2767 **Guidance:** This is the equivalent of recording the details of **identity-proofing** documents
2768 provided during (e.g.) face-face id-proofing. It is not required that the original credential
2769 be issued by a Kantara-Approved CSP.

2770 *AL3_ID_IDC#020 Record Original Credential*

2771 Record the details of the original credential.

2772 *AL3_ID_IDC#030 Issue Derived Credential*

2773 Before issuing the derived credential ensure that:

- 2774 a) for in-person issuance, the claimant is the Applicant;
2775 b) for remote issuance, token activation requires proof of possession of both the
2776 derived token and the original **Level 4** token.

2777 **5.3.2.8 Secondary Identity-proofing**

2778 In each of the above cases, the enterprise or specified service must also meet the
2779 following criteria:

2780 *AL3_ID_SCV#010 Secondary checks*

2781 Have in place additional measures (e.g., require additional documentary evidence, delay
2782 completion while out-of-band checks are undertaken) to deal with:

- 2783 a) any reasonably anomalous circumstance that can reasonably be anticipated (e.g.,
2784 a legitimate and recent change of address that has yet to be established as the
2785 address of record);
- 2786 b) any use of processes and/or technologies which may not fully meet the preceding
2787 applicable requirements but which are deemed to be comparable and thus able to
2788 support AL3.

2789 5.3.2.9 Identity-proofing Records

2790 The specific service must retain records of the identity proofing (verification) that it
2791 undertakes and provide them to qualifying parties when so required.

2792 The enterprise or specified service must:

2793 *AL3_ID_VRC#010 Verification Records for Personal Applicants*

2794 Log, taking account of all applicable legislative and policy obligations, a record of the
2795 facts of the verification process including a reference relating to the verification
2796 processes, the date and time of verification and the identity of the registrar (person, or
2797 entity if remote or automatic) performing the proofing functions.

2798 **Guidance:** The facts of the verification process should include the specific record
2799 information (source, unique reference, value/content) used in establishing the applicant's
2800 identity, and will be determined by the specific processes used and documents accepted
2801 by the CSP. The CSP need not retain these records itself if it uses a third-party service
2802 which retains such records securely and to which the CSP has access when required, in
2803 which case it must retain a record of the identity of the third-party service providing the
2804 verification service or the location at which the (in-house) verification was performed.

2805 *AL3_ID_VRC#020 Verification Records for Affiliated Applicants*

2806 In addition to the foregoing, log, taking account of all applicable legislative and policy
2807 obligations, a record of the additional facts of the verification process [omitted].

2808 **Guidance:** Although there is no specific stipulation as to what should be recorded the
2809 list below suggests facts which would typically be captured:

- 2810 a) the Subject's full name;
- 2811 b) the Subject's current telephone or email address of record;
- 2812 c) the Subject's acknowledgement of issuing the Subject with a credential;
- 2813 d) type, issuing authority, and reference number(s) of all documents checked in the
2814 identity proofing process;
- 2815 e) where required, a telephone or email address for related contact and/or delivery of
2816 credentials/notifications.

2817 *AL3_ID_VRC#025 Provide Subject Identity Records*

2818 If required, provide to qualifying parties records of identity proofing to the extent
2819 permitted by applicable legislation and/or agreed by the Subscriber.

2820 **Guidance:** the qualifier ‘if required’ is intended to account for circumstances where
2821 conditions such as whether a contract or a federation policy permits or is required or
2822 jurisdiction / legal injunction demand such provision. A qualifying party is any party to
2823 which provision of such info can justified according to circumstance: by contract/policy;
2824 with Subject’s agreement; with due authority (Court Order, e.g.). The CSP needs to make
2825 the case, according to their service’s characteristics and operating environment.

2826 *AL3_ID_VRC#030 Record Retention*

2827 Either retain, securely, the record of the verification/revocation process for the duration of
2828 the Subject account plus a further period sufficient to allow fulfillment of any period
2829 required legally, contractually or by any other form of binding agreement or obligation ,
2830 or submit the same record to a client CSP that has undertaken to retain the record for the
2831 requisite period or longer.

2832 *AL3_CM_IDP#010 Revision to Subject information*

2833 Provide a means for Subjects to securely amend their stored information after
2834 registration, either by re-proving their identity as in the initial registration process or by
2835 using their credentials to authenticate their revision. Successful revision must instigate
2836 the re-issuance of the credential when the data being revised are bound into the
2837 credential.

2838 **Guidance:** The necessity for re-issuance will be determined by, *inter alia*, policy, the
2839 technology and practices in use, the nature of change (e.g. registration data not bound into
2840 the credential) and the nature of the proofing processes.

2841 *AL3_CM_IDP#020 Authenticate Subject Information Changes*

2842 Permit only changes which are supported by appropriate and sufficient authentication of
2843 the legitimacy of change according, to its type.

2844 **Guidance:** The requirement to authenticate the legitimacy of a change will depend upon
2845 what is retained by the CSP and what is being changed: whereas a change of address may
2846 require less demanding authentication than may a change of name, a change of date-of-
2847 birth would be very unlikely and therefore would require substantial supporting
2848 authentication.

2849 **5.3.2.10 Credential Creation**

2850 These criteria define the requirements for creation of credentials whose highest use is
2851 AL3. Any credentials/tokens that comply with the criteria stipulated at AL4 are also
2852 acceptable at AL3 and below.

2853 Note, however, that a token and credential type required by a higher AL but created
2854 according to these criteria may not necessarily provide that higher level of assurance for
2855 the claimed identity of the Subject. Authentication can only be provided at the assurance
2856 level at which the identity is proven.

2857 An enterprise and its specified service must:

2858 *AL3_CM_CRN#010 Authenticated Request*

2859 Only accept a request to generate a credential and bind it to an identity if the source of the
2860 request, i.e., Registration Authority, can be authenticated as being authorized to perform
2861 identity proofing at AL3 or higher.

2862 *AL3_CM_CRN#020 Unique identity*

2863 Ensure that the identity which relates to a specific applicant is unique within the specified
2864 service, including identities previously used and that are now cancelled other than its re-
2865 assignment to the same applicant.

2866 **Guidance:** This requirement is intended to prevent identities that may exist in a Relying
2867 Party's access control lists from possibly representing a different physical person.

2868 Cf. AL3_CM_POL#020 which expresses a very similar requirement. Although
2869 presenting repetition for a single provider, if the identity-proofing functions and
2870 credential management functions are provided by separate CSPs, each needs to fulfill this
2871 requirement.

2872 *AL3_CM_CRN#030 Credential uniqueness*

2873 Allow the Subject to select a credential (e.g., UserID) that is verified to be unique within
2874 the specified service's community and assigned uniquely to a single identity Subject.
2875 **Default names shall not be permitted.** {source [5415] KI.10.3.2.1#04}

2876 *AL3_CM_CRN#035 Convey credential*

2877 Be capable of conveying the unique identity information associated with a credential to
2878 Verifiers and Relying Parties.

2879 *AL3_CM_CRN#040 Token strength*

2880 **Not use PIN/password tokens.**

2881 *AL3_CM_CRN#050 One-time password strength*

2882 Only allow one-time password tokens that:

- 2883 a) **depend on a symmetric key stored on a personal hardware device validated**
2884 **against [IS19790] Level 1 or higher, or equivalent, as established by a**
2885 **recognized national technical authority;**
2886 b) **permit at least 10⁶ possible password values;**
2887 c) **require password or biometric activation by the Subject.**

2888 *AL3_CM_CRN#055 No stipulation*

2889 *AL3_CM_CRN#060 Software cryptographic token strength*

2890 Ensure that software cryptographic keys stored on general-purpose devices:

- 2891 a) **are protected by a key and cryptographic protocol that are validated against**
2892 **[IS19790] Level 1, or equivalent, as established by a recognized national**
2893 **technical authority;**
2894 b) **require password or biometric activation by the Subject or employ a**
2895 **password protocol when being used for authentication;**

2896 c) **erase any unencrypted copy of the authentication key after each**
2897 **authentication.**

2898 *AL3_CM_CRN#070 Hardware token strength*

2899 Ensure that hardware tokens used to store cryptographic keys:

2900 a) employ a cryptographic module that is validated against [IS19790] Level 1 or
2901 higher, or equivalent, as established by a recognized national technical authority;

2902 b) **require password or biometric activation by the Subject or also employ a**
2903 **password when being used for authentication;**

2904 c) **erase any unencrypted copy of the authentication key after each**
2905 **authentication;**

2906 d) are locked prior to their delivery, once personalization processes have been
2907 completed. {source [5415] KI.10.2.2.1#07}

2908 *AL3_CM_CRN#075 No stipulation*

2909 *AL3_CM_CRN#080 Binding of key*

2910 **If the specified service generates the Subject's key pair, that the key generation**
2911 **process securely and uniquely binds that process to the certificate generation and**
2912 **maintains at all times the secrecy of the private key, until it is accepted by the**
2913 **Subject.**

2914 *AL3_CM_CRN#085 Hardware Inventory Control*

2915 **Prior to issuance, if a credential, or the means to produce credentials, is held on a**
2916 **hardware device, the hardware device shall be kept physically secure and the**
2917 **inventory tracked.** {source [5415] KI.10.2.2.1#08}

2918 *AL3_CM_CRN#090 Nature of Subject*

2919 Record the nature of the Subject of the credential (which must correspond to the manner
2920 of identity proofing performed), i.e., private person, a named person acting on behalf of a
2921 corporation or other legal entity, corporation or legal entity, or corporate machine entity,
2922 in a manner that can be unequivocally associated with the credential and the identity that
2923 it asserts.

2924 *AL3_CM_CRN#095 No stipulation*

2925 No stipulation

2926 **5.3.2.11 Subject Key Pair Generation**

2927 An enterprise and its specified service must:

2928 *AL3_CM_SKP#010 Key generation by Specified Service*

2929 **If the specified service generates the Subject's keys:**

- 2930 a) use an [IS19790] compliant algorithm, or equivalent, as established by a
2931 recognized national technical authority, that is recognized as being fit for the
2932 purposes of the service;
- 2933 b) only create keys of a key length and for use with an [IS19790] compliant
2934 public key algorithm, or equivalent, as established by a recognized national
2935 technical authority, recognized as being fit for the purposes of the service;
- 2936 c) generate and store the keys securely until delivery to and acceptance by the
2937 Subject;
- 2938 d) deliver the Subject's private key in a manner that ensures that the privacy of
2939 the key is not compromised and only the Subject has access to the private
2940 key.

