

1

2



3

4

5 **Identity Assurance Framework -** 6 **Service Assessment Criteria**

7 **Version:** 2.0 draft 0.4, 2009-05-18

8 **Editor:**

9 Richard G. Wilsher, Zyigma LLC

10 **Contributors:**

11 See the extensive contributors list in Section 5.

12

13 **Abstract:**

14 The Liberty Alliance Identity Assurance Expert Group (IAEG) was formed to foster
15 adoption of identity trust services. Utilizing initial contributions from the
16 e-Authentication Partnership (EAP) and the US E-Authentication Federation, the IAEG's
17 objective is to create a framework of baseline policies, business rules, and commercial
18 terms against which identity trust services can be assessed and evaluated. The goal is to
19 facilitate trusted identity federation to promote uniformity and interoperability amongst
20 identity service providers. The primary deliverable of IAEG is the Identity Assurance
21 Framework (IAF).

22

23 **Filename:**pdf

24

25 **Notice:**

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

32 Implementation or use of certain elements of this document may require licenses under
33 third party intellectual property rights, including without limitation, patent rights. The
34 Sponsors of and any other contributors to the Specification are not and shall not be held
35 responsible in any manner for identifying or failing to identify any or all such third party
36 intellectual property rights. **This Specification is provided "AS IS," and no**
37 **participant in the Liberty Alliance Project makes any warranty of any kind, express**
38 **or implied, including any implied warranties of merchantability, non-infringement**
39 **of third party intellectual property rights, and fitness for a particular purpose.**

40 Implementers of this Specification are advised to review the Liberty Alliance Project's
41 website (<http://www.projectliberty.org/>) for information concerning any Necessary
42 Claims Disclosure Notices that have been received by the Liberty Alliance Management
43 Board.

44 Copyright © 2007-2009 ActivIdentity, Trent Adams, Adetti, Adobe Systems, AOL,
45 BEA Systems, Berne, University of Applied Sciences, Gerald Beuchelt, BIPAC, John
46 Bradley, British Telecommunications plc, Hellmuth Broda, Bronnoysund Register
47 Centre, BUPA, CA, Canada Post Corporation, Center for Democracy and Technology,
48 Chief, Information Office Austria, China Internet Network Information Center (CNNIC),
49 ChoicePoint, Citi, City University, Clareity Security, Dan Combs, Computer &
50 Communications Industry Association, Courion Corporation, Danish Biometrics
51 Research Proj. Consortium, Danish National IT and Telecom Agency, Deny All,
52 Deutsche Telekom AG, DGME, Brian Dilley, Diversinet Corp., Drummond Group Inc.,
53 East of England Telematics Development Trust Ltd, EIfEL, Electronics and
54 Telecommunications Research Institute (ETRI), Engineering Partnership in Lancashire,
55 Enterprise Java Victoria Inc., Entr'ouvert, Ericsson, Evidian, Fidelity Investments,
56 Financial Services Technology Consortium (FSTC), Finland National Board of Taxes,
57 Fischer International, France Telecom, Fraunhofer-Gesellschaft, Fraunhofer Institute for
58 Integrated Circuits IIS, Fraunhofer Institute for Secure Information Technology (SIT),
59 Fraunhofer Institut for Experimentelles Software Engineering, Fugen Solutions, Fujitsu
60 Services Oy, Fun Communications GmbH, Gemalto, Giesecke & Devrient GMBH,
61 Global Platform, GSA Office of Governmentwide Policy, Healthcare Financial
62 Management Association (HFMA), Health Information and Management Systems
63 Society (HIMSS), Helsinki Institute of Physics, Jeff Hodges, Hongkong Post, Guy
64 Huntington, Imprivata, Information Card Foundation, Institute of Bioorganic Chemistry
65 Poland, Institute of Information Management of the University, Institut Experimentelles

66 Software Engineering (IESE), Intel Corporation, International Institute of
67 Telecommunications, International Security, Trust and Privacy Alliance, Internet2,
68 Interoperability Clearinghouse (ICH), ISOC, Java Wireless Competency Centre (JWCC),
69 Kantega AS, Kuppinger Cole & Partner, Kuratorium OFFIS e.V., Colin Mallett, Rob
70 Marano, McMaster University, MEDNETWorld.com, Methics Oy, Mortgage Bankers
71 Association (MBA), Mydex, National Institute for Urban Search & Rescue Inc NEC
72 Corporation, Network Applications Consortium (NAC), Neustar, Newspaper Association
73 of America, New Zealand Government State Services Commission, NHK (Japan
74 Broadcasting Corporation) Science & Technical Research Laboratories, Nippon
75 Telegraph and Telephone Company, Nokia Corporation, Nortel, NorthID Oy, Norwegian
76 Agency for Public Management and eGovernment, Norwegian Public Roads
77 Administration, Novell, NRI Pacific, Office of the Information Privacy Commissioner of
78 Ontario, Omnibranch, OpenIAM, Oracle USA, Inc., Organisation Internationale pour la
79 Sécurité des Transactions Électroniques (OISTE), Oslo University, Our New Evolution,
80 PAM Forum, Parity Communications, Inc., PayPal, Phase2 Technology, Ping Identity
81 Corporation, Bob Pinheiro, Platinum Solutions, Postsecondary Electronic Standards
82 Council (PESC), Purdue University, RSA Security, Mary Ruddy, SAFE Bio Pharma,
83 SanDisk Corporation, Shidler Center for Law, Andrew Shikiar, Signicat AS, Singapore
84 Institute of Manufacturing Technology, Software & Information Industry Association,
85 Software Innovation ASA, Sprint Nextel Corporation, Studio Notarile Genghini-SNG,
86 Sunderland City Council, SUNET, Sun Microsystems, SwissSign AG, Technische
87 Universitat Berlin, Telefonica S.A., TeleTrusT, TeliaSonera Mobile Networks AB,
88 TERENA, Thales e-Security, The Boeing Company, The Financial Services
89 Roundtable/BITS, The Open Group, The University of Chicago as Operator of Argonne
90 National Laboratory, TRUSTe, *tScheme* Limited, UNINETT AS, Universidad Politecnica
91 de Madrid, University of Birmingham, University of Kent, University of North Carolina
92 at Charlotte, University of Ottawa (TTBE), U.S. Department of Defense, VeriSign,
93 Vodafone Group Plc, Web Services Competence Center (WSCC), Zenn New Media

94

95

96 All rights reserved.

97

98

99 **Contents**

100

101 **1 Introduction5**

102 **2 Assurance Levels6**

103 2.1 Assurance Level Policy Overview6

104 2.2 Description of the Four Assurance Levels7

105 2.2.1 Assurance Level 18

106 2.2.2 Assurance Level 28

107 2.2.3 Assurance Level 38

108 2.2.4 Assurance Level 48

109 **3 Service Assessment Criteria10**

110 3.1 Context and Scope10

111 3.2 Readership10

112 3.3 Criteria Descriptions11

113 3.4 Terminology12

114 3.5 Common Organizational Service Assessment Criteria13

115 3.5.1 Assurance Level 113

116 3.5.2 Assurance Level 216

117 3.5.3 Assurance Level 326

118 3.5.4 Assurance Level 436

119 3.6 Identity Proofing Service Assessment Criteria53

120 3.6.1 Assurance Level 153

121 3.6.2 Assurance Level 255

122 3.6.3 Assurance Level 361

123 3.6.4 Assurance Level 467

124 3.6.5 Compliance Tables72

125 3.7 Credential Management Service Assessment Criteria76

126 3.7.1 Part A - Credential Operating Environment76

127 3.7.2 Part B - Credential Issuing89

128 3.7.3 Part C - Credential Renewal and Re-issuing103

129 3.7.4 Part D - Credential Revocation106

130 3.7.5 Part E - Credential Status Management117

131 3.7.6 Part F - Credential Validation/Authentication121

132 3.7.7 Compliance Tables127

133 **4 IAEG Glossary135**

134 **5 Publication Acknowledgements141**

135 **6 References145**

136

137

138 **1 Introduction**

139 Liberty Alliance Project formed the Identity Assurance Expert Group (IAEG) to foster
140 adoption of consistently managed identity trust services. Utilizing initial contributions
141 from the e-Authentication Partnership (EAP) and the US E-Authentication Federation,
142 the IAEG's objective is to create a framework of baseline policies requirements (criteria)
143 and rules against which identity trust services can be assessed and evaluated. The goal is
144 to facilitate trusted identity federation and to promote uniformity and interoperability
145 amongst identity service providers, with a specific focus on the level of trust, or
146 assurance, associated with identity assertions. The primary deliverable of IAEG is the
147 Identity Assurance Framework (IAF).

148 The IAF leverages the EAP Trust Framework [[EAPTrustFramework](#)] and the US
149 E-Authentication Federation Credential Assessment Framework ([[CAF](#)]) as baselines in
150 forming the criteria for a harmonized, best-of-breed, industry-recognized identity
151 assurance standard. The IAF is a framework supporting mutual acceptance, validation,
152 and life cycle maintenance across identity federations. The IAF is described in an
153 [Overview](#) publication which also includes the IAF Glossary. The present document
154 describes the Service Assessment Criteria component of the IAF, including setting-out the
155 Assurance Levels.

156 Assurance Levels (ALs) are the levels of trust associated with a credential as measured by
157 the associated technology, processes, and policy and practice statements controlling the
158 operational environment. The IAF defers to the guidance provided by the U.S. National
159 Institute of Standards and Technology (NIST) Special Publication 800-63 version 1.0.1
160 [[NIST800-63](#)] which outlines four (4) levels of assurance, ranging in confidence level
161 from low to very high. Use of ALs is determined by the level of confidence or trust (i.e.
162 assurance) necessary to mitigate risk in the transaction.

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

170 2 Assurance Levels

171 2.1 Assurance Level Policy Overview

172 An Assurance Level (AL) describes the degree to which a relying party in an electronic
173 business transaction can be confident that the identity information being presented by a
174 CSP actually represents the entity named in it and that it is the represented entity who is
175 actually engaging in the electronic transaction. ALs are based on two factors:

- 176 1. The extent to which the identity presented by a CSP in an identity assertion can be
177 trusted to actually belong to the entity represented. This factor is generally
178 established through the identity proofing process and identity information
179 management practices.
- 180 2. The extent to which the electronic credential presented to a CSP by an individual
181 can be trusted to be a proxy for the entity named in it and not someone else (known
182 as identity binding). This factor is directly related to the integrity and reliability of
183 the technology associated with the credential itself, the processes by which the
184 credential and its verification token are issued, managed, and verified, and the
185 system and security measures followed by the credential service provider
186 responsible for this service.

187 Managing risk in electronic transactions requires authentication and identity information
188 management processes that provide an appropriate level of assurance of identity. Because
189 different levels of risk are associated with different electronic transactions, IAEG has
190 adopted a multi-level approach to ALs. Each level describes a different degree of
191 certainty that the identity of the claimant is as proclaimed.

192 The IAEG defines four levels of assurance. The four IAEG ALs are based on the four
193 levels of assurance posited by the U.S. Federal Government and described in
194 OMB M-04-04 [[M-04-04](#)] and NIST Special Publication 800-63 [[NIST800-63](#)] for use by
195 Federal agencies. Accounting for minor semantic differences in the naming of the four
196 assurance levels in the EU IDABC “Proposal for a multi-level authentication mechanism
197 and a mapping of existing authentication mechanisms”, the European Union uses
198 substantially the same four assurance level model for identity assurance.

199 The IAEG ALs enable subscribers and relying parties to select appropriate electronic
200 identity trust services. IAEG uses the ALs to define the service assessment criteria to be
201 applied to electronic identity trust service providers when they are demonstrating
202 compliance through the IAEG assessment process. Relying parties should use the
203 assurance level descriptions to determine risk and map the type of credential issuance and
204 authentication services they require. Credential service providers (CSPs) should use the
205 ALs to determine what types of credentialing electronic identity trust services they are
206 capable of providing currently and/or aspire to provide in future service offerings.

207

208 **2.2 Description of the Four Assurance Levels**

209 The four ALs describe the degree of certainty associated with an identity assertion. The
210 levels are identified by both a number and a text label. The levels are defined as shown
211 in Table 2-1:

212

Table 2-1. Four Assurance Levels	
Level	Description
1	Little or no confidence in the asserted identity's validity
2	Some confidence in the asserted identity's validity
3	High confidence in the asserted identity's validity
4	Very high confidence in the asserted identity's validity

213

214 The choice of AL is based on the degree of certainty of identity required to mitigate the
215 risk resulting from an improper authentication, when related to the level of assurance
216 provided by the credentialing process. The degree of assurance required is determined by
217 the relying party through risk assessment processes covering the electronic transaction
218 system. By mapping risk impact levels to ALs, relying parties can then determine what
219 level of assurance they require. Further information on assessing impact levels is
220 provided in Table 2-2:

221

Table 2-2 Potential Impact at Each Assurance Level				
Potential Impact of Authentication Errors	Assurance Level*			
	1	2	3	4
Inconvenience, distress or damage to standing or reputation	Min	Mod	Sub	High
Financial loss or agency liability	Min	Mod	Sub	High
Harm to govt. agency programs or public interests	N/A	Min	Mod	High
Unauthorized release of sensitive information	N/A	Mod	Sub	High
Personal safety	N/A	N/A	Min	Sub, High
Civil or criminal violations	N/A	Min	Sub	High
<i>*Min=Minimum; Mod=Moderate; Sub=Substantial; High=High</i>				

222

223 The level of assurance provided is measured by the strength and rigor of the identity
224 proofing process, the credential's strength, and the management processes the service
225 provider applies to it. The IAEG has established service assessment criteria at each AL
226 for electronic trust services providing credential management services. These criteria are
227 described in Section 3.

228 CSPs can determine the AL at which their services might qualify by evaluating their
229 overall business processes and technical mechanisms against the IAEG service
230 assessment criteria. The service assessment criteria within each AL are the basis for
231 assessing and approving electronic trust services.

232 **2.2.1 Assurance Level 1**

233 At AL1, there is little or no confidence in the asserted identity. Use of this level is
234 appropriate when no negative consequences result from erroneous authentication and the
235 authentication mechanism used provides some assurance. A wide range of available
236 technologies and any of the token methods associated with higher ALs, including PINS,
237 can satisfy the authentication requirement. This level does not require use of
238 cryptographic methods.

239 **2.2.2 Assurance Level 2**

240 At AL2, there is some confidence that an asserted identity is accurate. Moderate risk is
241 associated with erroneous authentication. Single-factor remote network authentication is
242 appropriate. Successful authentication requires that the claimant prove control of the
243 token through a secure authentication protocol. Eavesdropper, replay, and online
244 guessing attacks are prevented. Identity proofing requirements are more stringent than
245 those for AL1 and the authentication mechanisms must be more secure, as well.

246 **2.2.3 Assurance Level 3**

247 AL3 is appropriate for transactions requiring high confidence in an asserted identity.
248 Substantial risk is associated with erroneous authentication. This level requires multi-
249 factor remote network authentication. Identity proofing procedures require verification of
250 identifying materials and information. Authentication must be based on proof of
251 possession of a key or password through a cryptographic protocol. Tokens can be “soft,”
252 “hard,” or “one-time password” device tokens. Note that both identity proofing and
253 authentication mechanism requirements are more substantial.