2941 *AL3_CM_SKP#020 Key generation by Subject*

2942 **If the Subject generates and presents its own keys, obtain the Subject's written**
2943 **confirmation that it has:**

- 2944 a) used an [IS19790] compliant algorithm, or equivalent, as established by a
2945 recognized national technical authority, that is recognized as being fit for the
2946 purposes of the service;
- 2947 b) created keys of a key length and for use with an [IS19790] compliant public
2948 key algorithm, or equivalent, as established by a recognized national
2949 technical authority, recognized as being fit for the purposes of the service.

2950 **5.3.2.12 Credential Delivery**

2951 An enterprise and its specified service must:

2952 *AL3_CM_CRD#010, Notify Subject of Credential Issuance*

2953 Notify the Subject of the credential's issuance and, if necessary, confirm Subject's contact
2954 information by:

- 2955 a) sending notice to the address of record confirmed during identity proofing, **and**
2956 **either:**
- 2957 i) **issuing the credential(s) in a manner that confirms the address of**
2958 **record supplied by the applicant during identity proofing, or;**
- 2959 ii) **issuing the credential(s) in a manner that confirms the ability of the**
2960 **applicant to receive telephone communications at a phone number**
2961 **supplied by the applicant during identity proofing, while recording**
2962 **the applicant's voice.**

2963 **Guidance:** The nature of issuance could mean that the Subject is fully aware and
2964 therefore no notification is necessary. If any other such circumstances prevailed, the CSP
2965 should identify them.

2966 *AL3_CM_CRD#015 Confirm Applicant's identity (in person)*

2967 Prior to delivering the credential, require the Applicant to identify themselves in person in
2968 any new transaction (beyond the first transaction or encounter) by either:

2969 (a) using a temporary secret which was established during **the** prior transaction or
2970 encounter (**whilst ensuring that such temporary secrets are used only**
2971 **once**), or sent to the Applicant's phone number, email address, or physical
2972 address of record, or;

2973 (b) matching a biometric sample against a reference sample that was recorded
2974 during a prior encounter.

2975 *AL3_CM_CRD#016 Confirm Applicant's identity (remotely)*

2976 Prior to **activating** the credential, require the Applicant to identify themselves in any new
2977 electronic transaction (beyond the first transaction or encounter) by presenting a
2978 temporary secret which was established during a prior transaction or encounter, or sent to
2979 the Applicant's phone number, email address, or physical address of record.

2980 **Guidance:** Activation typically requires that the credential be delivered to the
2981 Applicant/Subject before activation occurs.

2982 *AL3_CM_CRD#017 Protected Issuance of Permanent Secrets (in person)*

2983 **Only issue permanent secrets if the CSP has loaded the secret itself onto the physical**
2984 **device, which was either:**

2985 a) **issued in-person to the Applicant, or;**

2986 b) **delivered in a manner that confirms the address of record.**

2987 *AL3_CM_CRD#018 Protected Issuance of Permanent Secrets (remotely)*

2988 **Only issue permanent secrets within a protected session.**

2989 *AL3_CM_CRD#020 Subject's acknowledgement*

2990 **Receive acknowledgement of receipt of the credential before it is activated and its**
2991 **directory status record is published (and thereby the subscription becomes active or**
2992 **re-activated, depending upon the circumstances of issue).**

2993

2994 **5.3.3 Part C - Credential Renewal and Re-issuing**

2995 These criteria apply to the renewal and re-issuing of credentials. They address
2996 requirements levied by the use of various technologies to achieve Assurance Level 3.

2997 **5.3.3.1 Renewal/Re-issuance Procedures**

2998 These criteria address general renewal and re-issuance functions, to be exercised as
2999 specific controls in these circumstances while continuing to observe the general
3000 requirements established for initial credential issuance.

3001 An enterprise and its specified service must:

3002 *AL3_CM_RNR#010 Changeable PIN/Password*

3003 Permit Subjects to change **the passwords used to activate their credentials.**

3004 *AL3_CM_RNR#020 Proof-of-possession on Renewal/Re-issuance*

3005 Subjects wishing to change their passwords must demonstrate that they are in possession
3006 of the unexpired current token prior to the CSP proceeding to renew or re-issue it.

3007 *AL3_CM_RNR#030 Renewal/Re-issuance limitations*

3008 a) **No stipulation;**

3009 b) **neither renew nor re-issue expired tokens ;**

3010 c) **No stipulation;**

3011 **d)** conduct all renewal / re-issuance interactions with the Subject over a protected
3012 channel such as SSL/TLS.

3013 **Guidance:** Renewal is considered as an extension of usability, whereas re-issuance
3014 requires a change.

3015 *AL3_CM_RNR#040 No stipulation*

3016 No stipulation.

3017 *AL3_CM_RNR#050 Record Retention*

3018 Retain, securely, the record of any renewal/re-issuance process for the duration of the
3019 Subscriber's account plus a further period sufficient to allow fulfillment of any period
3020 required legally, contractually or by any other form of binding agreement or obligation, or
3021 submit same record to a client CSP that has undertaken to retain the record for the
3022 requisite period or longer.

3023 **5.3.4 Part D - Credential Revocation**

3024 These criteria deal with credential revocation and the determination of the legitimacy of a
3025 revocation request.

3026 **5.3.4.1 Revocation Procedures**

3027 These criteria address general revocation functions, such as the processes involved and
3028 the basic requirements for publication.

3029 An enterprise and its specified service must:

3030 *AL3_CM_RVP#010 Revocation procedures*

3031 a) State the conditions under which revocation of an issued credential may occur;

3032 b) State the processes by which a revocation request may be submitted;

- 3033 c) State the persons and organizations from which a revocation request will be
3034 accepted;
- 3035 d) State the validation steps that will be applied to ensure the validity (identity) of
3036 the Revocant, and;
- 3037 e) State the response time between a revocation request being accepted and the
3038 publication of revised certificate status.
- 3039 *AL3_CM_RVP#020 Secure status notification*
3040 Ensure that published credential status notification information can be relied upon in
3041 terms of the enterprise being its origin (i.e., its authenticity) and its correctness (i.e., its
3042 integrity).
- 3043 *AL3_CM_RVP#030 Revocation publication*
3044 **[Omitted]** Ensure that published credential status notification is revised within **24** hours
3045 of the receipt of a valid revocation request, such that any subsequent attempts to use that
3046 credential in an authentication shall be unsuccessful. **The nature of the revocation**
3047 **mechanism shall be in accord with the technologies supported by the service.**
- 3048 *AL3_CM_RVP#040 Verify Revocation Identity*
3049 Establish that the identity for which a revocation request is received is one that was
3050 issued by the specified service.
- 3051 *AL3_CM_RVP#045 No stipulation*
- 3052 *AL3_CM_RVP#050 Revocation Records*
3053 Retain a record of any revocation of a credential that is related to a specific identity
3054 previously verified, solely in connection to the stated credential. At a minimum, records
3055 of revocation must include:
- 3056 a) the Revocant's full name;
3057 b) the Revocant's authority to revoke (e.g., Subscriber or the Subject themselves,
3058 someone acting with the Subscriber's or the Subject's power of attorney, the
3059 credential issuer, law enforcement, or other legal due process);
3060 c) the Credential Issuer's identity (if not directly responsible for the identity
3061 proofing service);
3062 d) No stipulation;
3063 e) the reason for revocation.
- 3064 *AL3_CM_RVP#060 Record Retention*
3065 Retain, securely, the record of the revocation process for a period which is the maximum
3066 of:
- 3067 a) the records retention policy required by AL3_CM_CPP#010;
3068 b) applicable legislation, regulation, contract or standards.

3069 **5.3.4.2 Verify Revocant's Identity**

3070 Revocation of a credential requires that the requestor and the nature of the request be
3071 verified as rigorously as the original identity proofing. The enterprise should not act on a
3072 request for revocation without first establishing the validity of the request (if it does not,
3073 itself, determine the need for revocation).

3074 In order to do so, the enterprise and its specified service must:

3075 *AL3_CM_RVR#010 Verify revocation identity*

3076 Establish that the credential for which a revocation request is received is one that was
3077 initially issued by the specified service, applying the same process and criteria as would
3078 be applied to an original identity proofing, **ensuring that the Subject of the credential is**
3079 **uniquely identified.**

3080 *AL3_CM_RVR#020 Revocation reason*

3081 Establish the reason for the revocation request as being sound and well founded, in
3082 combination with verification of the Revocant, according to AL3_ID_RVR#030,
3083 AL3_ID_RVR#040, or AL3_ID_RVR#050.

3084 *AL3_CM_RVR#030 Verify Subscriber as Revocant*

3085 When the Subscriber or Subject seeks revocation of the Subject's credential:

- 3086 a) if in-person, require presentation of a primary Government Picture ID document
3087 that shall be electronically verified by a record check against the provided identity
3088 with the specified issuing authority's records;
3089 b) if remote:
3090 i. electronically verify a signature against records (if available), confirmed
3091 with a call to a telephone number of record, or;
3092 ii. as an electronic request, authenticate it as being from the same Subscriber
3093 or Subject, supported by a credential at Assurance Level 3 or higher.

3094 *AL3_CM_RVR#040 Verify CSP as Revocant*

3095 Where a CSP seeks revocation of a Subject's credential, establish that the request is
3096 either:

- 3097 a) from the specified service itself, with authorization as determined by established
3098 procedures, or;
3099 b) from the client Credential Issuer, by authentication of a formalized request over
3100 the established secure communications network.