254 **2.2.4 Assurance Level 4**

255 AL4 is appropriate for transactions requiring very high confidence in an asserted identity.
256 This level provides the best practical remote-network authentication assurance, based on
257 proof of possession of a key through a cryptographic protocol. Level 4 is similar to

258 Level 3 except that only “hard” cryptographic tokens are allowed. High levels of
259 cryptographic assurance are required for all elements of credential and token
260 management. All sensitive data transfers are cryptographically authenticated using keys
261 bound to the authentication process.
262

263 3 Service Assessment Criteria

264 3.1 Context and Scope

265 The IAEG Service Assessment Criteria (SAC) are prepared and maintained by the
266 Identity Assurance Expert Group (IAEG) as part of its Identity Assurance Framework.
267 These criteria set out the requirements for credential services and their providers at all
268 assurance levels within the Framework. These criteria focus on the specific requirements
269 for IAEG assessment at each Assurance Level (AL) for the following:

- 270 • The general business and organizational conformity of services and their
271 providers;
- 272 • The functional conformity of identity proofing services, and;
- 273 • The functional conformity of credential management services and their
274 providers.

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

277 These criteria have been approved under the IAEG's governance rules as being suitable
278 for use by Liberty-Accredited Assessors in the performance of their assessments of trust
279 services whose providers are seeking recognition by IAEG.

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

283 This document describes the specific criteria that must be met to achieve each of the four
284 ALs supported by the IAEG. To be certified under the IAF Accreditation and
285 Certification Scheme, services must comply with all criteria at the appropriate level.

286 3.2 Readership

287 This description of Service Assessment Criteria is required reading for all Liberty-
288 Accredited Assessors, since it sets out the requirements with which service functions
289 must be independently verified as being in compliance, in order to be granted Liberty
290 Recognition.

291 The description of criteria in Sections 3.5, 3.6 and 3.7 is required reading for all
292 organizations wishing to become Liberty-Recognized Service Providers, and also for
293 those wishing to become Liberty-Accredited Assessors . It is also recommended reading
294 for those involved in the governance and day-to-day administration of the Identity
295 Assurance Framework.

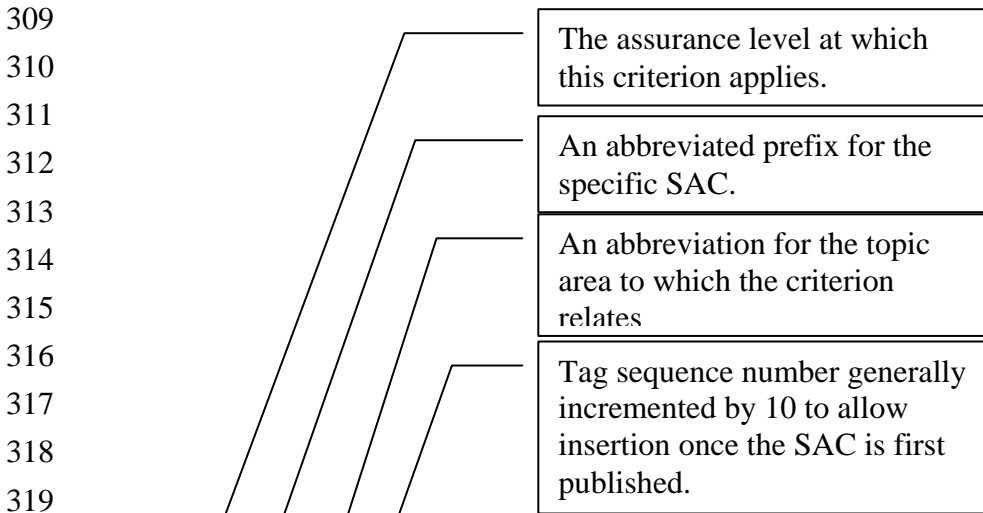
296 This document will also be of interest to those wishing to have a detailed understanding
297 of the operation of the Identity Assurance Framework but who are not actively involved
298 in its operations or in services that may fall within the scope of the framework.

299 3.3 Criteria Descriptions

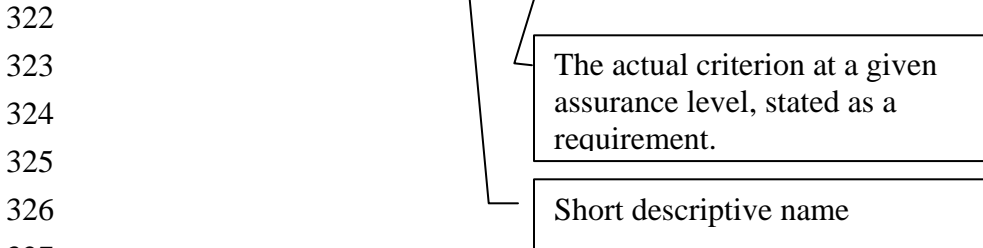
300 The Service Assessment Criteria are organized by AL. Subsections within each level
301 describe the criteria that apply to specific functions. The subsections are parallel.
302 Subsections describing the requirements for the same function at different levels of
303 assurance have the same title.

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

308 The criteria are described as follows:



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



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

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

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

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

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

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

345 **3.4 Terminology**

346 All special terms used in this description are defined in the IAF Glossary.

347 Note that when, in these criteria, the term 'Subscriber' is used it applies equally to
348 'Subscriber' and 'Subject' as defined in the IAF Glossary, according to the context in
349 which used. The term 'Subject' is used when the reference is explicitly towards that
350 party.

351

352 **3.5 Common Organizational Service Assessment Criteria**

353 The Service Assessment Criteria in this section establish the general business and
354 organizational requirements for conformity of services and service providers at all ALs
355 defined in Section 2. These criteria are generally referred to elsewhere within IAEG
356 documentation as CO-SAC.

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

359 **3.5.1 Assurance Level 1**

360 **3.5.1.1 Enterprise and Service Maturity**

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

364 An enterprise and its specified service must:

365 **AL1_CO_ESM#010 Established enterprise**

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

368 **AL1_CO_ESM#020 Established service**

369 Be fully operational in all areas described in the assessment package submitted for
370 assessment.

371 **Guidance:** Liberty will not recognize a service which is not fully released for the
372 provision of services to its intended user/client community. Systems, or parts thereof,
373 which are not fully proven and released shall not be considered in an assessment and
374 therefore should not be included within the scope of the assessment package. Parts of
375 systems still under development, or even still being planned, are therefore ineligible for
376 inclusion within the scope of assessment.

377 **AL1_CO_ESM#030 Legal & Contractual compliance**

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

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

383 even absent, even though compliance is apparent, and similarly, correct understanding
384 may not necessarily result in full compliance. The two are therefore complimentary.

385 **3.5.1.2 Notices and User information**

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

388 An enterprise and its specified service must:

389 **AL1_CO_NUI#010 General Service Definition**

390 Make available to the intended user community a service definition that includes a
391 Privacy Policy and all other applicable Terms, Conditions, Fees, and, including any
392 limitations of its usage.

393 **Guidance:** the intended user community encompasses potential and actual subscribers,
394 subjects and relying parties.

395 **AL1_CO_NUI#020 No stipulation**

396 **AL1_CO_NUI#030 Due notification**

397 Have in place and follow appropriate policy and procedures to ensure that it notifies
398 Users in a timely and reliable fashion of any changes to the service definition and any
399 applicable Terms, Conditions, and Privacy Policy for the specified service.

400 **AL1_CO_NUI#040 Subscriber Agreement**

401 Require subscribers and subjects to:

- 402 a) sign a user agreement accepting the terms of service prior to initiating service;
- 403 b) at periodic intervals, determined by significant service provision events (e.g.
404 issuance, re-issuance, renewal), re-affirm their understanding and observance of
405 the terms of service;
- 406 c) always provide full and correct responses to requests for information.

407 **AL1_CO_NUI#050 Record of Subscriber Agreement**

408 Obtain a record (hard-copy or electronic) of the subscriber's and subject's agreement to
409 the terms and conditions of service, prior to initiating the service and thereafter at
410 periodic intervals, determined by significant service provision events (e.g. re-issuance,
411 renewal).
412

413 **3.5.1.3 Not used**

414 **3.5.1.4 Not used**

415 **3.5.1.5 Not used**

416 **3.5.1.6 Not used**

417 **3.5.1.7 Secure Communications**

418 **AL1_CO_SCO#010 No stipulation**

419 **AL1_CO_SCO#020 Limited access to shared secrets**

420 Ensure that:

- 421 a) access to shared secrets shall be subject to discretionary controls which permit
- 422 access to those roles/applications needing such access;
- 423 b) stored shared secrets are not held in their plaintext form unless given adequate
- 424 physical or logical protection;
- 425 c) any plaintext passwords or secrets are not transmitted across any public or
- 426 unsecured network.

427

428

429 **3.5.2 Assurance Level 2**

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

433 **3.5.2.1 Enterprise and Service Maturity**

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

436 An enterprise and its specified service must:

437 **AL2_CO_ESM#010 Established enterprise**

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

440 **AL2_CO_ESM#020 Established service**

441 Be fully operational in all areas described in the assessment package submitted for
442 assessment.

443 **AL2_CO_ESM#030 Legal & Contractual compliance**

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

448 **Guidance:** Liberty will not recognize a service which is not fully released for the
449 provision of services to its intended user/client community. Systems, or parts thereof,
450 which are not fully proven and released shall not be considered in an assessment and
451 therefore should not be included within the scope of the assessment package. Parts of
452 systems still under development, or even still being planned, are therefore ineligible for
453 inclusion within the scope of assessment.

454 **AL2_CO_ESM#040 Financial Provisions**

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

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

461 how it has determined the degree of liability protection required, in view of its exposure
462 per 'service' and the number of users it has. This criterion helps ensure that Liberty does
463 not grant Recognition to services not likely to be sustainable over at least this minimum
464 period.

465 **AL2_CO_ESM#050 Data Retention and Protection**

466 **Specifically set out and demonstrate that it understands and complies with those**
467 **legal and regulatory requirements incumbent upon it concerning the retention and**
468 **destruction of private and identifiable information (personal and business)(i.e. its**
469 **secure storage and protection against loss, accidental public exposure and/or**
470 **improper destruction) and the protection of private information (against unlawful**
471 **or unauthorized access, excepting that permitted by the information owner or**
472 **required by due process).**

473 **Guidance:** Note that whereas the criterion is intended to address unlawful or
474 unauthorized access arising from malicious or careless actions (or inaction) some access
475 may be unlawful UNLESS authorized by the subject or effected as a part of a
476 specifically-executed legal process.
477

478 **3.5.2.2 Notices and User Information/Agreements**

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

482 An enterprise and its specified service must:

483 **AL2_CO_NUI#010 General Service Definition**

484 Make available to the intended user community a service definition that includes, *inter*
485 *alia*, **any specific uses or limitations on its use, Privacy, Identity Proofing &**
486 **Verification, and Revocation and Termination Policies**, all other applicable Terms,
487 Conditions, Fees, including any limitations of its usage, **and definitions of any terms**
488 **having specific intention or interpretation. Specific provisions are stated in further**
489 **criteria in this section.**

490 **Guidance:** the intended user community encompasses potential and actual subscribers,
491 subjects and relying parties.

492 **AL2_CO_NUI#020 Service Definition inclusions**

493 **Make available a service definition for the specified service containing clauses that**
494 **provide the following information:**

495 a) **The country in or legal jurisdiction under which the service is operated;**

- 496 b) if different from the above, the legal jurisdiction under which subscriber and
497 any relying party agreements are entered into;
498 c) applicable legislation with which the service complies;
499 d) obligations incumbent upon the CSP;
500 e) obligations incumbent upon the subscriber;
501 f) notifications and guidance for relying parties, especially in respect of actions
502 they are expected to take should they choose to rely upon the service;
503 g) statement of warranties;
504 h) statement of liabilities towards both Subjects and Relying Parties;
505 i) procedures for notification of changes to terms and conditions;
506 j) steps the CSP will take in the event that it chooses or is obliged to terminate
507 the service;
508 k) availability of the specified service per se and of its help desk facility.

509 **AL2_CO_NUI#030 Due notification**

510 Have in place and follow appropriate policy and procedures to ensure that it notifies
511 subscribers and subjects in a timely and reliable fashion of any changes to the service
512 definition and any applicable Terms, Conditions, Fees, and Privacy Policy for the
513 specified service **and provides a clear means by which subscribers and subjects must**
514 **indicate that they wish to accept the new terms or terminate their subscription.**

515 **AL2_CO_NUI#040 Subscriber Agreement**

516 Require subscribers and subjects to:

- 517 a) sign a user agreement accepting the terms of service prior to initiating service;
518 b) at periodic intervals, determined by significant service provision events (e.g.
519 issuance, re-issuance, renewal) **and otherwise at least once every 5 years**, re-
520 affirm their understanding and observance of the terms of service;
521 c) always provide full and correct responses to requests for information.

522 **AL2_CO_NUI#050 Record of Subscriber Information**

523 Obtain a record (hard-copy or electronic) of the subscriber's and subject's agreement to
524 the terms and conditions of service, prior to initiating the service and thereafter at
525 periodic intervals, determined by significant service provision events (e.g. re-issuance,
526 renewal) **and otherwise at least once every 5 years.**

527 **AL2_CO_NUI#060 Withdrawn**

528 Withdrawn.

529 **AL2_CO_NUI#070 Change of Subscriber Information**

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

534 **AL2_CO_NUI#080 Withdrawn**

535 Withdrawn.

536 **3.5.2.3 Information Security Management**

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

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

542 An enterprise and its specified service must:

543 **AL2_CO_ISM#010 Documented policies and procedures**

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

548 **AL2_CO_ISM#020 Policy Management and Responsibility**

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

553 **AL2_CO_ISM#030 Risk Management**

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

556 **AL2_CO_ISM#040 Continuity of Operations Plan**

557 **Have and shall keep updated a Continuity of Operations Plan that covers disaster**
558 **recovery and the resilience of the specified service.**

559 **AL2_CO_ISM#050 Configuration Management**

560 **Demonstrate that there is in place a configuration management system that at least**
561 **includes:**

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

565 **AL2_CO_ISM#060 Quality Management**

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

568 **AL2_CO_ISM#070 System Installation and Operation Controls**

569 **Apply controls during system development, procurement installation, and operation**
570 **that protect the security and integrity of the system environment, hardware,**
571 **software, and communications.**

572 **AL2_CO_ISM#080 Internal Service Audit**

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

577 **AL2_CO_ISM#090 Independent Audit**

578 **Be audited by an independent auditor at least every 24 months to ensure the**
579 **organization's security-related practices are consistent with the policies and**
580 **procedures for the specified service and the applicable SAC.**

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

586 **AL2_CO_ISM#100 Audit Records**

587 **Retain records of all audits, both internal and independent, for a period which, as a**
588 **minimum, fulfills its legal obligations and otherwise for greater periods either as it**
589 **may have committed to in its service definition or required by any other obligations**
590 **it has with/to a subscriber, and which in any event is not less than 36 months. Such**

591 records must be held securely and be protected against unauthorized access, loss,
592 alteration, public disclosure, or unapproved destruction.

593 **AL2_CO_ISM#110 Termination provisions**

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

599

600 **3.5.2.4 Security-relevant Event (Audit) Records**

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

603 An enterprise and its specified service must:

604 **AL2_CO_SER#010 Security event logging**

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

610 **Guidance:** it is sufficient that the accuracy of the time source is based upon an internal
611 computer/system clock synchronized to an internet time source. The time source need
612 not be authenticatable.

613

614 **3.5.2.5 Operational infrastructure**

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

618 An enterprise and its specified service must:

619 **AL2_CO_OPN#010 Technical security**

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

623 **these controls are effectively integrated with the applicable procedural and physical**
624 **security measures.**

625 **Guidance:** appropriate technical controls, suited to this Assurance Level, should be
626 selected from [NIST800-63] or its equivalent, as established by a recognized national
627 technical authority.

628 **AL2_CO_OPN#020 Defined security roles**

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

636 **AL2_CO_OPN#030 Personnel recruitment**

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

640 **AL2_CO_OPN#040 Personnel skills**

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

646 **AL2_CO_OPN#050 Adequacy of Personnel resources**

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

649 **AL2_CO_OPN#060 Physical access control**

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

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

654 Require a minimum of two person physical access control when accessing any
655 cryptographic modules.

656 **AL2_CO_OPN#070 Logical access control**

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

659

660 **3.5.2.6 External Services and Components**

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

664 An enterprise and its specified service must:

665 **AL2_CO_ESC#010 Contracted policies and procedures**

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

671 **AL2_CO_ESC#020 Visibility of contracted parties**

672 **Where the enterprise uses external suppliers for specific packaged components of**
673 **the service or for resources that are integrated with its own operations and under its**
674 **control, ensure that the suppliers' compliance with contractually-stipulated policies**
675 **and procedures, and thus with IAF service assessment criteria, can be independently**
676 **verified, and subsequently monitored if necessary.**

677

678 **3.5.2.7 Secure Communications**

679 An enterprise and its specified service must:

680 **AL2_CO_SCO#010 Secure remote communications**

681 **If the specific service components are located remotely from and communicate over**
682 **a public or unsecured network with other service components or other CSPs which**
683 **it services, the communications must be cryptographically authenticated, including**
684 **long-term and session tokens, by an authentication method that meets, at a**
685 **minimum, the requirements of AL2 and encrypted using a [[FIPS140-2](#)] Level 1-**

686 compliant encryption method or equivalent, as established by a recognized national
687 technical authority.

688 **AL2_CO_SCO#015 Verification / Authentication confirmation messages**

689 Ensure that any verification or confirmation of authentication messages, which
690 asserts either that a weakly bound credential is valid or that a strongly bound
691 credential has not been subsequently revoked, is logically bound to the credential
692 and that the message, the logical binding, and the credential are all transmitted
693 within a single integrity-protected session between the service and the Verifier /
694 Relying Party.

695 **AL2_CO_SCO#016 Verification of Revoked Credential**

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

- 698 a) the confirmation message shall be time-stamped, or;
- 699 b) the session keys shall expire with an expiration time no longer than that of
700 the applicable revocation list, or;
- 701 c) the time-stamped message, binding, and credential shall all be signed by the
702 service.

703 **AL2_CO_SCO#020 Limited access to shared secrets**

704 Ensure that:

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

711
712 These roles should be defined and documented by the CSP in accordance with
713 AL2_CO_OPN#020, above.

714 **AL2_CO_SCO#030 Logical protection of shared secrets**

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

- 716 a) concatenation of the password to a salt and/or username which is then hashed
717 with an Approved algorithm such that the computations used to conduct a

- 718 **dictionary or exhaustion attack on a stolen password file are not useful to**
719 **attack other similar password files, or;**
- 720 b) **encryption using an Approved algorithm and modes, and the shared secret**
721 **decrypted only when immediately required for authentication, or;**
- 722 c) **any secure method allowed to protect shared secrets at Level 3 or 4.**
- 723
- 724

725 **3.5.3 Assurance Level 3**

726 Achieving AL3 requires meeting more stringent criteria in addition to all criteria required
727 to achieve AL2.

728 **3.5.3.1 Enterprise and Service Maturity**

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

731 An enterprise and its specified service must:

732 **AL3_CO_ESM#010 Established enterprise**

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

735 **AL3_CO_ESM#020 Established service**

736 Be fully operational in all areas described in the assessment package submitted for
737 assessment .

738 **AL3_CO_ESM#030 Legal & Contractual compliance**

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

743 **Guidance:** Liberty will not recognize a service which is not fully released for the
744 provision of services to its intended user/client community. Systems, or parts thereof,
745 which are not fully proven and released shall not be considered in an assessment and
746 therefore should not be included within the scope of the assessment package. Parts of
747 systems still under development, or even still being planned, are therefore ineligible for
748 inclusion within the scope of assessment.

749 **AL3_CO_ESM#040 Financial Provisions**

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

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

757 per 'service' and the number of users it has. This criterion helps ensure that Liberty does
758 not grant Recognition to services not likely to be sustainable over at least this minimum
759 period.

760 **AL3_CO_ESM#050 Data Retention and Protection**

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

767 **AL3_CO_ESM#060 Ownership**

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

771 **AL3_CO_ESM#070 Independent management and operations**

772 **Demonstrate that, for the purposes of providing the specified service, its**
773 **management and operational structures are distinct, autonomous, have discrete**
774 **legal accountability, and operate according to separate policies, procedures, and**
775 **controls.**

776

777 **3.5.3.2 Notices and User Information**

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

781 An enterprise and its specified service must:

782 **AL3_CO_NUI#010 General Service Definition**

783 Make available to the intended user community a service definition which includes, *inter*
784 *alia*, any specific uses or limitations on its use, Privacy, Identity Proofing & Verification
785 Policy, and Revocation and Termination Policies, all other applicable Terms, Conditions,
786 Fees, including any limitations of its usage and definitions of any terms having specific
787 intention or interpretation. Specific provisions are stated in further criteria in this section.

788 **Guidance:** the intended user community encompasses potential and actual subscribers,
789 subjects and relying parties.

790 **AL3_CO_NUI#020 Service Definition inclusions**

791 Make available a service definition for the specified service containing clauses that
792 provide the following information:

- 793 a) the country in or the legal jurisdiction under which the service is operated;
- 794 b) if different to the above, the legal jurisdiction under which subscriber and any
795 relying party agreements are entered into;
- 796 c) applicable legislation with which the service complies;
- 797 d) obligations incumbent upon the CSP;
- 798 e) obligations incumbent upon the subscriber;
- 799 f) notifications and guidance for relying parties, especially in respect of actions they
800 are expected to take should they choose to rely upon the service's product;
- 801 g) statement of warranties;
- 802 h) statement of liabilities towards both Subjects and Relying Parties;
- 803 i) procedures for notification of changes to terms and conditions;
- 804 j) steps the CSP will take in the event that it chooses or is obliged to terminate the
805 service;
- 806 k) availability of the specified service *per se* and of its help desk facility.

807 **AL3_CO_NUI#030 Due notification**

808 Have in place and follow appropriate policy and procedures to ensure that it notifies
809 subscribers and subjects in a timely and reliable fashion of any changes to the service
810 definition and any applicable Terms, Conditions, Fees, and Privacy Policy for the
811 specified service and provides a clear means by which subscribers and subjects must
812 indicate that they wish to accept the new terms or terminate their subscription.

813 **AL3_CO_NUI#040 Subscriber Agreement**

814 Require subscribers and subjects to:

- 815 a) sign a user agreement accepting the terms of service prior to initiating service;
- 816 b) at periodic intervals, determined by significant service provision events (e.g.
817 issuance, re-issuance, renewal) and otherwise at least once every 5 years, re-affirm
818 their understanding and observance of the terms of service;
- 819 c) always provide full and correct responses to requests for information.

820 **AL3_CO_NUI#050 Record of Subscriber Information**

821 Obtain a record (hard-copy or electronic) of the subscriber's and subject's agreement to
822 the terms and conditions of service, prior to initiating the service and thereafter reaffirm
823 the agreement at periodic intervals, determined by significant service provision events
824 (e.g. re-issuance, renewal) and otherwise at least once every 5 years.

825 **AL3_CO_NUI#060** **Withdrawn**

826 Withdrawn.

827 **AL3_CO_NUI#070** **Change of Subscriber Information**

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

832 **AL3_CO_NUI#080** **Withdrawn**

833 Withdrawn.

834

835 **3.5.3.3 Information Security Management**

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

841 An enterprise and its specified service must:

842 **AL3_CO_ISM#010** **Documented policies and procedures**

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

847 **AL3_CO_ISM#020** **Policy Management and Responsibility**

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

852 **AL3_CO_ISM#030** **Risk Management**

853 Demonstrate a risk management methodology that adequately identifies and mitigates
854 risks related to the specified service and its user community **and must show that a risk**

855 **assessment review is performed at least once every six months, such as adherence to**
856 **SAS 70 or [\[IS27001\]](#) method.**

857 **AL3_CO_ISM#040 Continuity of Operations Plan**

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

861 **AL3_CO_ISM#050 Configuration Management**

862 Demonstrate that there is in place a configuration management system that at least
863 includes:

- 864 a) version control for software system components;
- 865 b) timely identification and installation of all organizationally-approved patches for
866 any software used in the provisioning of the specified service;
- 867 c) **version control and managed distribution for all documentation associated**
868 **with the specification, management, and operation of the system, covering**
869 **both internal and publicly available materials.**

870 **AL3_CO_ISM#060 Quality Management**

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

873 **AL3_CO_ISM#070 System Installation and Operation Controls**

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

- 877 a) **the software and hardware development environments, for customized**
878 **components;**
- 879 b) **the procurement process for commercial off-the-shelf (COTS) components;**
- 880 c) **contracted consultancy/support services;**
- 881 d) **shipment of system components;**
- 882 e) **storage of system components;**
- 883 f) **installation environment security;**
- 884 g) **system configuration;**
- 885 h) **transfer to operational status.**

886 **AL3_CO_ISM#080 Internal Service Audit**

887 Be audited at least once every 12 months for effective provision of the specified service
888 by independent internal audit functions of the enterprise responsible for the specified

889 service, unless it can show that by reason of its organizational size or due to other
890 **justifiable** operational restrictions it is unreasonable to be so audited.

891 **AL3_CO_ISM#090 Independent Audit**

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

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

900 **AL3_CO_ISM#100 Audit Records**

901 Retain records of all audits, both internal and independent, for a period which, as a
902 minimum, fulfils its legal obligations and otherwise for greater periods either as it may
903 have committed to in its service definition or required by any other obligations it has
904 with/to a subscriber, and which in any event is not less than 36 months. Such records
905 must be held securely and be protected against unauthorized access, loss, alteration,
906 public disclosure, or unapproved destruction.

907 **AL3_CO_ISM#110 Termination provisions**

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

913 **AL3_CO_ISM#120 Best Practice Security Management**

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

920

921 **3.5.3.4 Security-Relevant Event (Audit) Records**

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

924 An enterprise and its specified service must:

925 **AL3_CO_SER#010 Security Event Logging**

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

931 **Guidance:** it is sufficient that the accuracy of the time source is based upon an internal
932 computer/system clock synchronized to an internet time source. The time source need
933 not be authenticatable.

934

935 **3.5.3.5 Operational Infrastructure**

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

939 An enterprise and its specified service must:

940 **AL3_CO_OPN#010 Technical security**

941 Demonstrate that the technical controls employed will provide the level of security
942 protection required by the risk assessment and the ISMS, or other IT security
943 management methods recognized by a government or professional body, and that these
944 controls are effectively integrated with the applicable procedural and physical security
945 measures.

946 **Guidance:** appropriate technical controls, suited to this Assurance Level, should be
947 selected from [NIST800-63] or its equivalent, as established by a recognized national
948 technical authority.

949 **AL3_CO_OPN#020 Defined security roles**

950 Define, by means of a job description, the roles and responsibilities for each service-
951 related security-relevant task, relating it to specific procedures (which shall be set out in
952 the ISMS, or other IT security management methodology recognized by a government or
953 professional body) and other service-related job descriptions. Where the role is security-
954 critical or where special privileges or shared duties exist, these must be specifically

955 identified as such, including the applicable access privileges relating to logical and
956 physical parts of the service's operations.

957 **AL3_CO_OPN#030 Personnel recruitment**

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

963 **AL3_CO_OPN#040 Personnel skills**

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

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

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

972 **AL3_CO_OPN#060 Physical access control**

973 Apply physical access control mechanisms to ensure that:

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

978 **AL3_CO_OPN#070 Logical access control**

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

981

982 **3.5.3.6 External Services and Components**

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

986 An enterprise and its specified service must:

987 **AL3_CO_ESC#010 Contracted policies and procedures**

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

993 **AL3_CO_ESC#020 Visibility of contracted parties**

994 Where the enterprise uses external suppliers for specific packaged components of the
995 service or for resources which are integrated with its own operations and under its
996 controls, ensure that the suppliers' compliance with contractually-stipulated policies and
997 procedures, and thus with the IAF service assessment criteria, can be independently
998 verified, and subsequently monitored if necessary.

999

1000 **3.5.3.7 Secure Communications**

1001 An enterprise and its specified service must:

1002 **AL3_CO_SCO#010 Secure remote communications**

1003 If the specific service components are located remotely from and communicate over a
1004 public or unsecured network with other service components or other CSPs it services, the
1005 communications must be cryptographically authenticated, including long-term and
1006 session tokens, by an authentication protocol that meets, at a minimum, the requirements
1007 of AL3 and encrypted using **either a FIPS 140-2 [FIPS140-2] Level 2 (or higher)**
1008 **validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 validated**
1009 **cryptographic module**, or equivalent, as established by a recognized national technical
1010 authority.

1011 **AL3_CO_SCO#020 Limited access to shared secrets**

1012 Ensure that:

- 1013 a) access to shared secrets shall be subject to discretionary controls that permit
1014 access to those roles/applications requiring such access;
- 1015 b) stored shared secrets are **encrypted such that:**
 - 1016 i **the encryption key for the shared secret file is encrypted under a key**
1017 **held in either a FIPS 140-2 [FIPS140-2] Level 2 (or higher) validated**
1018 **hardware cryptographic module or any FIPS 140-2 Level 3 or 4**
1019 **validated cryptographic module, or equivalent, as established by a**

- 1020 **recognized national technical authority, and decrypted only as**
1021 **immediately required for an authentication operation;**
1022 ii **they are protected as a key within the boundary of either a FIPS 140-2**
1023 **Level 2 (or higher) validated hardware cryptographic module or any**
1024 **FIPS 140-2 Level 3 or 4 validated cryptographic module, or**
1025 **equivalent, as established by a recognized national technical**
1026 **authority, and are not exported from the module in plaintext;**
1027 iii **they are split by an "*n from m*" cryptographic secret-sharing method;**
1028 c) any long-term (i.e., not session) shared secrets are revealed only to the subscriber
1029 and CSP's direct agents (bearing in mind (a) above).

1030
1031 **These roles should be defined and documented by the CSP in accordance with**
1032 **AL3_CO_OPN#020, above.**

1033
1034

1035 **3.5.4 Assurance Level 4**

1036 Achieving AL4 requires meeting even more stringent criteria in addition to the criteria
1037 required to achieve AL3.

1038 **3.5.4.1 Enterprise and Service Maturity**

1039 Criteria in this section address the establishment of the enterprise offering the service and
1040 its basic standing as a legal and operational business entity.

1041 An enterprise and its specified service must:

1042 **AL4_CO_ESM#010 Established enterprise**

1043 Be a valid legal entity and a person with legal authority to commit the organization must
1044 submit the signed assessment package.

1045 **AL4_CO_ESM#020 Established service**

1046 Be fully operational in all areas described in the assessment package submitted for
1047 assessment.

1048 **AL4_CO_ESM#030 Legal & Contractual compliance**

1049 Demonstrate that it understands and complies with any legal requirements incumbent on
1050 it in connection with operation and delivery of the specified service, accounting for all
1051 jurisdictions within which its services may be offered. Any specific contractual
1052 requirements shall also be identified.

1053 **Guidance:** Liberty will not recognize a service which is not fully released for the
1054 provision of services to its intended user/client community. Systems, or parts thereof,
1055 which are not fully proven and released shall not be considered in an assessment and
1056 therefore should not be included within the scope of the assessment package. Parts of
1057 systems still under development, or even still being planned, are therefore ineligible for
1058 inclusion within the scope of assessment.

1059 **AL4_CO_ESM#040 Financial Provisions**

1060 Provide documentation of financial resources that allow for the continued operation of the
1061 service and demonstrate appropriate liability processes and procedures that satisfy the
1062 degree of liability exposure being carried.