3101 *AL3_CM_RVR#050 Verify Legal Representative as Revocant*

3102 Where the request for revocation is made by a law enforcement officer or presentation of
3103 a legal document:

- 3104 a) if in person, verify the identity of the person presenting the request, or;
3105 b) if remote:

- 3106 i. in paper/facsimile form, verify the origin of the legal document by a
3107 database check or by telephone with the issuing authority, or;
3108 ii. as an electronic request, authenticate it as being from a recognized legal
3109 office, supported by a credential at Assurance Level 3 or higher.

3110 **5.3.4.3 No stipulation**

3111 **5.3.4.4 Secure Revocation Request**

3112 This criterion applies when revocation requests must be communicated between remote
3113 components of the service organization.

3114 An enterprise and its specified service must:

3115 *AL3_CM_SRR#010 Submit Request*

3116 Submit a request for the revocation to the Credential Issuer service (function), using a
3117 secured network communication.

3118 **5.3.5 Part E - Credential Status Management**

3119 These criteria deal with credential status management, such as the receipt of requests for
3120 new status information arising from a new credential being issued or a revocation or other
3121 change to the credential that requires notification. They also deal with the provision of
3122 status information to requesting parties (Verifiers, Relying Parties, courts and others
3123 having regulatory authority, etc.) having the right to access such information.

3124 **5.3.5.1 Status Maintenance**

3125 An enterprise and its specified service must:

3126 *AL3_CM_CSM#010 Maintain Status Record*

3127 Maintain a record of the status of all credentials issued.

3128 *AL3_CM_CSM#020 Validation of Status Change Requests*

3129 Authenticate all requestors seeking to have a change of status recorded and published and
3130 validate the requested change before considering processing the request. Such validation
3131 should include:

- 3132 a) the requesting source as one from which the specified service expects to receive
3133 such requests;
3134 b) if the request is not for a new status, the credential or identity as being one for
3135 which a status is already held.

3136 *AL3_CM_CSM#030 Revision to Published Status*

3137 Process authenticated requests for revised status information and have the revised
3138 information available for access within a period of 72 hours.

3139 *AL3_CM_CSM#040 Status Information Availability*

3140 Provide, with 99% availability, a secure automated mechanism to allow relying parties to
3141 determine credential status and authenticate the Claimant's identity.

3142 *AL3_CM_CSM#050 Inactive Credentials*

3143 Disable any credential that has not been successfully used for authentication during a
3144 period of 18 months.

3145 **5.3.6 Part F - Credential Verification/Authentication**

3146 These criteria apply to credential validation and identity authentication.

3147 **5.3.6.1 Assertion Security**

3148 An enterprise and its specified service must:

3149 *AL3_CM_ASS#010 Validation and Assertion Security*

3150 Provide validation of credentials to a Relying Party using a protocol that:

- 3151 a) requires authentication of the specified service, itself, or of the validation source;
- 3152 b) ensures the integrity of the authentication assertion;
- 3153 c) protects assertions against manufacture, modification, substitution and disclosure,
3154 and secondary authenticators from manufacture, capture and replay;
- 3155 d) uses approved cryptography techniques;

3156 and which, specifically:

- 3157 e) creates assertions which are specific to a single transaction;
- 3158 f) where assertion references are used, generates a new reference whenever a new
3159 assertion is created;
- 3160 g) when an assertion is provided indirectly, either signs the assertion or sends it via a
3161 protected channel, using a strong binding mechanism between the secondary
3162 authenticator and the referenced assertion;
- 3163 h) send assertions either via a channel mutually-authenticated with the Relying
3164 Party, or signed and encrypted for the Relying Party;
- 3165 i) requires the secondary authenticator to:
 - 3166 i) be signed when provided directly to Relying Party, or;
 - 3167 ii) have a minimum of 64 bits of entropy when provision is indirect (i.e.
3168 through the credential user);
 - 3169 iii) be transmitted to the Subject through a protected channel which is linked
3170 to the primary authentication process in such a way that session hijacking
3171 attacks are resisted;
 - 3172 iv) not be subsequently transmitted over an unprotected channel or to an
3173 unauthenticated party while it remains valid.

3174 *AL3_CM_ASS#015 No False Authentication*

3175 Employ techniques which ensure that system failures do not result in ‘false positive
3176 authentication’ errors.

3177 *AL3_CM_ASS#018 Ensure token validity*

3178 **Ensure that tokens are either still valid or have been issued within the last 24 hours.**

3179 **Guidance:** The 24-hour period allows for the fact that if a freshly-issued credential is
3180 then revoked, notice of the revocation may take 24 hours to be publicised (per
3181 AL3_CM_RVP#030).

3182 *AL3_CM_ASS#020 Post Authentication*

3183 *Not* authenticate credentials that have been revoked unless the time of the transaction for
3184 which verification is sought precedes the time of revocation of the credential.

3185 **Guidance:** The purpose in this criterion is that, if a verification is intended to refer to the
3186 status of a credential at a specific historical point in time, e.g. to determine whether the
3187 Claimant was entitled to act as a signatory in a specific capacity at the time of the
3188 transaction, this may be done. It is implicit in this thinking that both the request and the
3189 response indicate the historical nature of the query and response; otherwise the default
3190 time is ‘now’. If no such service is offered then this criterion may simply be
3191 ‘Inapplicable’, for that reason.

3192 *AL3_CM_ASS#030 Proof of Possession*

3193 Use an authentication protocol that requires the claimant to prove possession and control
3194 of the authentication token.

3195 *AL3_CM_ASS#035 Limit authentication attempts*

3196 Unless the token authenticator has at least 64 bits of entropy, limit the number of failed
3197 authentication attempts to no more than 100 in any 30-day period.

3198 *AL3_CM_ASS#040 Assertion Lifetime*

3199 **For non-cryptographic credentials**, generate assertions so as to indicate and effect their
3200 expiration 12 hours after their creation; **otherwise, notify the relying party of how often**
3201 **the revocation status sources are updated.**

3202 **5.3.6.2 Authenticator-generated challenges**

3203 An enterprise and its specified service must:

3204 *AL3_CM_AGC#010 Entropy level*

3205 Create authentication secrets to be used during the authentication exchange (i.e. with out-
3206 of-band or cryptographic device tokens) with a degree of entropy appropriate to the token
3207 type in question.

3208 **5.3.6.3 Multi-factor authentication**

3209 An enterprise and its specified service must:

3210 *AL3_CM_MFA#010 Permitted multi-factor tokens*

3211 Require two tokens which, when used in combination within a single authentication
3212 exchange, are acknowledged as providing an equivalence of AL3, as determined by a
3213 recognized national technical authority.

3214 **5.3.6.4 Verifier's assertion schema**

3215 Note: Since assertions and related schema can be complex and may be modeled directly
3216 on the needs and preferences of the participants, the details of such schema fall outside
3217 the scope of the SAC's herein, which are expressed observing, insofar as is feasible, a
3218 technology-agnostic policy. The following criteria, therefore, are perhaps more open to
3219 variable conformity through their final implementation than are others in this document.

3220 These criteria are derived directly from NIST SP 800-63-2 and have been expressed in as
3221 generic a manner as they can be.

3222 *Editor's note: I have avoided reference to the RP here – I am concerned as to what the*
3223 *SAC requires services to do, not who might be using their products. SAC do not refer to*
3224 *RPs.*

3225 An enterprise and its specified service must:

3226 *AL3_CM_VAS#010 Approved cryptography*

3227 Apply assertion protocols which use cryptographic techniques approved by a national
3228 authority or other generally-recognized authoritative body.

3229 *AL3_CM_VAS#020 No stipulation*

3230 No stipulation.

3231 *AL3_CM_VAS#030 Assertion assurance level*

3232 Create assertions which, either explicitly or implicitly (using a mutually-agreed
3233 mechanism), indicate the assurance level at which the initial authentication of the Subject
3234 was made.

3235 *AL3_CM_VAS#040 No pseudonyms*

3236 Create assertions which indicate **only verified Subscriber names** in the credential
3237 subject to verification.

3238 *AL3_CM_VAS#050 Specify recipient*

3239 Create assertions which identify the intended recipient of the verification such that the
3240 recipient may validate that it is intended for them.

3241 *AL3_CM_VAS#060 No assertion manufacture/modification*

3242 Ensure that it is impractical to manufacture an assertion or assertion reference by **Signing**
3243 **the assertion and** using at least one of the following techniques:

3244 a) **no stipulation;**

- 3245 b) Encrypting the assertion using a secret key shared with the RP;
3246 c) Creating an assertion reference which has a minimum of 64 bits of entropy;
3247 d) Sending the assertion over a protected channel during a mutually-authenticated
3248 session.
- 3249 *AL3_CM_VAS#070 Assertion protections*
3250 Provide protection of assertion-related data such that:
- 3251 a) both assertions and assertion references are protected against capture and re-use;
3252 b) assertions are also protected against redirection;
3253 c) assertions, assertion references and session cookies used for authentication
3254 purposes, including any which are re-directed, are protected against session
3255 hijacking, for at least the duration of their validity (see AL3_CM_VAS#110).
- 3256 *AL3_CM_VAS#080 Single-use assertions*
3257 Limit to a single transaction the use of assertions which do not support proof of
3258 ownership.
- 3259 *AL3_CM_VAS#090 Single-use assertion references*
3260 Limit to a single transaction the use of assertion references.
- 3261 *AL3_CM_VAS#100 Bind reference to assertion*
3262 Provide a strong binding between the assertion reference and the corresponding assertion,
3263 based on integrity-protected (or signed) communications over which the Verifier has been
3264 authenticated.
- 3265 *AL3_CM_VAS#110 SSO provisions*
3266 **If SSO is supported, provide a re-authentication of the Subject so long as:**
- 3267 a) **the Subject has been successfully authenticated within the last 12 hours;**
3268 b) **the Subject continues to be able to demonstrate that they were the party that**
3269 **was previously authenticated;**
3270 c) **it can be ensured that the Subscriber has not been inactive for more than 30**
3271 **minutes.**
- 3272 **Guidance:** The conditional nature of this criterion is dictated by the phrasing used in
3273 NIST SP 800-63 which states ‘*may*’.
- 3274

3275 5.4 Assurance Level 4

3276 5.4.1 Part A - Credential Operating Environment

3277 These criteria describe requirements for the overall operational environment in which
3278 credential lifecycle management is conducted. The Common Organizational criteria
3279 describe broad requirements. The criteria in this Part describe operational
3280 implementation specifics.