1063 **Guidance:** The organization must show that it has a budgetary provision to operate the
1064 service for at least a twelve-month period, with a clear review of the budgetary planning
1065 within that period so as to keep the budgetary provisions extended. It must also show
1066 how it has determined the degree of liability protection required, in view of its exposure

1067 per ‘service’ and the number of users it has. This criterion helps ensure that Liberty does
1068 not grant Recognition to services not likely to be sustainable over at least this minimum
1069 period.

1070 **AL4_CO_ESM#050 Data Retention and Protection**

1071 Specifically set out and demonstrate that it understands and complies with those legal and
1072 regulatory requirements incumbent upon it concerning the retention and destruction of
1073 private and identifiable information (personal and business) (i.e. its secure storage and
1074 protection against loss, accidental public exposure and/or improper destruction) and the
1075 protection of private information (against unlawful or unauthorized access excepting that
1076 permitted by the information owner or required by due process).

1077 **AL4_CO_ESM#060 Ownership**

1078 If the enterprise named as the CSP is a part of a larger entity, the nature of the relationship
1079 with its parent organization, shall be disclosed to the assessors and, on their request, to
1080 customers.

1081 **AL4_CO_ESM#070 Independent Management and Operations**

1082 Demonstrate that, for the purposes of providing the specified service, its management and
1083 operational structures are distinct, autonomous, have discrete legal accountability, and
1084 operate according to separate policies, procedures, and controls.

1085

1086 **3.5.4.2 Notices and Subscriber Information/Agreements**

1087 Criteria in this section address the publication of information describing the service and
1088 the manner of and any limitations upon its provision, and how users are required to accept
1089 those terms.

1090 An enterprise and its specified service must:

1091 **AL4_CO_NUI#010 General Service Definition**

1092 Make available to the intended user community a service definition which includes, *inter*
1093 *alia*, any specific uses or limitations on its use, Privacy, Identity Proofing & Verification
1094 Policy and Revocation and Termination Policies, all other applicable Terms, Conditions,
1095 Fees, including any limitations of its usage and definitions of any terms having specific
1096 intention or interpretation. Specific provisions are stated in further criteria in this section.

1097 **Guidance:** the intended user community encompasses potential and actual subscribers,
1098 subjects and relying parties.

1099 **AL4_CO_NUI#020 Service Definition inclusions**

1100 Make available a service definition for the specified service containing clauses that
1101 provide the following information:

- 1102 a) the country in or legal jurisdiction under which the service is operated;
- 1103 b) if different to the above, the legal jurisdiction under which subscriber and any
1104 relying party agreements are entered into;
- 1105 c) applicable legislation with which the service complies;
- 1106 d) obligations incumbent upon the CSP;
- 1107 e) obligations incumbent upon the subscriber;
- 1108 f) notifications and guidance for relying parties, especially in respect of actions they
1109 are expected to take should they choose to rely upon the service's product;
- 1110 g) statement of warranties;
- 1111 h) statement of liabilities towards both Subjects and Relying Parties;
- 1112 i) procedures for notification of changes to terms and conditions;
- 1113 j) steps the CSP will take in the event that it chooses or is obliged to terminate the
1114 service;
- 1115 k) availability of the specified service *per se* and of its help desk facility.

1116 **AL4_CO_NUI#030 Due Notification**

1117 Have in place and follow appropriate policy and procedures to ensure that it notifies
1118 subscribers and subjects in a timely and reliable fashion of any changes to the service
1119 definition and any applicable Terms, Conditions, Fees, and Privacy Policy for the
1120 specified service and provides a clear means by which subscribers and subjects must
1121 indicate that they wish to accept the new terms or terminate their subscription.

1122 **AL4_CO_NUI#040 Subscriber Agreement**

1123 Require subscribers and subjects to:

- 1124 a) sign a user agreement accepting the terms of service prior to initiating service;
- 1125 b) at periodic intervals, determined by significant service provision events (e.g.
1126 issuance, re-issuance, renewal) and otherwise at least once every 5 years, re-affirm
1127 their understanding and observance of the terms of service;
- 1128 c) always provide full and correct responses to requests for information.

1129 **AL4_CO_NUI#050 Record of Subscriber Information**

1130 Obtain a record (hard-copy or electronic) of the subscriber's and subject's agreement to
1131 the terms and conditions of service, prior to initiating the service and thereafter reaffirm
1132 the agreement at periodic intervals, determined by significant service provision events
1133 (e.g. issuance, re-issuance, renewal) and otherwise at least once every 5 years.

1134 **AL4_CO_NUI#060** **Withdrawn**

1135 Withdrawn.

1136 **AL4_CO_NUI#070** **Change of Subscriber Information**

1137 Require and provide the mechanisms for subscribers and subjects to provide in a timely
1138 manner full and correct amendments should any of their recorded information change, as
1139 required under the terms of their use of the service, and only after the subscriber's and/or
1140 subject's identity has been authenticated.

1141 **AL4_CO_NUI#080** **Withdrawn**

1142 Withdrawn.

1143

1144 **3.5.4.3 Information Security Management**

1145 These criteria address the way in which the enterprise manages the security of its
1146 business, the specified service, and information it holds relating to its user community.

1147 This section focuses on the key components that comprise a well-established and
1148 effective Information Security Management System (ISMS), or other IT security
1149 management methodology recognized by a government or professional body.

1150 An enterprise and its specified service must:

1151 **AL4_CO_ISM#010** **Documented policies and procedures**

1152 Have documented all security-relevant administrative, management, and technical
1153 policies and procedures. The enterprise must ensure that these are based upon recognized
1154 standards, published references or organizational guidelines, are adequate for the
1155 specified service, and are implemented in the manner intended.

1156 **AL4_CO_ISM#020** **Policy Management and Responsibility**

1157 Have a clearly defined managerial role, at a senior level, where full responsibility for the
1158 business' security policies is vested and from which review, approval and promulgation of
1159 policy and related procedures is applied and managed. The latest approved versions of
1160 these policies must be applied at all times.

1161 **AL4_CO_ISM#030** **Risk Management**

1162 Demonstrate a risk management methodology that adequately identifies and mitigates
1163 risks related to the specified service and its user community and must show that on-going

1164 risk assessment review is conducted as a part of the business' procedures, such as
1165 adherence to SAS 70 or [\[IS27001\]](#) methods.

1166 **AL4_CO_ISM#040** **Continuity of Operations Plan**

1167 Have and shall keep updated a continuity of operations plan that covers disaster recovery
1168 and the resilience of the specified service and must show that **on-going review of this**
1169 **plan is conducted as a part of the business' procedures.**

1170 **AL4_CO_ISM#050** **Configuration Management**

1171 Demonstrate that there is in place a configuration management system that at least
1172 includes:

- 1173 a) version control for software system components;
- 1174 b) timely identification and installation of all organizationally-approved patches for
1175 any software used in the provisioning of the specified service;
- 1176 c) version control and managed distribution for all documentation associated with
1177 the specification, management, and operation of the system, covering both
1178 internal and publicly available materials.

1179 **AL4_CO_ISM#060** **Quality Management**

1180 Demonstrate that there is in place a quality management system that is appropriate for the
1181 specified service.

1182 **AL4_CO_ISM#070** **System Installation and Operation Controls**

1183 Apply controls during system development, procurement, installation, and operation that
1184 protect the security and integrity of the system environment, hardware, software, and
1185 communications having particular regard to:

- 1186 a) the software and hardware development environments, for customized
1187 components;
- 1188 b) the procurement process for commercial off-the-shelf (COTS) components;
- 1189 c) contracted consultancy/support services;
- 1190 d) shipment of system components;
- 1191 e) storage of system components;
- 1192 f) installation environment security;
- 1193 g) system configuration;
- 1194 h) transfer to operational status.

1195 **AL4_CO_ISM#080** **Internal Service Audit**

1196 Be audited at least once every 12 months for effective provision of the specified service
1197 by independent internal audit functions of the enterprise responsible for the specified

1198 service, unless it can show that by reason of its organizational size or due to other
1199 justifiable operational restrictions it is unreasonable to be so audited.

1200 **AL4_CO_ISM#090 Independent Audit**

1201 Be audited by an independent auditor at least every 24 months to ensure the
1202 organization's security-related practices are consistent with the policies and procedures
1203 for the specified service.

1204 **Guidance:** The appointed auditor should have appropriate accreditation or other
1205 acceptable experience and qualification, comparable to that required of Liberty-
1206 Accredited Assessors. It is expected that it will be cost-effective for the organization to
1207 use the same Liberty-Accredited Assessor for the purposes of fulfilling this criterion as
1208 they do for the maintenance of their grant of Liberty-Recognition.

1209 **AL4_CO_ISM#100 Audit Records**

1210 Retain records of all audits, both internal and independent, for a period which, as a
1211 minimum, fulfils its legal obligations and otherwise for greater periods either as it may
1212 have committed to in its service definition or required by any other obligations it has
1213 with/to a subscriber, and which in any event is not less than 36 months. Such records
1214 must be held securely and be protected against unauthorized access loss, alteration, public
1215 disclosure, or unapproved destruction.

1216 **AL4_CO_ISM#110 Termination provisions**

1217 Define the practices in place for the protection of subscribers' private and secret
1218 information related to their use of the service which must ensure the ongoing secure
1219 preservation and protection of legally-required records and for the secure destruction and
1220 disposal of any such information whose retention is no longer legally required. Specific
1221 details of these practices must be made available.

1222 **AL4_CO_ISM#120 Best Practice Security Management**

1223 Have in place a certified Information Security Management System (ISMS), or other IT
1224 security management methodology recognized by a government or professional body,
1225 that **has been assessed and found to be in compliance with the requirements of**
1226 **ISO/IEC 27001 [IS27001] and which applies and is appropriate to the CSP in**
1227 **question. All requirements expressed in preceding criteria in this section must *inter***
1228 ***alia* fall wholly within the scope of this ISMS, or the selected recognized alternative.**

1229

1230 **3.5.4.4 Security-Related (Audit) Records**

1231 The criteria in this section are concerned with the need to provide an auditable log of all
1232 events that are pertinent to the correct and secure operation of the service.

1233 An enterprise and its specified service must:

1234 **AL4_CO_SER#010 Security Event Logging**

1235 Maintain a log of all relevant security events concerning the operation of the service,
1236 together with a **precise** record of the time at which the event occurred (time-stamp)
1237 **provided by a trusted time-source** and retain such records with appropriate protection
1238 and controls to ensure successful retrieval, accounting for service definition, risk
1239 management requirements, applicable legislation and organizational policy.

1240 **Guidance:** the trusted time source could be an external trusted service or a network time
1241 server or other hardware timing device. The time source must be not only precise but
1242 authenticatable as well.

1243

1244 **3.5.4.5 Operational Infrastructure**

1245 The criteria in this section address the infrastructure within which the delivery of the
1246 specified service takes place. It puts particular emphasis upon the personnel involved,
1247 and their selection, training, and duties.

1248 An enterprise and its specified service must:

1249 **AL4_CO_OPN#010 Technical Security**

1250 Demonstrate that the technical controls employed will provide the level of security
1251 protection required by the risk assessment and the ISMS, or other IT security
1252 management methods recognized by a government or professional body, and that these
1253 controls are effectively integrated with the applicable procedural and physical security
1254 measures.

1255 **Guidance:** appropriate technical controls, suited to this Assurance Level, should be
1256 selected from [NIST800-63] or its equivalent, as established by a recognized national
1257 technical authority.

1258 **AL4_CO_OPN#020 Defined Security Roles**

1259 Define, by means of a job description, the roles and responsibilities for each service-
1260 related security-relevant task, relating it to specific procedures (which shall be set out in
1261 the ISMS, or other IT security management methodology recognized by a government or
1262 professional body) and other service-related job descriptions. Where the role is security-
1263 critical or where special privileges or shared duties exist, these must be specifically

1264 identified as such, including the applicable access privileges relating to logical and
1265 physical parts of the service's operations.

1266 **AL4_CO_OPN#030 Personnel Recruitment**

1267 Demonstrate that it has defined practices for the selection, vetting, and contracting of all
1268 service-related personnel, both direct employees and those whose services are provided
1269 by third parties. Full records of all searches and supporting evidence of qualifications and
1270 past employment must be kept for the duration of the individual's employment plus the
1271 longest lifespan of any credential issued under the service policy.

1272 **AL4_CO_OPN#040 Personnel skills**

1273 Ensure that employees are sufficiently trained, qualified, experienced, and current for the
1274 roles they fulfill. Such measures must be accomplished either by recruitment practices or
1275 through a specific training program. Where employees are undergoing on-the-job
1276 training, they must only do so under the guidance of a mentor possessing the defined
1277 service experiences for the training being provided.

1278 **AL4_CO_OPN#050 Adequacy of Personnel resources**

1279 Have sufficient staff to adequately operate and resource the specified service according to
1280 its policies and procedures.

1281 **AL4_CO_OPN#060 Physical access control**

1282 Apply physical access control mechanisms to ensure that:

- 1283 a) access to sensitive areas is restricted to authorized personnel;
- 1284 b) all removable media and paper documents containing sensitive information as
1285 plain-text are stored in secure containers;
- 1286 c) there is 24/7 monitoring for unauthorized intrusions.
1287

1288 **AL4_CO_OPN#070 Logical access control**

1289 Employ logical access control mechanisms that ensure access to sensitive system
1290 functions and controls is restricted to authorized personnel.

1291

1292 **3.5.4.6 External Services and Components**

1293 This section addresses the relationships and obligations upon contracted parties both to
1294 apply the policies and procedures of the enterprise and also to be available for assessment
1295 as critical parts of the overall service provision.

1296 An enterprise and its specified service must:

1297 **AL4_CO_ESC#010 Contracted Policies and Procedures**

1298 Where the enterprise uses external suppliers for specific packaged components of the
1299 service or for resources which are integrated with its own operations and under its
1300 control, ensure that those parties are engaged through reliable and appropriate contractual
1301 arrangements which stipulate which critical policies, procedures, and practices sub-
1302 contractors are required to fulfill.

1303 **AL4_CO_ESC#020 Visibility of Contracted Parties**

1304 Where the enterprise uses external suppliers for specific packaged components of the
1305 service or for resources which are integrated with its own operations and under its
1306 control, ensure that the suppliers' compliance with contractually-stipulated policies and
1307 procedures, and thus with the IAF service assessment criteria, can be independently
1308 verified, and subsequently monitored if necessary.

1309

1310 **3.5.4.7 Secure Communications**

1311 An enterprise and its specified service must:

1312 **AL4_CO_SCO#010 Secure remote communications**

1313 If the specific service components are located remotely from and communicate over a
1314 public or unsecured network with other service components or other CSPs it services, the
1315 communications must be cryptographically authenticated, including long-term and
1316 session tokens, by an authentication protocol that meets the requirements of AL4 and
1317 encrypted using either a FIPS 140-2 [FIPS140-2] Level 2 (or higher) validated hardware
1318 cryptographic module or any FIPS 140-2 Level 3 or 4 validated cryptographic module, or
1319 equivalent, as established by a recognized national technical authority.

1320 **AL4_CO_SCO#020 Limited access to shared secrets**

1321 Ensure that:

- 1322 a) access to shared secrets shall be subject to discretionary controls which permit
1323 access to those roles/applications which need such access;
1324 b) stored shared secrets are encrypted such that:

- 1325 i the encryption key for the shared secret file is encrypted under a key held
1326 in a FIPS 140-2 [FIPS140-2] Level 2 (or higher) validated hardware
1327 cryptographic module, or equivalent, as established by a recognized
1328 national technical authority, or any FIPS 140-2 Level 3 or 4 validated
1329 cryptographic module, or equivalent, as established by a recognized
1330 national technical authority, and decrypted only as immediately required
1331 for an authentication operation;
1332 ii they are protected as a key within the boundary of a FIPS 140-2 Level 2
1333 (or higher) validated hardware cryptographic module, or equivalent, as
1334 established by a recognized national technical authority, or any
1335 FIPS 140-2 Level 3 or 4 cryptographic module, or equivalent, as
1336 established by a recognized national technical authority, and are not
1337 exported in plaintext from the module;
1338 iii they are split by an "*n from m*" cryptographic secret-sharing method;
1339 c) any long-term (i.e., not session) shared secrets are revealed only to the subscriber
1340 and the CSP's direct agents (bearing in mind (a) above).
1341
1342

1343 **3.5.5 Compliance Tables**

1344 Use the following tables to correlate criteria for a particular Assurance Level (AL) and
1345 the evidence offered to support compliance.