3281 These criteria apply exclusively to cryptographic technology deployed through a Public
3282 Key Infrastructure. This technology requires hardware tokens protected by password or
3283 biometric controls. No other forms of credential are permitted at AL4.

3284 The following four criteria are **MANDATORY** for all Services, Full or Component, and
3285 are individually marked as such:

3286 AL4_CM_CPP#020, AL4_CM_CPP#030, AL4_CM_CTR#030, AL4_CM_SER#010.

3287 5.4.1.1 Certification Policy and Practices

3288 These criteria apply to the policy and practices under which certificates are managed.

3289 An enterprise and its specified service must:

3290 *AL4_CM_CPP#010 No stipulation*

3291 *AL4_CM_CPP#020 Certificate Policy/Certification Practice Statement*

3292 **MANDATORY.**

3293 **Include in its Service Definition its full Certificate Policy and may include the**
3294 **corresponding Certification and Practice Statement. The Certificate Policy and**
3295 **Certification Practice Statement must conform to IETF RFC 3647 (2003-11) [RFC**
3296 **3647] in their content and scope or be demonstrably consistent with the content or**
3297 **scope of that RFC. At a minimum, the Certificate Policy must specify:**

- 3298 a) applicable OIDs for each certificate type issued;
3299 b) how users may subscribe to the service/apply for certificates, and how
3300 certificates will be issued to them;
3301 c) if users present their own keys, how they will be required to demonstrate
3302 possession of the private key;
3303 d) if users' keys are generated for them, how the private keys will be delivered
3304 to them;
3305 e) how Subjects acknowledge receipt of tokens and credentials and what
3306 obligations they accept in so doing (including whether they consent to
3307 publication of their details in certificate status directories);

- 3308 f) **how certificates may be renewed, re-keyed, modified, revoked, and**
3309 **suspended, including how requestors are authenticated or their identity**
3310 **proven;**
3311 g) **what actions a Subject must take to terminate their subscription.**

3312 **Guidance:** Publication of the CSP is optional since in some cases its release may present
3313 a risk to the service. CSPs are therefore allowed to exercise their discretion in this matter.

3314 *AL4_CM_CPP#030 Management Authority*

3315 **MANDATORY.**

3316 Have a nominated or appointed high-level management body with authority and
3317 responsibility for approving the Certificate Policy and Certification Practice Statement,
3318 including ultimate responsibility for their proper implementation.

3319 *AL4_CM_CPP#040 Discretionary Access Control*

3320 **Apply discretionary access controls that limit access to trusted administrators and to**
3321 **those applications that require access.**

3322 **Guidance:** This requirement was previously AL3_CM_STS#010 b) (part a) having been
3323 withdrawn, which left part b) somewhat out of context.

3324 **5.4.1.2 Security Controls**

3325 An enterprise and its specified service must:

3326 *AL4_CM_CTR#010 Withdrawn*

3327 *AL4_CM_CTR#020 Protocol threat risk assessment and controls*

3328 Account for at least the following protocol threats in its risk assessment and apply
3329 controls that reduce them to acceptable risk levels:

- 3330 a) password guessing, **showing that there is sufficient entropy;**
3331 b) message replay, showing that it is impractical;
3332 c) eavesdropping, showing that it is impractical;
3333 d) relying party (verifier) impersonation, showing that it is impractical;
3334 e) man-in-the-middle attack, showing that it is impractical;

3335

3336 **f) session hijacking, showing that it is impractical.**

3337 The above list shall not be considered to be a complete list of threats to be addressed by
3338 the risk assessment.

3339 **Guidance:** Organizations should consider potential protocol threats identified in other
3340 sources, e.g. ISO/IEC 29115:2013 “Information technology -- Security techniques –
3341 Entity authentication assurance framework”.*AL4_CM_CTR#025 No stipulation*

3342 *AL4_CM_CTR#028 No Stipulation*

3343 *AL4_CM_CTR#030 System threat risk assessment and controls*

3344 **MANDATORY.**

3345 Account for the following system threats in its risk assessment and apply controls that
3346 reduce them to acceptable risk levels:

- 3347 a) the introduction of malicious code;
- 3348 b) compromised authentication arising from insider action;
- 3349 c) out-of-band attacks by both users and system operators (e.g., shoulder-surfing);
- 3350 d) spoofing of system elements/applications;
- 3351 e) malfeasance on the part of Subscribers and Subjects;
- 3352 f) intrusions leading to information theft.

3353 The above list shall not be considered to be a complete list of threats to be addressed by
3354 the risk assessment.

3355 **Guidance:** the risk assessment should address these threats from any perspective in
3356 which they might adversely affect the operation of the service, whether they be from
3357 within the organization (e.g. in its development environment, the hosting environment) or
3358 without (e.g. network attacks, hackers).

3359 *AL4_CM_CTR#040 Specified Service's Key Management*

3360 Specify and observe procedures and processes for the generation, storage, and destruction
3361 of its own cryptographic keys used for securing the specific service's assertions and other
3362 publicized information. At a minimum, these should address:

- 3363 a) the physical security of the environment;
- 3364 b) access control procedures limiting access to the minimum number of authorized
3365 personnel;
- 3366 c) public-key publication mechanisms;
- 3367 d) application of controls deemed necessary as a result of the service's risk
3368 assessment;
- 3369 e) destruction of expired or compromised private keys in a manner that prohibits
3370 their retrieval, or their archival in a manner which prohibits their reuse;
- 3371 f) applicable cryptographic module security requirements, quoting [IS19790] or
3372 equivalent, as established by a recognized national technical authority.

3373 **5.4.1.3 Storage of Long-term Secrets**

3374 The enterprise and its specified service must meet the following criteria:

3375 *AL4_CM_STS#010 Withdrawn*

3376 Withdrawn (AL4_CO_SCO#020 (a) & (b) enforce this requirement part a) and
3377 AL4_CM_CPP#040 now enforces part b))

3378 *AL4_CM_STS#020 Stored Secret Encryption*

3379 Encrypt such [omitted] secret files so that:

- 3380 a) the encryption key for the [omitted] secret file is encrypted under a key held in an
3381 [IS19790] [FIPS140-2] Level 2 or higher validated hardware cryptographic
3382 module or any [IS19790] Level 3 or 4 cryptographic module, or equivalent, as
3383 established by a recognized national technical authority;
- 3384 b) the [omitted] secret file is decrypted only as immediately required for a key
3385 recovery operation;
- 3386 c) [omitted] secrets are protected as a key within the boundary of an [IS19790]
3387 Level 2 or higher validated hardware cryptographic module or any [IS19790]
3388 Level 3 or 4 cryptographic module and are not exported from the module in
3389 plaintext, or equivalent, as established by a recognized national technical
3390 authority;
- 3391 d) escrowed secrets are split by an "n from m" cryptographic secret **storing** method.

3392 5.4.1.4 Security-relevant Event (Audit) Records

3393 These criteria describe the need to provide an auditable log of all events that are pertinent
3394 to the correct and secure operation of the service. The common organizational criteria
3395 relating to the recording of all security-related events must also be considered carefully.
3396 These criteria carry implications for credential management operations.

3397 In the specific context of a certificate management service, an enterprise and its specified
3398 service must:

3399 *AL4_CM_SER#010 Security event logs*

3400 **MANDATORY**, to the extent that the sub-items relate to the scope of service.

3401 Ensure that such audit records include:

- 3402 a) the identity of the point of registration (irrespective of whether internal or
3403 outsourced);
- 3404 b) generation of the Subject's keys or evidence that the Subject was in possession of
3405 both parts of the key-pair;
- 3406 c) generation of the Subject's certificate;
- 3407 d) dissemination of the Subject's certificate;
- 3408 e) any revocation or suspension associated with the Subject's credential.

3409 5.4.1.5 Subject Options

3410 *AL4_CM_OPN#010 Changeable PIN/Password*

3411 Withdrawn – see AL4_CM_RNR#010.

3412 **5.4.2 Part B - Credential Issuing**

3413 These criteria apply to the verification of the identity of the Subject of a credential and
3414 with token strength and credential delivery mechanisms. They address requirements
3415 levied by the use of various technologies to achieve Assurance Level 4.

3416 **5.4.2.1 Identity Proofing Policy**

3417 Identity proofing at Assurance Level 4 requires the physical presence of the applicant in
3418 front of the registration officer with photo ID or other readily verifiable biometric identity
3419 information, as well as the requirements set out by the following criteria.

3420 The specific service must show that it applies identity proofing policies and procedures
3421 and that it retains appropriate records of identity proofing activities and evidence.

3422 An enterprise and its specified service must:

3423 *AL4_ID_POL#010 Unique service identity*

3424 Ensure that a unique identity is attributed to the specific service, such that credentials
3425 issued by it can be distinguishable from those issued by other services, including services
3426 operated by the same enterprise.

3427 *AL4_ID_POL#020 Unique Subject identity*

3428 Ensure that each applicant's identity is unique within the service's community of Subjects
3429 and uniquely associable with tokens and/or credentials issued to that identity.

3430 **Guidance:** Cf. AL4_CM_CRN#020 which expresses a very similar requirement.

3431 Although presenting repetition for a single provider, if the identity-proofing functions and
3432 credential management functions are provided by separate CSPs, each needs to fulfill this
3433 requirement.

3434 *AL4_ID_POL#030 Published Proofing Policy*

3435 Make available the Identity Proofing Policy under which it verifies the identity of
3436 applicants⁶ in form, language, and media accessible to the declared community of users.

3437 *AL4_ID_POL#040 Adherence to Proofing Policy*

3438 Perform all identity proofing strictly in accordance with its published Identity Proofing
3439 Policy, through application of the procedures and processes set out in its Identity Proofing
3440 Practice Statement (IdPPS).

⁶ 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.