1346 Service providers preparing for an assessment can use the table appropriate to the AL at
1347 which they are seeking approval to correlate evidence with criteria or to justify non-
1348 applicability (e.g., "specific service types not offered").

1349 Assessors can use the tables to record the steps in their assessment and their
1350 determination of compliance or failure.

1351 **Table 3-1. CO-SAC - AL1 Compliance**

Clause	Description	Compliance
AL1_CO_ESM#010	Established enterprise	
AL1_CO_ESM#020	Established service	
AL1_CO_ESM#030	Legal & Contractual compliance	
AL1_CO_NUI#010	General Service Definition	
AL1_CO_NUI#020	No stipulation	No conformity requirement
AL1_CO_NUI#030	Due notification	
AL1_CO_NUI#040	Subscriber Agreement	
AL1_CO_SCO#010	No stipulation	No conformity requirement
AL1_CO_SCO#020	Limited access to shared secrets	

1352

1353

1354

Table 3-2. CO-SAC - AL2 Compliance

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

AL2_CO_ESC#010	Contracted policies and procedures	
AL2_CO_ESC#020	Visibility of contracted parties	
AL2_CO_SCO#010	Secure remote communications	
AL2_CO_SCO#015	Verification / Authentication confirmation messages	
AL2_CO_SCO#016	Verification of Revoked Credential	
AL2_CO_SCO#020	Limited access to shared secrets	
AL2_CO_SCO#030	Logical protection of shared secrets	

1355

1356

1357

Table 3-3. CO-SAC - AL3 compliance

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

AL3_CO_OPN#050	Adequacy of Personnel resources	
AL3_CO_OPN#060	Physical access control	
AL3_CO_OPN#070	Logical access control	
AL3_CO_ESC#010	Contracted policies and procedures	
AL3_CO_ESC#020	Visibility of contracted parties	
AL3_CO_SCO#010	Secure remote communications	
AL3_CO_SCO#020	Limited access to shared secrets	

1358

1359

1360

Table 3-4. CO-SAC - AL4 compliance

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

AL4_CO_OPN#050	Adequacy of Personnel resources	
AL4_CO_OPN#060	Physical access control	
AL4_CO_OPN#070	Logical access control	
AL4_CO_ESC#010	Contracted Policies and Procedures	
AL4_CO_ESC#020	Visibility of Contracted Parties	
AL4_CO_SCO#010	Secure remote communications	
AL4_CO_SCO#020	Limited access to shared secrets	

1361

1362

1363 **3.6 Identity Proofing Service Assessment Criteria**

1364 The Service Assessment Criteria in this section establish the requirements for the
1365 technical conformity of identity proofing services at all ALs defined in Section 2. These
1366 criteria apply to a particular kind of electronic trust service (ETS) recognized by the
1367 IAEG and to the related credential service provider (CSP)—an identity proofing service
1368 for both individual identity and institutional identity credentials¹. (For definitions of
1369 terms used in this section, see Section 6). These criteria are generally referred to
1370 elsewhere within IAEG documentation as ID-SAC [**ID-SAC**].

1371 These criteria do not address the delivery of a credential to the applicant/subscriber,
1372 which is dealt with by the Credential Management SAC (CM-SAC), described in Section
1373 **3.7**.

1374 These criteria may only be used in an assessment in one of the following circumstances:

- 1375 • In conjunction with the Common Organizational SAC (CO-SAC), described in
1376 Section **3.5**, for a standalone identity proofing service.
- 1377 • In combination with one or more other SACs that must include the CO-SAC and
1378 where the identity proofing functions that these criteria address form part of a
1379 larger service offering.

1380 **3.6.1 Assurance Level 1**

1381 **3.6.1.1 Policy**

1382 An enterprise or specified service must:

1383 **AL1_ID_POL#010 Unique service identity**

1384 Ensure that a unique identity is attributed to the specific service, such that credentials
1385 issued by it can be distinguishable from those issued by other services, including services
1386 operated by the same enterprise.

1387 **AL1_ID_POL#020 Unique subject identity**

1388 Ensure that each applicant's identity is unique within the service's community of subjects
1389 and uniquely associable with tokens and/or credentials issued to that identity.

¹ Identity proofing processes for entities that are not human persons will vary by assurance level and will utilize existing SSL and EV SSL issuance requirements from the CA Browser Forum for the appropriate level of assurance. Non-individual verification requirements will be attached as an appendix to this document.

1390

1391 **3.6.1.2 Identity Verification**

1392 **3.6.1.2.1 In-Person Public Verification**

1393 An enterprise or specified service must:

1394 **AL1_ID_IPV#010 Required evidence**

1395 Accept a self-assertion of identity.

1396 **AL1_ID_IPV#020 Evidence checks**

1397 Accept self-attestation of evidence.

1398

1399 **3.6.1.2.2 Remote Public Verification**

1400 If the specific service offers remote identity proofing to applicants with whom it has no
1401 previous relationship, then it must comply with the criteria in this section.

1402 An enterprise or specified service must:

1403 **AL1_ID_RPV#010 Required evidence**

1404 Require the applicant to provide a contact telephone number or email address.

1405 **AL1_ID_RPV#020 Evidence checks**

1406 Verify the provided information by either:

1407 a) confirming the request by calling the number;

1408 b) successfully sending a confirmatory email and receiving a positive
1409 acknowledgement.

1410

1411 **3.6.1.2.3 Secondary Verification**

1412 In each of the above cases, an enterprise or specified service must:

1413 **AL1_ID_SCV#010 Secondary checks**

1414 Have in place additional measures (e.g., require additional documentary evidence, delay
1415 completion while out-of-band checks are undertaken) to deal with any anomalous
1416 circumstances that can be reasonably anticipated (e.g., a legitimate and recent change of
1417 address that has yet to be established as the address of record).

1418

1419

1420 **3.6.2 Assurance Level 2**

1421 **3.6.2.1 Policy**

1422 The specific service must show that it applies identity proofing policies and procedures
1423 and that it retains appropriate records of identity proofing activities and evidence.

1424 The enterprise or specified service must:

1425 **AL2_ID_POL#010 Unique service identity**

1426 Ensure that a unique identity is attributed to the specific service, such that credentials
1427 issued by it can be distinguishable from those issued by other services, including services
1428 operated by the same enterprise.

1429 **AL2_ID_POL#020 Unique subject identity**

1430 Ensure that each applicant's identity is unique within the service's community of subjects
1431 and uniquely associable with tokens and/or credentials issued to that identity.

1432 **AL2_ID_POL#030 Published Proofing Policy**

1433 **For each service it offers, make available the Identity Proofing Policy under which it**
1434 **verifies the identity of applicants² in form, language, and media accessible to the**
1435 **declared community of Users.**

1436 **AL2_ID_POL#040 Adherence to Proofing Policy**

1437 **Perform all identity proofing strictly in accordance with its published Identity**
1438 **Proofing Policy.**

1439

1440 **3.6.2.2 Identity Verification**

1441 The enterprise or specific service must:

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

- 1442 **AL2_ID_IDV#000 Identity Proofing classes**
- 1443 a) include in its Service Definition at least one of the following classes of identity
- 1444 proofing service, and;
- 1445 b) may offer any additional classes of identity proofing service it chooses,
- 1446 subject to the nature and the entitlement of the CSP concerned;
- 1447 c) Fulfill the applicable assessment criteria according to its choice of identity
- 1448 proofing service, i.e. conform to at least one of the criteria sets defined in:
- 1449 i) §3.6.2.2.1, “[In-Person Public Verification](#)”;
- 1450 ii) §3.6.2.2.2, “[Remote Public Verification](#)”;
- 1451 iii) §3.6.2.2.3, “[Current Relationship Verification](#)”;
- 1452 iv) §3.6.2.2.4, “[Affiliation Verification](#)”.

1453 **3.6.2.2.1 In-Person Public Verification**

1454 If the specific service offers in-person identity proofing to applicants with whom it has no

1455 previous relationship, then it must comply with the criteria in this section.

1456 The enterprise or specified service must:

1457 **AL2_ID_IPV#010 Required evidence**

1458 Ensure that the applicant is in possession of a primary Government Picture ID

1459 document that bears a photographic image of the holder.

1460 **AL2_ID_IPV#020 Evidence checks**

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

- 1462 a) appears to be a genuine document properly issued by the claimed issuing
- 1463 authority and valid at the time of application;
- 1464 b) bears a photographic image of the holder that matches that of the applicant;
- 1465 c) provides all reasonable certainty that the identity exists and that it uniquely
- 1466 identifies the applicant.
- 1467

1468 **3.6.2.2.2 Remote Public Verification**

1469 If the specific service offers remote identity proofing to applicants with whom it has no

1470 previous relationship, then it must comply with the criteria in this section.

1471 An enterprise or specified service must:

- 1472 **AL2_ID_RPV#010 Required evidence**
- 1473 **Ensure that the applicant submits the references of and attests to current possession**
1474 **of a primary Government Picture ID document, and one of**
- 1475 **a) a second Government ID;**
 - 1476 **b) an employee or student ID number;**
 - 1477 **c) a financial account number (e.g., checking account, savings account, loan or**
1478 **credit card) or;**
 - 1479 **d) a utility service account number (e.g., electricity, gas, or water) for an address**
1480 **matching that in the primary document.**
- 1481 **Ensure that the applicant provides additional verifiable personal information that at**
1482 **a minimum must include:**
- 1483 **a) a name that matches the referenced photo-ID;**
 - 1484 **b) date of birth and;**
 - 1485 **c) current address or personal telephone number.**
- 1486 **Additional information may be requested so as to ensure a unique identity, and**
1487 **alternative information may be sought where the enterprise can show that it leads to**
1488 **at least the same degree of certitude when verified.**
- 1489 **AL2_ID_RPV#020 Evidence checks**
- 1490 **Inspection and analysis of records against the provided identity references with the**
1491 **specified issuing authorities/institutions or through similar databases:**
- 1492 **a) the existence of such records with matching name and reference numbers;**
 - 1493 **b) corroboration of date of birth, current address of record, and other personal**
1494 **information sufficient to ensure a unique identity.**
- 1495
1496
- 1497 **Confirm address of record by at least one of the following means:**
- 1498 **a) RA sends notice to an address of record confirmed in the records check and**
1499 **receives a mailed or telephonic reply from applicant;**
 - 1500 **b) RA issues credentials in a manner that confirms the address of record**
1501 **supplied by the applicant, for example by requiring applicant to enter on-line**
1502 **some information from a notice sent to the applicant;**
 - 1503 **c) RA issues credentials in a manner that confirms ability of the applicant to**
1504 **receive telephone communications at telephone number or email at email**
1505 **address associated with the applicant in records. Any secret sent over an**
1506 **unprotected channel shall be reset upon first use.**
- 1507
1508 **Additional checks should be performed so as to establish the uniqueness of the**
1509 **claimed identity.**

1510 **Alternative checks may be performed where the enterprise can show that they lead**
1511 **to at least the same degree of certitude.**

1512

1513 **3.6.2.2.3 Current Relationship Verification**

1514 If the specific service offers identity proofing to applicants with whom it has a current
1515 relationship, then it must comply with the criteria in this section.

1516 The enterprise or specified service must:

1517 **AL2_ID_CRV#010 Required evidence**

1518 **Ensure that it has previously exchanged with the applicant a shared secret (e.g., a**
1519 **PIN or password) that meets AL2 (or higher) entropy requirements³.**

1520 **AL2_ID_CRV#020 Evidence checks**

1521 **Ensure that it has:**

- 1522 a) **only issued the shared secret after originally establishing the applicant's**
1523 **identity with a degree of rigor equivalent to that required under either the**
1524 **AL2 (or higher) requirements for in-person or remote public verification;**
1525 b) **an ongoing business relationship sufficient to satisfy the enterprise of the**
1526 **applicant's continued personal possession of the shared secret.**
1527

1528 **3.6.2.2.4 Affiliation Verification**

1529 If the specific service offers identity proofing to applicants on the basis of some form of
1530 affiliation, then it must comply with the criteria in this section for the purposes of
1531 establishing that affiliation, in addition to the previously stated requirements for the
1532 verification of the individual's identity.

1533 The enterprise or specified service must:

1534 **AL2_ID_AFV#000 Meet preceding criteria**

1535 **Meet all the criteria set out above, under §3.6.2.2.3, “[Current Relationship](#)**
1536 **[Verification](#)”.**

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

1537 **AL2_ID_AFV#010** Required evidence

1538 **Ensure that the applicant possesses:**

- 1539 a) **identification from the organization with which it is claiming affiliation;**
1540 b) **agreement from the organization that the applicant may be issued a**
1541 **credential indicating that an affiliation exists.**

1542 **AL2_ID_AFV#020** Evidence checks

1543 **Have in place and apply processes which ensure that the presented documents:**

- 1544 a) **each appear to be a genuine document properly issued by the claimed issuing**
1545 **authorities and valid at the time of application;**
1546 b) **refer to an existing organization with a contact address;**
1547 c) **indicate that the applicant has some form of recognizable affiliation with the**
1548 **organization;**
1549 d) **appear to grant the applicant an entitlement to obtain a credential indicating**
1550 **its affiliation with the organization.**

1551

1552 **3.6.2.2.5 Secondary Verification**

1553 In each of the above cases, the enterprise or specified service must:

1554 **AL2_ID_SCV#010** Secondary checks

1555 Have in place additional measures (e.g., require additional documentary evidence, delay
1556 completion while out-of-band checks are undertaken) to deal with any anomalous
1557 circumstances that can be reasonably anticipated (e.g., a legitimate and recent change of
1558 address that has yet to be established as the address of record).

1559

1560 **3.6.2.3 Verification Records**

1561 The specific service must retain records of the identity proofing (verification) that it
1562 undertakes and provide them to qualifying parties when so required.

1563 An enterprise or specified service must:

1564 **AL2_ID_VRC#010** Verification Records for Personal Applicants

1565 **Log, taking account of all applicable legislative and policy obligations, a record of**
1566 **the facts of the verification process, including a reference relating to the verification**
1567 **processes and the date and time of verification.**

1568 **Guidance:** the facts of the verification process should include the specific record
1569 information (source, unique reference, value/content) used in establishing the applicant's

1570 identity, and will be determined by the specific processes used and documents accepted
1571 by the CSP. The CSP need not retain these records itself if it uses a third-party service
1572 which retains such records securely and to which the CSP has access when required, in
1573 which case it must retain a record of the identity of the third-party service providing the
1574 verification service or the location at which the (in-house) verification was performed.

1575 a)

1576 **AL2_ID_VRC#020 Verification Records for Affiliated Applicants**

1577 **In addition to the foregoing, log, taking account of all applicable legislative and**
1578 **policy obligations, a record of the additional facts of the verification process. At a**
1579 **minimum, records of identity information must include:**

- 1580 a) **the subscriber's full name;**
- 1581 b) **the subscriber's current address of record;**
- 1582 c) **the subscriber's current telephone or email address of record;**
- 1583 d) **the subscriber's acknowledgement for issuing the subject with a credential;**
- 1584 e) **type, issuing authority, and reference number(s) of all documents checked in**
1585 **the identity proofing process.**

1586 **AL2_ID_VRC#030 Record Retention**

1587 **Either retain, securely, the record of the verification process for the duration of the**
1588 **subscriber account plus 7.5 years, or submit same record to a client CSP that has**
1589 **undertaken to retain the record for the requisite period or longer.**

1590

1591

1592 **3.6.3 Assurance Level 3**

1593 **3.6.3.1 Policy**

1594 The specific service must show that it applies identity proofing policies and procedures
1595 and that it retains appropriate records of identity proofing activities and evidence.

1596 The enterprise or specified service must:

1597 **AL3_ID_POL#010 Unique service identity**

1598 Ensure that a unique identity is attributed to the specific service, such that credentials
1599 issued by it can be distinguishable from those issued by other services, including services
1600 operated by the same enterprise.

1601 **AL3_ID_POL#020 Unique subject identity**

1602 Ensure that each applicant's identity is unique within the service's community of subjects
1603 and uniquely associable with tokens and/or credentials issued to that identity.

1604 **AL3_ID_POL#030 Published Proofing Policy**

1605 Make available the Identity Proofing Policy under which it verifies the identity of
1606 applicants⁴ in form, language, and media accessible to the declared community of Users.

1607 **AL3_ID_POL#040 Adherence to Proofing Policy**

1608 Perform all identity proofing strictly in accordance with its published Identity Proofing
1609 Policy, through application of the procedures and processes set out in its Identity Proofing
1610 Practice Statement.

1611

1612 **3.6.3.2 Identity Verification**

1613 The enterprise or specific service must:

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

1614 **AL3_ID_IDV#000 Identity Proofing classes**

- 1615 a) include in its Service Definition at least one of the following classes of identity
1616 proofing services, and;
- 1617 b) may offer any additional classes of identity proofing service it chooses, subject to
1618 the nature and the entitlement of the CSP concerned;
- 1619 c) Fulfill the applicable assessment criteria according to its choice of identity
1620 proofing service, i.e. conform to at least one of the criteria sets defined in:
- 1621 i) §3.6.3.2.1, “[In-Person Public Verification](#)”;
- 1622 ii) §3.6.3.2.2, “[Remote Public Verification](#)”;
- 1623 iii) §3.6.3.2.4, “[Affiliation Verification](#)”.
- 1624

1625 **3.6.3.2.1 In-Person Public Verification**

1626 A specific service that offers identity proofing to applicants with whom it has no previous
1627 relationship must comply with the criteria in this section.

1628 The enterprise or specified service must:

1629 **AL3_ID_IPV#010 Required evidence**

1630 Ensure that the applicant is in possession of a primary Government Picture ID document
1631 that bears a photographic image of the holder.

1632 **AL3_ID_IPV#020 Evidence checks**

1633 **Have in place and apply processes which ensure** that the presented document:

- 1634 a) appears to be a genuine document properly issued by the claimed issuing
1635 authority and valid at the time of application;
- 1636 b) bears a photographic image of the holder that matches that of the applicant;
- 1637 c) **is electronically verified by a record check with the specified issuing
1638 authority or through similar databases that:**
- 1639 i) **establishes the existence of such records with matching name and
1640 reference numbers;**
- 1641 ii) **corroborates date of birth, current address of record, and other
1642 personal information sufficient to ensure a unique identity;**
- 1643 d) provides all reasonable certainty that the identity exists and that it uniquely
1644 identifies the applicant.
- 1645

1646 **3.6.3.2.2 Remote Public Verification**

1647 A specific service that offers remote identity proofing to applicants with whom it has no
1648 previous relationship must comply with the criteria in this section.

1649 The enterprise or specified service must:

1650 **AL3_ID_RPV#010 Required evidence**

1651 Ensure that the applicant submits the references of and attests to current possession of a
1652 primary Government Picture ID document, and one of:

- 1653 a) a second Government ID;
- 1654 b) an employee or student ID number;
- 1655 c) a financial account number (e.g., checking account, savings account, loan or
1656 credit card), or;
- 1657 d) a utility service account number (e.g., electricity, gas, or water) for an address
1658 matching that in the primary document.

1659 Ensure that the applicant provides additional verifiable personal information that at a
1660 minimum must include:

- 1661 e) a name that matches the referenced photo-ID;
- 1662 f) date of birth;
- 1663 g) current address or personal telephone number.

1664 Additional information may be requested so as to ensure a unique identity, and alternative
1665 information may be sought where the enterprise can show that it leads to at least the same
1666 degree of certitude when verified.

1667

1668 **AL3_ID_RPV#020 Evidence checks**

1669 **Electronically verify by a record check against the provided identity references with**
1670 **the specified issuing authorities/institutions or through similar databases:**

- 1671 a) the existence of such records with matching name and reference numbers;
- 1672 b) corroboration of date of birth, current address of record **or personal telephone**
1673 **number**, and other personal information sufficient to ensure a unique identity;
- 1674 c) **dynamic verification of personal information previously provided by or**
1675 **likely to be known only by the applicant.**

1676

1677

1678 Confirm address of record by at least one of the following means:

- 1679 a) RA sends notice to an address of record confirmed in the records check and
1680 receives a mailed or telephonic reply from applicant;

- 1681 b) RA issues credentials in a manner that confirms the address of record supplied by
1682 the applicant, for example by requiring applicant to enter on-line some
1683 information from a notice sent to the applicant;
1684 c) RA issues credentials in a manner that confirms ability of the applicant to receive
1685 telephone communications at telephone number or e mail at e mail address
1686 associated with the applicant in records. Any secret sent over an unprotected
1687 channel shall be reset upon first use.
1688

1689 Additional checks may be performed so as to establish the uniqueness of the claimed
1690 identity, and alternative checks may be performed where the enterprise can show that they
1691 lead to at least the same degree of certitude.

1692 **3.6.3.2.3 Current Relationship Verification**

1693 No stipulation.
1694

1695 **3.6.3.2.4 Affiliation Verification**

1696 A specific service that offers identity proofing to applicants on the basis of some form of
1697 affiliation must comply with the criteria in this section to establish that affiliation and
1698 with the previously stated requirements to verify the individual's identity.

1699 The enterprise or specified service must:

1700 **AL3_ID_AFV#000 Meet preceding criteria**

1701 Meet all the the criteria set out above, under §3.6.3.2.2, "[Remote Public Verification](#)".

1702 **AL3_ID_AFV#010 Required evidence**

1703 Ensure that the applicant possesses:

- 1704 a) identification from the organization with which it is claiming affiliation;
1705 b) agreement from the organization that the applicant may be issued a credential
1706 indicating that an affiliation exists.

1707 **AL3_ID_AFV#020 Evidence checks**

1708 Have in place and apply processes which ensure that the presented documents:

- 1709 a) each appear to be a genuine document properly issued by the claimed issuing
1710 authorities and valid at the time of application;
1711 b) refer to an existing organization with a contact address;
1712 c) indicate that the applicant has some form of recognizable affiliation with the
1713 organization;

- 1714 d) appear to grant the applicant an entitlement to obtain a credential indicating an
1715 affiliation with the organization.
1716

1717 **3.6.3.2.5 Secondary Verification**

1718 In each of the above cases, the enterprise or specified service must also meet the
1719 following criteria:

1720 **AL3_ID_SCV#010 Secondary checks**

1721 Have in place additional measures (e.g., require additional documentary evidence, delay
1722 completion while out-of-band checks are undertaken) to deal with any anomalous
1723 circumstance that can reasonably be anticipated (e.g., a legitimate and recent change of
1724 address that has yet to be established as the address of record).

1725 **3.6.3.3 Verification Records**

1726 The specific service must retain records of the identity proofing (verification) that it
1727 undertakes and provide them to qualifying parties when so required.

1728 The enterprise or specified service must:

1729 **AL3_ID_VRC#010 Verification Records for Personal Applicants**

1730 Log, taking account of all applicable legislative and policy obligations, a record of the
1731 facts of the verification process **and the identity of the registrar**, including a reference
1732 relating to the verification processes and the date and time of verification.

1733 **Guidance:** the facts of the verification process should include the specific record
1734 information (source, unique reference, value/content) used in establishing the applicant's
1735 identity, and will be determined by the specific processes used and documents accepted
1736 by the CSP. The CSP need not retain these records itself if it uses a third-party service
1737 which retains such records securely and to which the CSP has access when required, in
1738 which case it must retain a record of the identity of the third-party service providing the
1739 verification service or the location at which the (in-house) verification was performed.

1740 **AL3_ID_VRC#020 Verification Records for Affiliated Applicants**

1741 In addition to the foregoing, log, taking account of all applicable legislative and policy
1742 obligations, a record of the additional facts of the verification process. At a minimum,
1743 records of identity information must include:

- 1744 a) the subscriber's full name;
1745 b) the subscriber's current address of record;
1746 c) the subscriber's current telephone or email address of record;
1747 d) the subscriber's acknowledgement of issuing the subject with a credential;

- 1748 e) type, issuing authority, and reference number(s) of all documents checked in the
1749 identity proofing process;
1750 f) **where required, a telephone or email address for related contact and/or**
1751 **delivery of credentials/notifications.**

1752 **AL3_ID_VRC#030 Record Retention**

1753 Either retain, securely, the record of the verification/revocation process for the duration of
1754 the subscriber account plus 7.5 years, or submit the same record to a client CSP that has
1755 undertaken to retain the record for the requisite period or longer.

1756

1757

1758 **3.6.4 Assurance Level 4**

1759 Identity proofing at Assurance Level 4 requires the physical presence of the applicant in
1760 front of the registration officer with photo ID or other readily verifiable biometric identity
1761 information, as well as the requirements set out by the following criteria.

1762 **3.6.4.1 Policy**

1763 The specific service must show that it applies identity proofing policies and procedures
1764 and that it retains appropriate records of identity proofing activities and evidence.

1765 The enterprise or specified service must:

1766 **AL4_ID_POL#010 Unique service identity**

1767 Ensure that a unique identity is attributed to the specific service, such that credentials
1768 issued by it can be distinguishable from those issued by other services, including services
1769 operated by the same enterprise.

1770 **AL4_ID_POL#020 Unique subject identity**

1771 Ensure that each applicant's identity is unique within the service's community of subjects
1772 and uniquely associable with tokens and/or credentials issued to that identity.

1773 **AL4_ID_POL#030 Published Proofing Policy**

1774 Make available the Identity Proofing Policy under which it verifies the identity of
1775 applicants⁵ in form, language, and media accessible to the declared community of users.

1776 **AL4_ID_POL#040 Adherence to Proofing Policy**

1777 Perform all identity proofing strictly in accordance with its published Identity Proofing
1778 Policy, through application of the procedures and processes set out in its Identity Proofing
1779 Practice Statement.

1780

1781 **3.6.4.2 Identity Verification**

1782 The enterprise or specific service may:

⁵ For an identity proofing service that is within the management scope of a credential management service provider, this should be the credential management service's definitive policy; for a stand-alone identity proofing service, the policy may be either that of a client which has defined one through contract, the ID service's own policy or a separate policy that explains how the client's policies will be complied with.

1783 **AL4_ID_IDV#000 Identity Proofing classes**

1784 **[Omitted] offer only face-to-face identity proofing service. Remote verification is not**
1785 **allowed at this assurance level;**

1786

1787 The enterprise or specified service must:

1788 **3.6.4.2.1 In-Person Public Verification**

1789 **AL4_ID_IPV#010 Required evidence**

1790 Ensure that the applicant is in possession of:

- 1791 a) a primary Government Picture ID document that bears a photographic image of
1792 the **holder and either:**
1793 i) **secondary Government Picture ID or an account number issued by a**
1794 **regulated financial institution or;**
1795 ii) **two items confirming name, and address or telephone number, such**
1796 **as: utility bill, professional license or membership, or other evidence**
1797 **of equivalent standing.**

1798 **AL4_ID_IPV#020 No stipulation**

1799 **AL4_ID_IPV#030 Evidence checks – primary ID**

1800 Ensure that the presented document:

- 1801 a) **appears to be a genuine document properly issued by the claimed issuing**
1802 **authority and valid at the time of application;**
1803 b) **bears a photographic image of the holder which matches that of the**
1804 **applicant;**
1805 c) **is electronically verified by a record check with the specified issuing**
1806 **authority or through similar databases that:**
1807 i) **establishes the existence of such records with matching name and**
1808 **reference numbers;**
1809 ii) **corroborates date of birth, current address of record, and other**
1810 **personal information sufficient to ensure a unique identity;**
1811 d) **provides all reasonable certainty, at AL4, that the identity exists and that it**
1812 **uniquely identifies the applicant.**

1813 **AL4_ID_IPV#040 Evidence checks – secondary ID**

1814 Ensure that the presented document meets the following conditions:

- 1815 a) **If it is secondary Government Picture ID:**

- 1816 i) appears to be a genuine document properly issued by the claimed
1817 issuing authority and valid at the time of application;
1818 ii) bears a photographic image of the holder which matches that of the
1819 applicant;
1820 iii) states an address at which the applicant can be contacted.
1821 b) If it is a financial institution account number, is verified by a record check
1822 with the specified issuing authority or through similar databases that:
1823 i) establishes the existence of such records with matching name and
1824 reference numbers;
1825 ii) corroborates date of birth, current address of record, and other
1826 personal information sufficient to ensure a unique identity;
1827 c) If it is two utility bills or equivalent documents:
1828 i) each appears to be a genuine document properly issued by the
1829 claimed issuing authority;
1830 ii) corroborates current address of record or telephone number
1831 sufficient to ensure a unique identity.

1832 **AL4_ID_IPV#050 Applicant knowledge checks**

1833 Where the applicant is unable to satisfy any of the above requirements, that the
1834 applicant can provide a unique identifier, such as a Social Security Number (SSN),
1835 that matches the claimed identity.

1836

1837 **3.6.4.2.2 Remote Public Verification**

1838 Not permitted

1839 **3.6.4.2.3 Affiliation Verification**

1840 A specific service that offers identity proofing to applicants on the basis of some form of
1841 affiliation must comply with the criteria in this section to establish that affiliation, in
1842 addition to complying with the previously stated requirements for verifying the
1843 individual's identity.

1844 The enterprise or specified service must:

1845 **AL4_ID_AFV#000 Meet preceding criteria**

1846 Meet all the criteria set out above, under §3.6.4.2.1, "[In-Person Public Verification](#)".

1847 **AL4_ID_AFV#010 Required evidence**

1848 Ensure that the applicant possesses:

- 1849 a) identification from the organization with which it is claiming affiliation;

- 1850 b) agreement from the organization that the applicant may be issued a credential
1851 indicating that an affiliation exists.

1852 **AL4_ID_AFV#020 Evidence checks**

1853 Have in place and apply processes which ensure that the presented documents:

- 1854 a) each appear to be a genuine document properly issued by the claimed issuing
1855 authorities and valid at the time of application;
1856 b) refer to an existing organization with a contact address;
1857 c) indicate that the applicant has some form of recognizable affiliation with the
1858 organization;
1859 d) appear to grant the applicant an entitlement to obtain a credential indicating an
1860 affiliation with the organization.
1861

1862 **3.6.4.2.4 Secondary Verification**

1863 In each of the above cases, the enterprise or specified service must also meet the
1864 following criteria:

1865 **AL4_ID_SCV#010 Secondary checks**

1866 Have in place additional measures (e.g., require additional documentary evidence, delay
1867 completion while out-of-band checks are undertaken) to deal with any anomalous
1868 circumstances that can reasonably be anticipated (e.g., a legitimate and recent change of
1869 address that has yet to be established as the address of record).

1870

1871 **3.6.4.3 Verification Records**

1872 The specific service must retain records of the identity proofing (verification) that it
1873 undertakes and provide them to qualifying parties when so required.