3441 **5.4.2.2 Identity Verification**

3442 The enterprise or specific service may:

3443 *AL4_ID_IDV#000 Identity Proofing classes*

3444 **[Omitted] offer only face-to-face identity proofing service. Remote verification is not**
3445 **allowed at this assurance level;**

3446 *AL4_ID_IDV#010 - Identity Verification Measures*

3447 **[Omitted]** Justify the identity verification measures described in its IdPPS (see
3448 *AL4_ID_POL#040*) by describing how these meet or exceed the requirements of
3449 applicable policies, regulations, adopted standards and other relevant conditions in order
3450 to maintain a level of rigour consistent with the **AL4**.

3451 **Guidance:** Although strict requirements for identity proofing and verification can be
3452 defined, a real-world approach must account for instances where there is not 100%
3453 certitude. To cope with this CSPs need to have a set of prescribed (through policy – see
3454 *AL4_ID_POL#030*) and applied measures (see *AL4_ID_POL#040*) which observe
3455 policy, identify the measures taken according to the degree of certitude determined by
3456 each step in the verification process and what additional measures are taken. The CSP
3457 must present a case which shows that their solution is sufficient to ensure that the basic
3458 requirements of the applicable AL are met or exceeded.

3459 Note that in each set of proofing service criteria below there are criteria with specific
3460 requirements for evidence checks and an additional criterion for ‘secondary’ checks, all of
3461 which have an interplay with these overall requirements to have a policy and practice
3462 statement and to demonstrate processes which sustain confidence that AL3 is being
3463 achieved.

3464 Even though a CSP may use the services of a component service for the performance of
3465 the identity-proofing within its own service, it still needs to ensure that its policy is both
3466 justified and upheld. Where another service provider is used appropriate stipulations in
3467 contracts should be established, but any internal adherence to (e.g.) ‘POL#040 should be
3468 determined by the fact that the component service is already Kantara Approved.

3469 **5.4.2.3 In-Person Public Identity Proofing**

3470 A specific service that offers identity proofing to applicants with whom it has no previous
3471 relationship must comply with the criteria in this section.

3472 The enterprise or specified service must:

3473 *AL4_ID_IPV#010 Required evidence*

3474 Ensure that the applicant is in possession of:

3475 **a)** a primary Government Picture ID document that bears a photographic image of
3476 **the holder and either:**

- 3477 i) secondary Government Picture ID or an account number issued by a
3478 regulated financial institution or;
3479 ii) two items confirming name, and address or telephone number, such
3480 as: utility bill, professional license or membership, or other evidence
3481 of equivalent standing.

3482 *AL4_ID_IPV#020 No stipulation*

3483 *AL4_ID_IPV#030 Evidence checks – primary ID*

3484 **Ensure that the presented document:**

- 3485 a) appears to be a genuine document properly issued by the claimed issuing
3486 authority and valid at the time of application;
3487 b) bears a photographic image of the holder which matches that of the
3488 applicant;
3489 c) is electronically verified by a record check with the specified issuing
3490 authority or through similar databases that:
3491 i) establishes the existence of such records with matching name and
3492 reference numbers;
3493 ii) corroborates date (year, month and day) of birth, current address of
3494 record, and other personal information sufficient to ensure a unique
3495 identity;
3496 d) provides all reasonable certainty, at AL4, that the identity exists and that it
3497 uniquely identifies the applicant.

3498 *AL4_ID_IPV#040 Evidence checks – secondary ID*

3499 **Ensure that the presented document meets the following conditions:**

- 3500 a) **If it is secondary Government Picture ID:**
3501 i) appears to be a genuine document properly issued by the claimed
3502 issuing authority and valid at the time of application;
3503 ii) bears a photographic image of the holder which matches that of the
3504 applicant;
3505 iii) states an address at which the applicant can be contacted.
3506 b) **If it is a financial institution account number, is verified by a record check**
3507 **with the specified issuing authority or through similar databases that:**
3508 i) establishes the existence of such records with matching name and
3509 reference numbers;
3510 ii) corroborates date (year, month and day) of birth, current address of
3511 record, and other personal information sufficient to ensure a unique
3512 identity.
3513 c) **If it is two utility bills or equivalent documents:**
3514 i) each appears to be a genuine document properly issued by the
3515 claimed issuing authority;
3516 ii) corroborates current address of record or telephone number sufficient to
3517 ensure a unique identity.

3518 *AL4_ID_IPV#050 Applicant knowledge checks*

3519 **Where the applicant is unable to satisfy any of the above requirements, that the**
3520 **applicant can provide a unique identifier, such as a Social Security Number (SSN),**
3521 **that matches the claimed identity.**

3522 **5.4.2.4 Remote Public Identity Proofing**

3523 **Not permitted.**

3524 **5.4.2.5 Current Relationship Identity Proofing**

3525 **Not permitted**

3526 **5.4.2.6 Affiliation Identity Proofing**

3527 A specific service that offers identity proofing to applicants on the basis of some form of
3528 affiliation must comply with the criteria in this section to establish that affiliation, in
3529 addition to complying with the previously stated requirements for verifying the
3530 individual's identity.

3531 The enterprise or specified service must:

3532 *AL4_ID_AJV#000 Meet preceding criteria*

3533 Meet all the criteria set out above, under §5.4.2.3, “[In-Person Public Identity](#)
3534 [Verification](#)”.

3535 *AL4_ID_AJV#010 Required evidence*

3536 Ensure that the applicant possesses:

- 3537 a) identification from the organization with which it is claiming affiliation;
3538 b) agreement from the organization that the applicant may be issued a credential
3539 indicating that an affiliation exists.

3540 *AL4_ID_AJV#020 Evidence checks*

3541 Have in place and apply processes which ensure that the presented documents:

- 3542 a) each appear to be a genuine document properly issued by the claimed issuing
3543 authorities and valid at the time of application;
3544 b) refer to an existing organization with a contact address;
3545 c) indicate that the applicant has some form of recognizable affiliation with the
3546 organization;
3547 d) appear to grant the applicant an entitlement to obtain a credential indicating an
3548 affiliation with the organization.

3549 **5.4.2.7 Issuing Derived Credentials**

3550 Where the Applicant already possesses recognized original credentials the CSP may
3551 choose to accept the verified identity of the Applicant as a substitute for identity proofing,
3552 subject to the following specific provisions. All other identity proofing requirements
3553 must also be observed.

3554 *AL4_ID_IDC#010 Authenticate Original Credential*

3555 Prior to issuing any derived credential the original credential on which the identity-
3556 proofing relies must be:

- 3557 a) authenticated by a source trusted by the CSP as being valid and un-revoked;
3558 b) issued at Assurance Level 4;
3559 c) issued in the same name as that which the Applicant is claiming;
3560 d) proven to be in the possession and under the control of the Applicant, **who shall**
3561 **be physically present.**

3562 **Guidance:** This is the equivalent of recording the details of identity-proofing documents
3563 provided during (e.g.) face-face id-proofing. It is not required that the original credential
3564 be issued by a Kantara-Approved CSP.

3565 *AL4_ID_IDC#020 Record Original Credential*

3566 Record the details of the original credential, **the biometric sample related to the**
3567 **original credential and the biometric sample captured when authenticating the**
3568 **Applicant.**

3569 *AL4_ID_IDC#030 Issue Derived Credential*

3570 **Only issue the derived credential in-person after performing biometric**
3571 **authentication of the Applicant .**

3572 **5.4.2.8 Secondary Identity Verification**

3573 In each of the above cases, the enterprise or specified service must also meet the
3574 following criteria:

3575 *AL4_ID_SCV#010 Secondary checks*

3576 Have in place additional measures (e.g., require additional documentary evidence, delay
3577 completion while out-of-band checks are undertaken) to deal with any anomalous
3578 circumstances that can reasonably be anticipated (e.g., a legitimate and recent change of
3579 address that has yet to be established as the address of record).

3580

3581 **5.4.2.9 Identity-proofing Records**

3582 The specific service must retain records of the identity proofing (verification) that it
3583 undertakes and provide them to qualifying parties when so required.

3584 The enterprise or specified service must:

3585 *AL4_ID_VRC#010 Verification Records for Personal Applicants*

3586 Log, taking account of all applicable legislative and policy obligations, a record of the
3587 facts of the verification process and the identity of the registrar (person, or entity if
3588 remote or automatic) performing the proofing functions, including a reference relating to
3589 the verification processes and the date and time of verification **issued by a trusted time-**
3590 **source**.

3591 **Guidance:** The facts of the verification process should include the specific record
3592 information (source, unique reference, value/content) used in establishing the applicant's
3593 identity, and will be determined by the specific processes used and documents accepted
3594 by the CSP. The CSP need not retain these records itself if it uses a third-party service
3595 which retains such records securely and to which the CSP has access when required, in
3596 which case it must retain a record of the identity of the third-party service providing the
3597 verification service or the location at which the (in-house) verification was performed.

3598 *AL4_ID_VRC#020 Verification Records for Affiliated Applicants*

3599 In addition to the foregoing, log, taking account of all applicable legislative and policy
3600 obligations, a record of the additional facts of the verification process [omitted].

3601 **Guidance:** Although there is no specific stipulation as to what should be recorded the
3602 list below suggests facts which would typically be captured at this level:

- 3603 a) the Subject's full name;
3604 b) the Subject's current address of record;
3605 c) the Subject's current telephone or email address of record;
3606 d) the Subscriber's authorization for issuing the Subject a credential;
3607 e) type, issuing authority, and reference number(s) of all documents checked in the
3608 identity proofing process;
3609 f) a biometric record of each required representative of the affiliating organization
3610 (e.g., a photograph, fingerprint, voice recording), as determined by that
3611 organization's governance rules/charter.

3612 *AL4_ID_VRC#025 Provide Subject identity records*

3613 If required, provide to qualifying parties records of identity proofing to the extent
3614 permitted by applicable legislation and/or agreed by the Subscriber.

3615 **Guidance:** the qualifier 'if required' is intended to account for circumstances where
3616 conditions such as whether a contract or a federation policy permits or is required or
3617 jurisdiction / legal injunction demand such provision. A qualifying party is any party to
3618 which provision of such info can justified according to circumstance: by contract/policy;

3619 with Subject's agreement; with due authority (Court Order, e.g.). The CSP needs to make
3620 the case, according to their service's characteristics and operating environment.