1874 The enterprise or specified service must:

1875 **AL4_ID_VRC#010 Verification Records for Personal Applicants**

1876 Log, taking account of all applicable legislative and policy obligations, a record of the
1877 facts of the verification process and the identity of the registrar, including a
1878 reference relating to the verification processes and the date and time of verification
1879 **issued by a trusted time-source.**

1880 **Guidance:** the facts of the verification process should include the specific record
1881 information (source, unique reference, value/content) used in establishing the applicant's
1882 identity, and will be determined by the specific processes used and documents accepted
1883 by the CSP. The CSP need not retain these records itself if it uses a third-party service

1884 which retains such records securely and to which the CSP has access when required, in
1885 which case it must retain a record of the identity of the third-party service providing the
1886 verification service or the location at which the (in-house) verification was performed.

1887 **AL4_ID_VRC#020 Verification Records for Affiliated Applicants**

1888 In addition to the foregoing, log, taking account of all applicable legislative and policy
1889 obligations, a record of the additional facts of the verification process. At a minimum,
1890 records of identity information must include:

- 1891 a) the subscriber's full name;
- 1892 b) the subscriber's current address of record;
- 1893 c) the subscriber's current telephone or email address of record;
- 1894 d) the subscriber's authorization for issuing the subject a credential;
- 1895 e) type, issuing authority, and reference number(s) of all documents checked in the
1896 identity proofing process;
- 1897 **f) a biometric record of each required representative of the affiliating**
1898 **organization (e.g., a photograph, fingerprint, voice recording), as determined**
1899 **by that organization's governance rules/charter.**

1900 **AL4_ID_VRC#030 Record Retention**

1901 Either retain, securely, the record of the verification/revocation process for the duration of
1902 the subscriber account plus **10.5** years, or submit the record to a client CSP that has
1903 undertaken to retain the record for the requisite period or longer.

1904

1905

1906 **3.6.5 Compliance Tables**

1907 Use the following tables to correlate criteria for a particular Assurance Level (AL) and
1908 the evidence offered to support compliance.

1909 Service providers preparing for an assessment can use the table appropriate to the AL at
1910 which they are seeking approval to correlate evidence with criteria or to justify non-
1911 applicability (e.g., "specific service types not offered").

1912 Assessors can use the tables to record the steps in their assessment and their
1913 determination of compliance or failure.

1914 **Table 3-5. ID-SAC - AL1 Compliance**

Clause	Description	Compliance
AL1_ID_POL#010	Unique service identity	
AL1_ID_POL#020	Unique subject identity	
AL1_ID_IPV#010	Required evidence	
AL1_ID_IPV#020	Evidence checks	
AL1_ID_RPV#010	Required evidence	
AL1_ID_RPV#020	Evidence checks	
AL1_ID_SCV#010	Secondary checks	

1915

1916

1917

Table 3-6. ID-SAC - AL2 Compliance

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

1918

1919

1920

Table 3-7. ID-SAC - AL3 compliance

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

1921

1922

1923

Table 3-8. ID-SAC - AL4 compliance

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

1924

1925

1926 **3.7 Credential Management Service Assessment Criteria**

1927 The Service Assessment Criteria in this section establish requirements for the functional
1928 conformity of credential management services and their providers at all ALs defined in
1929 Section 2. These criteria are generally referred to elsewhere within IAF documentation as
1930 CM-SAC.

1931 The criteria are divided into five parts. Each part deals with a specific functional aspect
1932 of the overall credential management process.

1933 This SAC must be used in conjunction with the Common Organizational SAC
1934 (CO-SAC), described in Section 3.5, and, in addition, must either:

- 1935 • explicitly include the criteria of the Identity Proofing SAC ([ID-SAC]) described
1936 in Section 3.6, or
- 1937 • rely upon the criteria of the ID-SAC [ID-SAC] being fulfilled by the use of an
1938 IAEG-approved ID-proofing service.

1939 **3.7.1 Part A - Credential Operating Environment**

1940 The criteria in this part deal with the overall operational environment in which the
1941 credential life-cycle management is conducted. The credential management service
1942 assessment criteria must be used in conjunction with the Common Organizational criteria
1943 described in Section 3.5. In addition, they must either explicitly include the identity
1944 proofing service assessment criteria described in Section 3.6 or rely upon those criteria
1945 being fulfilled by the use of an IAEG-approved identity proofing service.

1946 These criteria describe requirements for the overall operational environment in which
1947 credential lifecycle management is conducted. The common organizational criteria
1948 describe broad requirements. The criteria in this section describe implementation
1949 specifics. Implementation depends on the AL. The procedures and processes required to
1950 create a secure environment for management of credentials and the particular
1951 technologies that are considered strong enough to meet the assurance requirements differ
1952 considerably from level to level.

1953 **3.7.1.1 Assurance Level 1**

1954 These criteria apply to PINs and passwords, as well as SAML assertions.

1955 **3.7.1.1.1 Not used**

1956 No stipulation.

1957

1958 **3.7.1.1.2 Security Controls**

1959 An enterprise and its specified service must:

-
- 1960 **AL1_CM_CTR#010** **No stipulation**
- 1961 **AL1_CM_CTR#020** **Protocol threat risk assessment and controls**
- 1962 Account for at least the following protocol threats and apply appropriate controls:
- 1963 a) password guessing, such that the resistance to an on-line guessing attack against a
1964 selected user/password is at least 1 in 2^{10} (1,024);
- 1965 b) message replay.
- 1966 **AL1_CM_CTR#025** **No stipulation**
- 1967 **AL1_CM_CTR#030** **System threat risk assessment and controls**
- 1968 Account for the following system threats and apply appropriate controls:
- 1969 a) the introduction of malicious code;
- 1970 b) compromised authentication arising from insider action;
- 1971 c) out-of-band attacks by other users and system operators (e.g., the ubiquitous
1972 shoulder-surfing);
- 1973 d) spoofing of system elements/applications;
- 1974 e) malfeasance on the part of subscribers and subjects.
- 1975
- 1976 **3.7.1.1.3 Storage of Long-term Secrets**
- 1977 **AL1_CM_STS#010** **Withdrawn**
- 1978 Withdrawn (AL1_CO_SCO#020 (a) & (b) enforce this requirement)
- 1979
- 1980 **3.7.1.1.4 Not used**
- 1981 **3.7.1.1.5 Subject Options**
- 1982 **AL1_CM_OPN#010** **Withdrawn**
- 1983 Withdrawn – see AL1_CM_RNR#010.
- 1984

1985 **3.7.1.2 Assurance Level 2**

1986 These criteria apply to passwords, as well as acceptable SAML assertions.

1987 **3.7.1.2.1 Credential Policy and Practices**

1988 These criteria apply to the policy and practices under which credentials are managed.

1989 An enterprise and its specified service must:

1990 **AL2_CM_CPP#010 Credential Policy and Practice Statement**

1991 **Include in its service definition a description of the policy against which it issues**
1992 **credentials and the corresponding practices it applies in their management. At a**
1993 **minimum, the Credential Policy and Practice Statement must specify:**

- 1994 a) **if applicable, any OIDs related to the Practice and Policy Statement;**
1995 b) **how users may subscribe to the service/apply for credentials and how users'**
1996 **credentials will be delivered to them;**
1997 c) **how subscribers acknowledge receipt of tokens and credentials and what**
1998 **obligations they accept in so doing (including whether they consent to**
1999 **publication of their details in credential status directories);**
2000 d) **how credentials may be renewed, modified, revoked, and suspended,**
2001 **including how requestors are authenticated or their identity re-proven;**
2002 e) **what actions a subscriber must take to terminate a subscription;**
2003 f) **how records are retained and archived.**

2004 **AL2_CM_CPP#020 No stipulation**

2005 **AL2_CM_CPP#030 Management Authority**

2006 **Have a nominated management body with authority and responsibility for**
2007 **approving the Credential Policy and Practice Statement and for its implementation.**

2008

2009 **3.7.1.2.2 Security Controls**

2010 An enterprise and its specified service must:

2011 **AL2_CM_CTR#010 Secret revelation**

2012 **Withdrawn.**

2013 **AL2_CM_CTR#020 Protocol threat risk assessment and controls**

2014 Account for at least the following protocol threats **in its risk assessment** and apply
2015 **[omitted] controls that reduce them to acceptable risk levels:**

- 2016 a) password guessing, such that the resistance to an on-line guessing attack against a
2017 selected user/password is at least 1 in 2^{14} (**16,384**);
2018 b) message replay, **showing that it is impractical**;
2019 c) **eavesdropping, showing that it is impractical.**

2020 **AL2_CM_CTR#025 Permitted authentication protocols**

2021 **Permit only the following authentication protocols:**

- 2022 a) **tunneled password;**
2023 b) **zero knowledge-base password;**
2024 c) **SAML assertions.**

2025 **AL2_CM_CTR#028 One-time passwords**

2026 **Use only one-time passwords which:**

- 2027 a) **are generated using an approved block-cipher or hash function to combine a**
2028 **symmetric key, stored on the device, with a nonce;**
2029 b) **derive the nonce from a date and time, or a counter generated on the device;**
2030 c) **have a limited lifetime, in the order of minutes.**
2031

2032 **AL2_CM_CTR#030 System threat risk assessment and controls**

2033 Account for the following system threats **in its risk assessment** and apply **[omitted]**
2034 **controls that reduce them to acceptable risk levels:**

- 2035 a) the introduction of malicious code;
2036 b) compromised authentication arising from insider action;
2037 c) out-of-band attacks by both users and system operators (e.g., the ubiquitous
2038 shoulder-surfing);
2039 d) spoofing of system elements/applications;
2040 e) malfeasance on the part of subscribers and subjects;
2041 f) **intrusions leading to information theft.**

2042 **AL2_CM_CTR#040 Specified Service's Key Management**

2043 **Specify and observe procedures and processes for the generation, storage, and**
2044 **destruction of its own cryptographic keys used for securing the specific service's**
2045 **assertions and other publicized information. At a minimum, these should address:**

- 2046 a) **the physical security of the environment;**
2047 b) **access control procedures limiting access to the minimum number of**
2048 **authorized personnel;**
2049 c) **public-key publication mechanisms;**
2050 d) **application of controls deemed necessary as a result of the service's risk**
2051 **assessment;**

- 2052 e) **destruction of expired or compromised private keys in a manner that**
2053 **prohibits their retrieval, or their archival in a manner that prohibits their**
2054 **reuse;**
2055 f) **applicable cryptographic module security requirements, quoting FIPS 140-2**
2056 **[FIPS140-2] or equivalent, as established by a recognized national technical**
2057 **authority.**
2058

2059 **3.7.1.2.3 Storage of Long-term Secrets**

2060 **AL2_CM_STS#010 Withdrawn**

2061 Withdrawn (AL2_CO_SCO#020 (a) & (b) enforce this requirement).

2062

2063 **3.7.1.2.4 Security-Relevant Event (Audit) Records**

2064 **3.7.1.2.5 No stipulation**

2065 **AL2_CM_OPN#010 Withdrawn**

2066 Withdrawn – see AL2_CM_RNR#010.

2067

2068

2069 **3.7.1.3 Assurance Level 3**

2070 These criteria apply to one-time password devices and soft crypto applications protected
2071 by passwords or biometric controls, as well as cryptographically-signed SAML
2072 assertions.

2073 **3.7.1.3.1 Credential Policy and Practices**

2074 These criteria apply to the policy and practices under which credentials are managed.

2075 An enterprise and its specified service must:

2076 **AL3_CM_CPP#010 Credential Policy and Practice Statement**

2077 Include in its service definition a full description of the policy against which it issues
2078 credentials and the corresponding practices it applies in their issuance. At a minimum,
2079 the Credential Policy and Practice Statement must specify:

- 2080 a) if applicable, any OIDs related to the Credential Policy and Practice Statement;
- 2081 b) how users may subscribe to the service/apply for credentials and how the users'
2082 credentials will be delivered to them;
- 2083 c) how subscribers acknowledge receipt of tokens and credentials and what
2084 obligations they accept in so doing (including whether they consent to publication
2085 of their details in credential status directories);
- 2086 d) how credentials may be renewed, modified, revoked, and suspended, including
2087 how requestors are authenticated or their identity -proven;
- 2088 e) what actions a subscriber must take to terminate a subscription;
- 2089 f) how records are retained and archived..

2090 **AL3_CM_CPP#020 No stipulation**

2091 **AL3_CM_CPP#030 Management Authority**

2092 Have a nominated or appointed high-level management body with authority and
2093 responsibility for approving the Certificate Policy and Certification Practice Statement,
2094 including ultimate responsibility for their proper implementation.

2095

2096 **3.7.1.3.2 Security Controls**

2097 **AL3_CM_CTR#010 No stipulation**

2098 **AL3_CM_CTR#020 Protocol threat risk assessment and controls**

2099 Account for at least the following protocol threats in its risk assessment and apply
2100 controls that reduce them to acceptable risk levels:

- 2101 a) password guessing, such that the resistance to an on-line guessing attack against a
2102 selected user/password is at least 1 in 2^{14} (**16,384**);
- 2103 b) message replay, showing that it is impractical;
- 2104 c) eavesdropping, showing that it is impractical;
- 2105 **d) relying party (verifier) impersonation, showing that it is impractical;**
- 2106 **e) man-in-the-middle attack, showing that it is impractical.**

2107 **The above list shall not be considered to be a complete list of threats to be addressed**
2108 **by the risk assessment.**

2109 **AL3_CM_CTR#025 Permitted authentication protocols**

2110 For non-PKI credentials, permit only the following authentication protocols:

- 2111 a) tunneled password;
- 2112 b) zero knowledge-base password;
- 2113 c) SAML assertions.

2114 **AL3_CM_CTR#030 System threat risk assessment and controls**

2115 Account for the following system threats in its risk assessment and apply controls that
2116 reduce them to acceptable risk levels:

- 2117 a) the introduction of malicious code;
- 2118 b) compromised authentication arising from insider action;
- 2119 c) out-of-band attacks by both users and system operators (e.g., shoulder-surfing);
- 2120 d) spoofing of system elements/applications;
- 2121 e) malfeasance on the part of subscribers and subjects;
- 2122 f) intrusions leading to information theft.

2123 The above list shall not be considered to be a complete list of threats to be addressed by
2124 the risk assessment.

2125 **AL3_CM_CTR#040 Specified Service's Key Management**

2126 Specify and observe procedures and processes for the generation, storage, and destruction
2127 of its own cryptographic keys used for securing the specific service's assertions and other
2128 publicized information. At a minimum, these should address:

- 2129 a) the physical security of the environment;
- 2130 b) access control procedures limiting access to the minimum number of authorized
2131 personnel;
- 2132 c) public-key publication mechanisms;
- 2133 d) application of controls deemed necessary as a result of the service's risk
2134 assessment;
- 2135 e) destruction of expired or compromised private keys in a manner that prohibits
2136 their retrieval or their archival in a manner that prohibits their reuse;
- 2137 f) applicable cryptographic module security requirements, quoting FIPS 140-2
2138 [FIPS140-2] or equivalent, as established by a recognized national technical
2139 authority.
- 2140

2141 **3.7.1.3.3 Storage of Long-term Secrets**

2142 An enterprise and its specified service must:

2143 **AL3_CM_STS#010 Withdrawn**

2144 Withdrawn (AL3_CO_SCO#020 (a) & (b) enforce this requirement).

2145 **AL3_CM_STS#020 Stored Secret Encryption**

2146 Encrypt such shared secret files so that:

- 2147 a) the encryption key for the shared secret file is encrypted under a key held in a
2148 FIPS 140-2 [FIPS140-2] Level 2 or higher validated hardware or software
2149 cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module, or
2150 equivalent, as established by a recognized national technical authority;
- 2151 b) the shared secret file is decrypted only as immediately required for an
2152 authentication operation;
- 2153 c) shared secrets are protected as a key within the boundary of a FIPS 140-2 Level 2
2154 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or
2155 4 cryptographic module and are not exported from the module in plain text, or
2156 equivalent, as established by a recognized national technical authority;
- 2157 d) shared secrets are split by an "n from m" cryptographic secret sharing method.
2158

2159 **3.7.1.3.4 Security-relevant Event (Audit) Records**

2160 These criteria describe the need to provide an auditable log of all events that are pertinent
2161 to the correct and secure operation of the service. The common organizational criteria
2162 applying to provision of an auditable log of all security-related events pertinent to the
2163 correct and secure operation of the service must also be considered carefully. These
2164 criteria carry implications for credential management operations.