3621 *AL4_ID_VRC#030 Record Retention*

3622 Either retain, securely, the record of the verification/revocation process for the duration of
3623 the Subject account plus a further period sufficient to allow fulfillment of any period
3624 required legally, contractually or by any other form of binding agreement or obligation, or
3625 submit the record to a client CSP that has undertaken to retain the record for the requisite
3626 period or longer.

3627 *AL4_CM_IDP#010 Revision to Subscriber information*

3628 Provide a means for Subscribers and Subjects to securely amend their stored information
3629 after registration, either by re-proving their identity as in the initial registration process or
3630 by using their credentials to authenticate their revision. Successful revision must, where
3631 necessary, instigate the re-issuance of the credential.

3632 *AL4_CM_IDP#020 No stipulation*

3633 **5.4.2.10 Credential Creation**

3634 These criteria define the requirements for creation of credentials whose highest use is
3635 AL4.

3636 Note, however, that a token and credential created according to these criteria may not
3637 necessarily provide that level of assurance for the claimed identity of the Subject.
3638 Authentication can only be provided at the assurance level at which the identity is proven.

3639 An enterprise and its specified service must:

3640 *AL4_CM_CRN#010 Authenticated Request*

3641 Only accept a request to generate a credential and bind it to an identity if the source of the
3642 request, i.e., Registration Authority, can be authenticated as being authorized to perform
3643 identity proofing at AL4.

3644 *AL4_CM_CRN#020 Unique identity*

3645 Ensure that the identity which relates to a specific applicant is unique within the specified
3646 service, including identities previously used and that are now cancelled, other than its re-
3647 assignment to the same applicant.

3648 **Guidance:** This requirement is intended to prevent identities that may exist in a Relying
3649 Party's access control lists from possibly representing a different physical person.

3650 Cf. AL4_CM_POL#020 which expresses a very similar requirement. Although
3651 presenting repetition for a single provider, if the identity-proofing functions and
3652 credential management functions are provided by separate CSPs, each needs to fulfill this
3653 requirement.

3654 *AL4_CM_CRN#030 Credential uniqueness*

3655 Allow the Subject to select a credential (e.g., UserID) that is verified to be unique within
3656 the specified service's community and assigned uniquely to a single identity Subject.
3657 Default names shall not be permitted. {source [5415] KI.10.3.2.1#04}

3658 *AL4_CM_CRN#035 Convey credential*

3659 Be capable of conveying the unique identity information associated with a credential to
3660 Verifiers and Relying Parties.

3661 *AL4_CM_CRN#040 Token strength*

3662 Not use PIN/password tokens.

3663 *AL4_CM_CRN#050 One-time password strength*

3664 **Not use one-time password tokens.**

3665 *AL4_CM_CRN#055 No stipulation*

3666 *AL4_CM_CRN#060 Software cryptographic token strength*

3667 **Not use software cryptographic tokens.**

3668 *AL4_CM_CRN#070 One-time password hardware token strength*

3669 Ensure that hardware tokens used to store cryptographic keys:

- 3670 a) employ a cryptographic module that is validated against [IS19790] Level 2 or
3671 higher, or equivalent, as determined by a recognized national technical authority;
3672 b) require password or biometric activation by the Subject [omitted];

3673 c) **Generate a one-time password using an algorithm recognized by a national
3674 technical authority;**

3675 d) are locked prior to their delivery, once personalization processes have been
3676 completed. {source [5415] KI.10.2.2.1#07}

3677 *AL4_CM_CRN#075 Multi-factor hardware cryptographic token strength*

3678 **Ensure that hardware tokens used to store cryptographic keys:**

3679 a) **employ a cryptographic module that is validated against [IS19790] Level 2 or
3680 higher, or equivalent, as determined by a recognized national technical
3681 authority;**

3682 b) **are validated against [IS19790] Level 3 or higher, or equivalent, as
3683 determined by a recognized national technical authority, for their physical
3684 security;**

3685 c) **require password, PIN or biometric activation by the Subject when being
3686 used for authentication;**

3687 d) **do not permit the export of authentication keys;**

3688 e) **are locked prior to their delivery, once personalization processes have been
3689 completed.** {source [5415] KI.10.2.2.1#07}

3690 *AL4_CM_CRN#080 Binding of key*

3691 If the specified service generates the Subject's key pair, that the key generation process
3692 securely and uniquely binds that process to the certificate generation and maintains at all
3693 times the secrecy of the private key, until it is accepted by the Subject.

3694 *AL4_CM_CRN#085 Hardware Inventory Control*

3695 Prior to issuance, if a credential, or the means to produce credentials, is held on a
3696 hardware device, the hardware device shall be kept physically secure and the inventory
3697 tracked. {source [5415] KI.10.2.2.1#08}

3698 *AL4_CM_CRN#090 Nature of Subject*

3699 Record the nature of the Subject of the credential **[omitted]**, i.e., private person, a named
3700 person acting on behalf of a corporation or other legal entity, corporation or legal entity,
3701 or corporate machine entity, in a manner that can be unequivocally associated with the
3702 credential and the identity that it asserts.

3703 *AL4_CM_CRN#095 No stipulation*

3704 No stipulation

3705 **5.4.2.11 Subject Key Pair Generation**

3706 An enterprise and its specified service must:

3707 *AL4_CM_SKP#010 Key generation by Specified Service*

3708 If the specified service generates the Subject's keys:

- 3709 a) use an **[IS19790]** compliant algorithm, or equivalent, as established by a
3710 recognized national technical authority, that is recognized as being fit for the
3711 purposes of the service;
- 3712 b) only create keys of a key length and for use with an **[IS19790]** compliant public
3713 key algorithm, or equivalent, as established by a recognized national technical
3714 authority, recognized as being fit for the purposes of the service;
- 3715 c) generate and store the keys securely until delivery to and acceptance by the
3716 Subject;
- 3717 d) deliver the Subject's private key in a manner that ensures that the privacy of the
3718 key is not compromised and only the Subject has access to the private key.

3719 *AL4_CM_SKP#020 Key generation by Subject*

3720 If the Subject generates and presents its own keys, obtain the Subject's written
3721 confirmation that it has:

- 3722 a) used an **[IS19790]** compliant algorithm, or equivalent, as established by a
3723 recognized national technical authority, that is recognized as being fit for the
3724 purposes of the service;
- 3725 b) created keys of a key length and for use with an **[IS19790]** compliant public key
3726 algorithm, or equivalent, as established by a recognized national technical
3727 authority, recognized as being fit for the purposes of the service.

3728 **5.4.2.12 Credential Delivery**

3729 An enterprise and its specified service must:

3730 *AL4_CM_CRD#010 Notify Subject of Credential Issuance*

3731 Notify the Subject of the credential's issuance and, if necessary, confirm Subject's contact
3732 information by:

- 3733 a) sending notice to the address of record confirmed during identity proofing;
3734 b) **unless the Subject presented with a private key, issuing the hardware token**
3735 **to the Subject in a manner that confirms the address of record supplied by**
3736 **the applicant during identity proofing;**
3737 c) **issuing the certificate to the Subject over a separate channel in a manner that**
3738 **confirms either the address of record or the email address supplied by the**
3739 **applicant during identity proofing.**

3740 **Guidance:** The nature of issuance could mean that the Subject is fully aware and
3741 therefore no notification is necessary. If any other such circumstances prevailed, the CSP
3742 should identify them.

3743 *AL4_CM_CRD#015 Confirm Applicant's identity (in person)*

3744 Prior to delivering the credential, require the Applicant to identify themselves in person in
3745 any new transaction (beyond the first transaction or encounter) **[deleted]** through the use
3746 of a biometric that was recorded during **the first** encounter.

3747 *AL4_CM_CRD#016 No stipulation*

3748 **No stipulation.**

3749 *AL4_CM_CRD#017 Protected Issuance of Permanent Secrets (in person)*

3750 Only issue permanent secrets if the CSP has loaded the secret itself onto the physical
3751 device, which was either:

- 3752 a) issued in-person to the Applicant, or;
3753 b) delivered in a manner that confirms the address of record.

3754 *AL4_CM_CRD#018 No stipulation*

3755 **No stipulation.**

3756 *AL4_CM_CRD#020 Subject's acknowledgement*

3757 Receive acknowledgement of receipt of the **hardware token** before it is activated and **the**
3758 **corresponding certificate and** its directory status record are published (and thereby the
3759 subscription becomes active or re-activated, depending upon the circumstances of issue).

3760 *AL4_CM_CRD#030 Activation window*

3761 **Require activation of the credential within a time period specified in the Certificate**
3762 **Policy.** {source [5415] KI.10.2.2.1#17}

3763 **5.4.3 Part C - Credential Renewal and Re-issuing**

3764 These criteria apply to the renewal and re-issuing of credentials. They address
3765 requirements levied by the use of various technologies to achieve Assurance Level 4.

3766 **5.4.3.1 Renewal/Re-issuance Procedures**

3767 These criteria address general renewal and re-issuance functions, to be exercised as
3768 specific controls in these circumstances while continuing to observe the general
3769 requirements established for initial credential issuance.

3770 An enterprise and its specified service must:

3771 *AL4_CM_RNR#010 Changeable PIN/Password*

3772 Permit Subjects to change the passwords used to activate their credentials.

3773 *AL4_CM_RNR#020 Proof-of-possession on Renewal/Re-issuance*

3774 Subjects wishing to change their passwords must demonstrate that they are in possession
3775 of the unexpired current token prior to the CSP proceeding to renew or re-issue it.

3776 *AL4_CM_RNR#030 Renewal/Re-issuance limitations*

3777 a) No stipulation;

3778 b) **neither renew nor re-issue expired tokens;**

3779 c) No stipulation;

3780 d) **cryptographically authenticate all sensitive renewal / re-issuance interactions**
3781 **with the Subject using keys bound to the authentication process.**

3782 **Guidance:** Renewal is considered as an extension of usability, whereas re-issuance
3783 requires a change.

3784 *AL4_CM_RNR#040 Authentication key life*

3785 **Expire after 24 hours all temporary or short-term keys derived during the**
3786 **authentication process.**

3787 *AL4_CM_RNR#050 Record Retention*

3788 Retain, securely, the record of any renewal/re-issuance process for the duration of the
3789 Subscriber's account plus a further period sufficient to allow fulfillment of any period
3790 required legally, contractually or by any other form of binding agreement or obligation, or
3791 submit same record to a client CSP that has undertaken to retain the record for the
3792 requisite period or longer.

3793 **5.4.4 Part D - Credential Revocation**

3794 These criteria deal with credential revocation and the determination of the legitimacy of a
3795 revocation request.

3796 **5.4.4.1 Revocation Procedures**

3797 These criteria address general revocation functions, such as the processes involved and
3798 the basic requirements for publication.

3799 An enterprise and its specified service must:

3800 *AL4_CM_RVP#010 Revocation procedures*

3801 a) State the conditions under which revocation of an issued certificate may occur;

3802 b) State the processes by which a revocation request may be submitted;

3803 c) State the persons and organizations from which a revocation request will be
3804 accepted;

3805 d) State the validation steps that will be applied to ensure the validity (identity) of
3806 the Revocant, and;

3807 e) State the response time between a revocation request being accepted and the
3808 publication of revised certificate status.

3809 *AL4_CM_RVP#020 Secure status notification*

3810 Ensure that published credential status notification information can be relied upon in
3811 terms of the enterprise of its origin (i.e., its authenticity) and its correctness (i.e., its
3812 integrity).

3813 *AL4_CM_RVP#030 Revocation publication*

3814 Ensure that published credential status notification is revised within **18** hours of the
3815 receipt of a valid revocation request, such that any subsequent attempts to use that
3816 credential in an authentication shall be unsuccessful. The nature of the revocation
3817 mechanism shall be in accordance with the technologies supported by the service.

3818 *AL4_CM_RVP#045 No stipulation*

3819 *AL4_CM_RVP#040 Verify Revocation Identity*

3820 Establish that the identity for which a revocation request is received is one that was
3821 issued by the specified service.

3822 *AL4_CM_RVP#050 Revocation Records*

3823 Retain a record of any revocation of a credential that is related to a specific identity
3824 previously verified, solely in connection to the stated credential. At a minimum, records
3825 of revocation must include:

3826 a) the Revocant's full name;

3827 b) the Revocant's authority to revoke (e.g., Subscriber or Subject themselves,
3828 someone acting with the Subscriber's or Subject's power of attorney, the
3829 credential issuer, law enforcement, or other legal due process);

3830 c) the Credential Issuer's identity (if not directly responsible for the identity
3831 proofing service);

3832 d) No stipulation;

3833 e) the reason for revocation.

3834 *AL4_CM_RVP#060 Record Retention*

3835 Retain, securely, the record of the revocation process for a period which is the maximum
3836 of:

3837 a) the records retention policy required by **AL4_CM_CPP#020**;

3838 b) applicable legislation, regulation, contract or standards.

3839 **5.4.4.2 Verify Revocant's Identity**

3840 Revocation of a credential requires that the requestor and the nature of the request be
3841 verified as rigorously as the original identity proofing. The enterprise should not act on a
3842 request for revocation without first establishing the validity of the request (if it does not,
3843 itself, determine the need for revocation).

3844 In order to do so, the enterprise and its specified service must:

3845 *AL4_CM_RVR#010 Verify revocation identity*

3846 Establish that the credential for which a revocation request is received is one that was
3847 initially issued by the specified service, applying the same process and criteria as would
3848 apply to an original identity proofing.

3849 *AL4_CM_RVR#020 Revocation reason*

3850 Establish the reason for the revocation request as being sound and well founded, in
3851 combination with verification of the Revocant, according to *AL4_CM_RVR#030*,
3852 *AL4_CM_RVR#040*, or *AL4_CM_RVR#050*.

3853 *AL4_CM_RVR#030 Verify Subscriber as Revocant*

3854 Where the Subscriber or Subject seeks revocation of the Subject's credential:

3855 a) if in person, require presentation of a primary Government Picture ID document
3856 that shall be **[Omitted]** verified by a record check against the provided identity
3857 with the specified issuing authority's records;

3858 b) if remote:

3859 i. verify a signature against records (if available), confirmed with a call to a
3860 telephone number of record, or;

3861 ii. as an electronic request, authenticate it as being from the same Subscriber
3862 or Subject, supported by a **different** credential at **Assurance Level 4**.

3863 *AL4_CM_RVR#040 Verify CSP as Revocant*

3864 Where a CSP seeks revocation of a Subject's credential, establish that the request is
3865 either:

3866 a) from the specified service itself, with authorization as determined by established
3867 procedures, or;

3868 b) from the client Credential Issuer, by authentication of a formalized request over
3869 the established secure communications network.

3870 *AL4_CM_RVR#050 Verify Legal Representative as Revocant*

3871 Where the request for revocation is made by a law enforcement officer or presentation of
3872 a legal document:

- 3873 a) if in-person, verify the identity of the person presenting the request, or;
- 3874 b) if remote:
 - 3875 i. in paper/facsimile form, verify the origin of the legal document by a
 - 3876 database check or by telephone with the issuing authority;
 - 3877 ii. as an electronic request, authenticate it as being from a recognized legal
 - 3878 office, supported by a different credential at **Assurance Level 4**.

3879 **5.4.4.3 Re-keying a credential**

3880 Re-keying of a credential requires that the requestor be verified as the Subject with as
3881 much rigor as was applied to the original identity proofing. The enterprise should not act
3882 on a request for re-key without first establishing that the requestor is identical to the
3883 Subject.

3884 In order to do so, the enterprise and its specified service must:

3885 *AL4_CM_RKY#010 Verify Requestor as Subscriber*

3886 **Where the Subject seeks a re-key for the Subject's own credential:**

- 3887 a) **if in-person, require presentation of a primary Government Picture ID**
- 3888 **document that shall be verified by a record check against the provided**
- 3889 **identity with the specified issuing authority's records;**
- 3890 b) **if remote:**
 - 3891 i. **verify a signature against records (if available), confirmed with a call**
 - 3892 **to a telephone number of record, or;**
 - 3893 ii. **authenticate an electronic request as being from the same Subject,**
 - 3894 **supported by a different credential at Assurance Level 4.**

3895 *AL4_CM_RKY#020 Re-key requests other than Subject*

3896 **Re-key requests from any parties other than the Subject must not be accepted.**

3897 **5.4.4.4 Secure Revocation/Re-key Request**

3898 This criterion applies when revocation **or re-key** requests must be communicated
3899 between remote components of the service organization.

3900 The enterprise and its specified service must:

3901 *AL4_CM_SRR#010 Submit Request*

3902 Submit a request for the revocation to the Credential Issuer service (function), using a
3903 secured network communication.

3904 **5.4.5 Part E - Credential Status Management**

3905 These criteria deal with credential status management, such as the receipt of requests for
3906 new status information arising from a new credential being issued or a revocation or other
3907 change to the credential that requires notification. They also deal with the provision of
3908 status information to requesting parties (Verifiers, Relying Parties, courts and others
3909 having regulatory authority, etc.) having the right to access such information.

3910 **5.4.5.1 Status Maintenance**

3911 An enterprise and its specified service must:

3912 *AL4_CM_CSM#010 Maintain Status Record*

3913 Maintain a record of the status of all credentials issued.

3914 *AL4_CM_CSM#020 Validation of Status Change Requests*

3915 Authenticate all requestors seeking to have a change of status recorded and published and
3916 validate the requested change before considering processing the request. Such validation
3917 should include:

3918 a) the requesting source as one from which the specified service expects to receive
3919 such requests;

3920 b) if the request is not for a new status, the credential or identity as being one for
3921 which a status is already held.

3922 *AL4_CM_CSM#030 Revision to Published Status*

3923 Process authenticated requests for revised status information and have the revised
3924 information available for access within a period of 72 hours.

3925 *AL4_CM_CSM#040 Status Information Availability*

3926 Provide, with 99% availability, a secure automated mechanism to allow relying parties to
3927 determine credential status and authenticate the Claimant's identity.

3928 *AL4_CM_CSM#050 Inactive Credentials*

3929 Disable any credential that has not been successfully used for authentication during a
3930 period of 18 months.

3931

3932 **5.4.6 Part F - Credential Verification/Authentication**

3933 These criteria apply to credential validation and identity authentication.

3934 **5.4.6.1 Assertion Security**

3935 An enterprise and its specified service must:

3936 *AL4_CM_ASS#010 Validation and Assertion Security*

3937 Provide validation of credentials to a Relying Party using a protocol that:

- 3938 a) requires authentication of the specified service, itself, or of the validation source;
- 3939 b) ensures the integrity of the authentication assertion;
- 3940 c) protects assertions against manufacture, modification, substitution and disclosure,
- 3941 and secondary authenticators from manufacture, capture and replay;
- 3942 d) uses approved **strong** cryptography techniques;

3943 and which, specifically:

- 3944 e) creates assertions which are specific to a single transaction;
- 3945 f) where assertion references are used, generates a new reference whenever a new
- 3946 assertion is created;
- 3947 g) when an assertion is provided indirectly, either signs the assertion or sends it via a
- 3948 protected channel, using a strong binding mechanism between the secondary
- 3949 authenticator and the referenced assertion;
- 3950 h) send assertions either via a channel mutually-authenticated with the Relying
- 3951 Party, or signed and encrypted for the Relying Party;
- 3952 i) requires the secondary authenticator to:
 - 3953 i) be signed when provided directly to Relying Party, or;
 - 3954 ii) have a minimum of 64 bits of entropy when provision is indirect (i.e.
 - 3955 through the credential user);
 - 3956 iii) be transmitted to the Subject through a protected channel which is linked
 - 3957 to the primary authentication process in such a way that session hijacking
 - 3958 attacks are resisted;
 - 3959 iv) not be subsequently transmitted over an unprotected channel or to an
 - 3960 unauthenticated party while it remains valid.

3961 *AL4_CM_ASS#015 No False Authentication*

3962 Employ techniques which ensure that system failures do not result in ‘false positive

3963 authentication’ errors.

3964 *AL4_CM_ASS#018 Ensure token validity*

3965 Ensure that tokens are either still valid or have been issued within the last 24 hours.

3966 **Guidance:** The 24-hour period allows for the fact that if a freshly-issued credential is

3967 then revoked, notice of the revocation may take 24 hours to be publicised (per

3968 AL3_CM_RVP#030)..

3969 *AL4_CM_ASS#020 Post Authentication*

3970 *Not* authenticate credentials that have been revoked unless the time of the transaction for

3971 which verification is sought precedes the time of revocation of the credential.

3972 **Guidance:** The purpose in this criterion is that, if a verification is intended to refer to the

3973 status of a credential at a specific historical point in time, e.g. to determine whether the

3974 Claimant was entitled to act as a signatory in a specific capacity at the time of the

3975 transaction, this may be done. It is implicit in this thinking that both the request and the
3976 response indicate the historical nature of the query and response; otherwise the default
3977 time is ‘now’. If no such service is offered then this criterion may simply be
3978 ‘Inapplicable’, for that reason.

3979 *AL4_CM_ASS#030 Proof of Possession*

3980 Use an authentication protocol that requires the claimant to prove possession and control
3981 of the authentication token.

3982 *AL4_CM_ASS#035 No stipulation*

3983 *AL4_CM_ASS#040 Assertion Life-time*

3984 **[Omitted]** Notify the relying party of how often the revocation status sources are
3985 updated.

3986 **5.4.6.2 Authenticator-generated challenges**

3987 An enterprise and its specified service must:

3988 *AL4_CM_AGC#010 Entropy level*

3989 Create authentication secrets to be used during the authentication exchange (i.e. with out-
3990 of-band or cryptographic device tokens) with a degree of entropy appropriate to the token
3991 type in question.

3992 *AL4_CM_AGC#020 Limit password validity*

3993 **Employ one-time passwords which expire within two minutes.**

3994 **5.4.6.3 Multi-factor authentication**

3995 An enterprise and its specified service must:

3996 *AL4_CM_MFA#010 Permitted multi-factor tokens*

3997 Require two tokens which, when used in combination within a single authentication
3998 exchange, are acknowledged as providing an equivalence of AL4, as determined by a
3999 recognized national technical authority.

4000 **5.4.6.4 Verifier’s assertion schema**

4001 Note: Since assertions and related schema can be complex and may be modeled directly
4002 on the needs and preferences of the participants, the details of such schema fall outside
4003 the scope of the SAC’s herein, which are expressed observing, insofar as is feasible, a
4004 technology-agnostic policy. The following criteria, therefore, are perhaps more open to
4005 variable conformity through their final implementation than are others in this document.

4006 These criteria are derived directly from NIST SP 800-63-2 and have been expressed in as
4007 generic a manner as they can be.

- 4008 An enterprise and its specified service must:
- 4009 *AL4_CM_VAS#010 Approved cryptography*
- 4010 Apply assertion protocols which use cryptographic techniques approved by a national
4011 authority or other generally-recognized authoritative body.
- 4012 *AL4_CM_VAS#020 No browser/bearer assertions*
- 4013 **Not issue browser / bearer assertions.**
- 4014 *AL4_CM_VAS#030 Assertion assurance level*
- 4015 Create assertions which, either explicitly or implicitly (using a mutually-agreed
4016 mechanism), indicate the assurance level at which the initial authentication of the Subject
4017 was made.
- 4018 *AL4_CM_VAS#040 No pseudonyms*
- 4019 Create assertions which indicate only verified Subscriber names in the credential subject
4020 to verification.
- 4021 *AL4_CM_VAS#050 Specify recipient*
- 4022 Create assertions which identify the intended recipient of the verification such that the
4023 recipient may validate that it is intended for them.
- 4024 *AL4_CM_VAS#060 No assertion manufacture/modification*
- 4025 Ensure that it is impractical to manufacture an assertion or assertion reference by Signing
4026 the assertion and using at least one of the following techniques:
- 4027 a) [Omitted];
- 4028 b) Encrypting the assertion using a secret key shared with the RP;
- 4029 c) Creating an assertion reference which has a minimum of 64 bits of entropy;
- 4030 d) Sending the assertion over a protected channel during a mutually-authenticated
4031 session.
- 4032 *AL4_CM_VAS#070 Assertion protections*
- 4033 Provide protection of assertion-related data such that:
- 4034 a) both assertions and assertion references are protected against capture and re-use;
- 4035 b) assertions are also protected against redirection
- 4036 c) assertions, assertion references and session cookies used for authentication
4037 purposes, including any which are re-directed, are protected against session
4038 hijacking, for at least the duration of their validity (see AL1_CM_VAS#110).
- 4039 *AL4_CM_VAS#080 Single-use assertions*
- 4040 Limit to a single transaction the use of assertions which do not support proof of
4041 ownership.

- 4042 *AL4_CM_VAS#090 Single-use assertion references*
4043 Limit to a single transaction the use of assertion references.
- 4044 *AL4_CM_VAS#100 Bind reference to assertion*
4045 Provide a strong binding between the assertion reference and the corresponding assertion,
4046 based on integrity-protected (or signed) communications over which the Verifier has been
4047 authenticated.
- 4048 *AL4_CM_VAS#110 No stipulation*
4049 No stipulation.

4050

4051 **6 REFERENCES**

4052

4053 [CAF] Louden, Chris, Spencer, Judy; Burr, Bill; Hawkins, Kevin; Temoshok, David;
4054 Cornell, John; Wilsher, Richard G.; Timchak, Steve; Sill, Stephen; Silver, Dave; Harrison,
4055 Von; eds., "E-Authentication Credential Assessment Framework (CAF)," E-
4056 Authentication Initiative, Version 2.0.0 (March 16, 2005).
4057 <http://www.cio.gov/eauthentication/documents/CAF.pdf>

4058

4059 [EAP CSAC 04011] "EAP working paper: Identity Proofing Service Assessment Criteria
4060 (ID-SAC)," Electronic Authentication Partnership, Draft 0.1.3 (July 20, 2004)
4061 http://eap.projectliberty.org/docs/Jul2004/EAP_CSAC_04011_0-1-3_ID-SAC.doc

4062

4063 [EAPTrustFramework] "Electronic Authentication Partnership Trust Framework"
4064 Electronic Authentication Partnership, Version 1.0. (January 6, 2005)
4065 http://eap.projectliberty.org/docs/Trust_Framework_010605_final.pdf

4066

4067 [FIPS140-2] "Security Requirements for Cryptographic Modules" Federal Information
4068 Processing Standards. (May 25, 2001) [http://csrc.nist.gov/publications/fips/fips140-](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)
4069 [2/fips1402.pdf](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)

4070

4071 [IS27001] ISO/IEC 27001:2013 "Information technology - Security techniques -
4072 Requirements for information security management systems", International Organization
4073 for Standardization.
4074 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

4075

4076 [IS19790] ISO/IEC 19790:2012 "Information technology - Security techniques -
4077 Security requirements for cryptographic modules", International Organization for
4078 Standardization.
4079 http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=52906

4080

4081 [M-04-04] Bolton, Joshua B., ed., "E-Authentication Guidance for Federal Agencies",
4082 Office of Management and Budget, (December 16, 2003).
4083 <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>

4084

4085 [NIST800-63] Burr, William E.; Dodson, Donna F.; Polk, W. Timothy; eds., "Electronic
4086 Authentication Guideline: : Recommendations of the National Institute of Standards and
4087 Technology," Version 1.0.2, National Institute of Standards and Technology, (April,
4088 2006). http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

4089

4090 [RFC 3647] Chokhani, S.; Ford, W.; Sabett, R.; Merrill, C.; Wu, S.; eds., "Internet X.509
4091 Public Key Infrastructure Certificate Policy and Certification Practices Framework," The
4092 Internet Engineering Task Force (November, 2003). <http://www.ietf.org/rfc/rfc3647.txt>

4093

4094 [5415] Ed. Wilsher, Richard G. "SAC mapping – ISO/IEC 29115 / ITU-T X.1254 –
4095 Entity authentication assurance framework" v0.7.0.

4096

4097 **7 REVISION HISTORY**

- 4098 2008-05-08 – Identity Assurance Framework Version 1.0 Initial Draft
- 4099 a. Released by Liberty Alliance
- 4100 b. Revision and scoping of Initial Draft release
- 4101 2008-06-23 – Identity Assurance Framework Version 1.1 Final Draft
- 4102 Released by Liberty Alliance
- 4103 Inclusion of comments to Final Draft
- 4104 2009-10-01 – Identity Assurance Framework Version 1.1 Final Draft
- 4105 Documents contributed to Kantara Initiative, Inc. by Liberty Alliance
- 4106 2010-04-dd – SAC Version 2.0
- 4107 Released by Kantara Initiative, Inc.
- 4108 Significant scope build
- 4109 Original Identity Assurance Framework all inclusive document broken in to a
- 4110 set of documents with specific focus:
- 4111 Kantara IAF-1000-Overview
- 4112 Kantara IAF-1100-Glossary
- 4113 Kantara IAF-1200-Levels of Assurance
- 4114 Kantara IAF-1300-Assurance Assessment Scheme
- 4115 Kantara IAF-1400-Service Assessment Criteria (this document)
- 4116 Kantara IAF-1600-Assessor Qualifications and Requirements
- 4117 2012-10-10 - SAC Version 3.0
- 4118 Revision to accommodate Full/Component Service Assessment and Approval.
- 4119 2014-05-14 – SAC Version 4.0
- 4120 Revision to map SAC against NIST SP 800-63-2;
- 4121 Alignment to revised Glossary.
- 4122 2016-09-08 – SAC Version 5.0
- 4123 General refinements having no significant load upon implementers or
- 4124 assessors;
- 4125 Revision to existing and introduction of new criteria as a consequence of
- 4126 mapping to ISO/IEC 29115:2013 (see [5415]).
- 4127