2165 In the specific context of a certificate management service, an enterprise and its specified
2166 service must:

2167 **AL3_CM_SER#010 Security event logs**

2168 Ensure that such audit records include:

- 2169 a) the identity of the point of registration (irrespective of whether internal or
2170 outsourced);
2171 b) generation of the subscriber's keys or the evidence that the subscriber was in
2172 possession of both parts of their own key-pair;
2173 c) generation of the subscriber's certificate;
2174 d) dissemination of the subscriber's certificate;
2175 e) any revocation or suspension associated with the subscriber's certificate.
2176

2177 **3.7.1.3.5 Subject options**

2178 **AL3_CM_OPN#010 Changeable PIN/Password**

2179 Withdrawn – see AL3_CM_RNR#010.

2180

2181 **3.7.1.4 Assurance Level 4**

2182 These criteria apply exclusively to cryptographic technology deployed through a Public
2183 Key Infrastructure. This technology requires hardware tokens protected by password or
2184 biometric controls. No other forms of credential are permitted at AL4.

2185 **3.7.1.4.1 Certification Policy and Practices**

2186 These criteria apply to the policy and practices under which certificates are managed.

2187 An enterprise and its specified service must:

2188 **AL4_CM_CPP#010 No stipulation**

2189 **AL4_CM_CPP#020 Certificate Policy/Certification Practice Statement**

2190 **Include in its service definition its full Certificate Policy and the corresponding**
2191 **Certification and Practice Statement. The Certificate Policy and Certification**
2192 **Practice Statement must conform to IETF RFC 3647 (2003-11) [RFC 3647] in their**
2193 **content and scope or be demonstrably consistent with the content or scope of that**
2194 **RFC. At a minimum, the Certificate Policy must specify:**

- 2195 a) **applicable OIDs for each certificate type issued;**
- 2196 b) **how users may subscribe to the service/apply for certificates, and how**
2197 **certificates will be issued to them;**
- 2198 c) **if users present their own keys, how they will be required to demonstrate**
2199 **possession of the private key;**
- 2200 d) **if users' keys are generated for them, how the private keys will be delivered**
2201 **to them;**
- 2202 e) **how subscribers acknowledge receipt of tokens and credentials and what**
2203 **obligations they accept in so doing (including whether they consent to**
2204 **publication of their details in certificate status directories);**
- 2205 f) **how certificates may be renewed, re-keyed, modified, revoked, and**
2206 **suspended, including how requestors are authenticated or their identity**
2207 **proven;**
- 2208 g) **what actions a subscriber must take to terminate their subscription.**

2209 **AL4_CM_CPP#030 Management Authority**

2210 Have a nominated or appointed high-level management body with authority and
2211 responsibility for approving the Certificate Policy and Certification Practice Statement,
2212 including ultimate responsibility for their proper implementation.

2213

2214 **3.7.1.4.2 Security Controls**

2215 An enterprise and its specified service must:

2216 **AL4_CM_CTR#010 No stipulation**

2217 **AL4_CM_CTR#020 Protocol threat risk assessment and controls**

2218 Account for at least the following protocol threats in its risk assessment and apply
2219 controls that reduce them to acceptable risk levels:

- 2220 a) password guessing, showing that there is sufficient entropy;
- 2221 b) message replay, showing that it is impractical;
- 2222 c) eavesdropping, showing that it is impractical;
- 2223 d) relying party (verifier) impersonation, showing that it is impractical;
- 2224 e) man-in-the-middle attack, showing that it is impractical;
- 2225 f) **session hijacking, showing that it is impractical.**

2226 The above list shall not be considered to be a complete list of threats to be addressed by
2227 the risk assessment.

2228 **AL4_CM_CTR#025 No stipulation**

2229 **AL4_CM_CTR#030 System threat risk assessment and controls**

2230 Account for the following system threats in its risk assessment and apply controls that
2231 reduce them to acceptable risk levels:

- 2232 a) the introduction of malicious code;
- 2233 b) compromised authentication arising from insider action;
- 2234 c) out-of-band attacks by both users and system operators (e.g., shoulder-surfing);
- 2235 d) spoofing of system elements/applications;
- 2236 e) malfeasance on the part of subscribers and subjects;
- 2237 f) intrusions leading to information theft.

2238 The above list shall not be considered to be a complete list of threats to be addressed by
2239 the risk assessment.

2240 **AL4_CM_CTR#040 Specified Service's Key Management**

2241 Specify and observe procedures and processes for the generation, storage, and destruction
2242 of its own cryptographic keys used for securing the specific service's assertions and other
2243 publicized information. At a minimum, these should address:

- 2244 a) the physical security of the environment;

- 2245 b) access control procedures limiting access to the minimum number of authorized
2246 personnel;
2247 c) public-key publication mechanisms;
2248 d) application of controls deemed necessary as a result of the service's risk
2249 assessment;
2250 e) destruction of expired or compromised private keys in a manner that prohibits
2251 their retrieval, or their archival in a manner which prohibits their reuse;
2252 f) applicable cryptographic module security requirements, quoting FIPS 140-2
2253 [FIPS140-2] or equivalent, as established by a recognized national technical
2254 authority.
2255

2256 **3.7.1.4.3 Storage of Long-term Secrets**

2257 The enterprise and its specified service must meet the following criteria:

2258 **AL4_CM_STS#010 Stored Secrets**

- 2259 a) Withdrawn (AL4_CO_SCO#020 (a) & (b) enforce this requirement)
2260 b) **apply discretionary access controls that limit access to trusted administrators**
2261 **and to those applications that require access.**

2262 **AL4_CM_STS#020 Stored Secret Encryption**

2263 Encrypt such [omitted] secret files so that:

- 2264 a) the encryption key for the [omitted] secret file is encrypted under a key held in a
2265 FIPS 140-2 [FIPS140-2] Level 2 or higher validated hardware cryptographic
2266 module or any FIPS 140-2 Level 3 or 4 cryptographic module, or equivalent, as
2267 established by a recognized national technical authority;
2268 b) the [omitted] secret file is decrypted only as immediately required for a key
2269 recovery operation;
2270 c) [omitted] secrets are protected as a key within the boundary of a FIPS 140-2
2271 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2
2272 Level 3 or 4 cryptographic module and are not exported from the module in
2273 plaintext, or equivalent, as established by a recognized national technical
2274 authority;
2275 d) escrowed secrets are split by an "*n from m*" cryptographic secret **storing** method.
2276

2277 **3.7.1.4.4 Security-relevant Event (Audit) Records**

2278 These criteria describe the need to provide an auditable log of all events that are pertinent
2279 to the correct and secure operation of the service. The common organizational criteria
2280 relating to the recording of all security-related events must also be considered carefully.
2281 These criteria carry implications for credential management operations.

2282 In the specific context of a certificate management service, an enterprise and its specified
2283 service must:

2284 **AL4_CM_SER#010 Security event logs**

2285 Ensure that such audit records include:

- 2286 a) the identity of the point of registration (irrespective of whether internal or
2287 outsourced);
- 2288 b) generation of the subscriber's keys or evidence that the subscriber was in
2289 possession of both parts of the key-pair;
- 2290 c) generation of the subscriber's certificate;
- 2291 d) dissemination of the subscriber's certificate;
- 2292 e) any revocation or suspension associated with the subscriber's credential.

2293

2294 **3.7.1.4.5 Subject Options**

2295 **AL4_CM_OPN#010 Changeable PIN/Password**

2296 Withdrawn – see AL4_CM_RNR#010.

2297

2298 **3.7.2 Part B - Credential Issuing**

2299 These criteria apply to the verification of the identity of the subject of a credential and
2300 with token strength and credential delivery mechanisms. They address requirements
2301 levied by the use of various technologies to achieve the appropriate AL⁶. These criteria
2302 include by reference all applicable criteria in Section 3.6.

2303 **3.7.2.1 Assurance Level 1**

2304 **3.7.2.1.1 Identity Proofing**

2305 These criteria determine how the enterprise shows compliance with the criteria for
2306 fulfilling identity proofing functions.

2307 The enterprise and its specified service must:

2308 **AL1_CM_IDP#010 Self-managed Identity Proofing**

2309 If the enterprise assumes direct responsibility for identity proofing functions, show, by
2310 direct inclusion, compliance with all applicable identity proofing service assessment
2311 criteria⁷ ([ID-SAC]) for AL1 or higher.

2312 **AL1_CM_IDP#020 Liberty-Recognized outsourced service**

2313 If the enterprise outsources responsibility for identity proofing functions and uses a
2314 service already Liberty-Recognized, show that the service in question has been approved
2315 at AL1 or higher.

2316 **AL1_CM_IDP#030 Non-recognized outsourced service**

2317 If the enterprise outsources responsibility for identity proofing functions, ensure that each
2318 provider of such a service demonstrates compliance with all applicable identity proofing
2319 service assessment criteria for AL1 or higher, and that the enterprise, itself, has in place
2320 controls to ensure the continued fulfillment of those criteria by the provider to which the
2321 functions have been outsourced.

2322 **AL1_CM_IDP#040 Revision to subscriber information**

2323 Provide a means for subscribers to amend their stored information after registration.

2324

⁶ Largely driven by the guidance in NIST SP 800-63 [NIST800-63].

⁷ Not all criteria may be applicable – the precise scope (definition) of the identity proofing performed by a particular service may exclude certain functionality and therefore certain criteria.

2325 **3.7.2.1.2 Credential Creation**

2326 These criteria address the requirements for creation of credentials that can only be used at
2327 AL1. Any credentials/tokens that comply with the criteria stipulated for AL2 and higher
2328 are acceptable at AL1.

2329 An enterprise and its specified service must:

2330 **AL1_CM_CRN#010 Authenticated Request**

2331 Only accept a request to generate a credential and bind it to an identity if the source of the
2332 request can be authenticated as being authorized to perform identity proofing at AL1 or
2333 higher.

2334 **AL1_CM_CRN#020 No stipulation**

2335 **AL1_CM_CRN#030 Credential uniqueness**

2336 Allow the subscriber to select a credential (e.g., UserID) that is verified to be unique
2337 within the specified service's community and assigned uniquely to a single identity
2338 subject.

2339 **3.7.2.1.3 Not used**

2340 **3.7.2.1.4 Not used**

2341

2342

2343 **3.7.2.2 Assurance Level 2**

2344 **3.7.2.2.1 Identity Proofing**

2345 These criteria determine how the enterprise shows compliance with the criteria for
2346 fulfilling identity proofing functions.

2347 The enterprise and its specified service must:

2348 **AL2_CM_IDP#010 Self-managed Identity Proofing**

2349 If the enterprise assumes direct responsibility for identity proofing functions, show, by
2350 direct inclusion, compliance with all applicable identity proofing service assessment
2351 criteria ([ID-SAC]) for AL2 or higher.

2352 **AL2_CM_IDP#020 Liberty-Recognized outsourced service**

2353 If the enterprise outsources responsibility for identity proofing functions and uses a
2354 service already Liberty-Recognized, show that the service in question has been approved
2355 at AL2 or higher **and that its approval has at least 6 months of remaining validity.**

2356 **AL2_CM_IDP#030 Non Liberty-Recognized outsourced service**

2357 If the enterprise outsources responsibility for identity proofing functions, ensure that each
2358 provider of such a service demonstrates compliance with all applicable identity proofing
2359 service assessment criteria for AL2 or higher, and that the enterprise, itself, has in place
2360 controls to ensure the continued fulfillment of those criteria by the provider to which the
2361 functions have been outsourced.

2362 **AL2_CM_IDP#040 Revision to subscriber information**

2363 Provide a means for subscribers to **securely** amend their stored information after
2364 registration, **either by re-proving their identity, as in the initial registration process,**
2365 **or by using their credentials to authenticate their revision.**

2366

2367 **3.7.2.2.2 Credential Creation**

2368 These criteria define the requirements for creation of credentials whose highest use is at
2369 AL2. Credentials/tokens that comply with the criteria stipulated at AL3 and higher are
2370 also acceptable at AL2 and below.

2371 Note, however, that a token and credential required by a higher AL but created according
2372 to these criteria may not necessarily provide that higher level of assurance for the claimed
2373 identity of the subscriber. Authentication can only be provided at the assurance level at
2374 which the identity is proven.

2375 An enterprise and its specified service must:

2376 **AL2_CM_CRN#010 Authenticated Request**

2377 Only accept a request to generate a credential and bind it to an identity if the source of the
2378 request can be authenticated, **i.e., Registration Authority, as being authorized to**
2379 **perform identity proofing at AL2 or higher.**

2380 **AL2_CM_CRN#020 Unique identity**

2381 **Ensure that the identity which relates to a specific applicant is unique within the**
2382 **specified service, including identities previously used and that are now cancelled,**
2383 **other than its re-assignment to the same applicant.**

2384 Guidance: This requirement is intended to prevent identities that may exist in a Relying
2385 Party's access control list from possibly representing a different physical person.

2386 **AL2_CM_CRN#030 Credential uniqueness**

2387 Allow the subscriber to select a credential (e.g., UserID) that is verified to be unique
2388 within the specified service's community and assigned uniquely to a single identity
2389 subject.

2390 **AL2_CM_CRN#035 Convey credential**

2391 **Be capable of conveying the unique identity information associated with a credential**
2392 **to Verifiers and Relying Parties.**

2393 **AL2_CM_CRN#040 Password strength**

2394 **Only allow passwords that, over the life of the password, have resistance to an on-**
2395 **line guessing attack against a selected user/password of at least 1 in 2^{14} (16,384),**
2396 **accounting for state-of-the-art attack strategies, and at least 10 bits of min-entropy⁸.**

2397 **AL2_CM_CRN#050 One-time password strength**

2398 **Only allow password tokens that have a resistance to online guessing attack against**
2399 **a selected user/password of at least 1 in 2^{14} (16,384), accounting for state-of-the-art**
2400 **attack strategies, and at least 10 bits of min-entropy⁸.**

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

-
- 2401 **AL2_CM_CRN#060 Software cryptographic token strength**
- 2402 **Ensure that software cryptographic keys stored on general-purpose devices:**
- 2403 a) **are protected by a key and cryptographic protocol that are evaluated against**
- 2404 **FIPS 140-2 [[FIPS140-2](#)] Level 2, or equivalent, as established by a recognized**
- 2405 **national technical authority;**
- 2406 b) **require password or biometric activation by the subscriber or employ a**
- 2407 **password protocol when being used for authentication.**
- 2408 **AL2_CM_CRN#070 Hardware token strength**
- 2409 **Ensure that hardware tokens used to store cryptographic keys:**
- 2410 a) **employ a cryptographic module that is evaluated against FIPS 140-2**
- 2411 **[[FIPS140-2](#)] Level 1 or higher, or equivalent, as established by a recognized**
- 2412 **national technical authority;**
- 2413 b) **require password or biometric activation by the subscriber or also employ a**
- 2414 **password when being used for authentication.**
- 2415 **AL2_CM_CRN#080 No stipulation**
- 2416 **AL2_CM_CRN#090 Nature of subject**
- 2417 **Record the nature of the subject of the credential (which must correspond to the**
- 2418 **manner of identity proofing performed), i.e., physical person, a named person acting**
- 2419 **on behalf of a corporation or other legal entity, corporation or legal entity, or**
- 2420 **corporate machine entity, in a manner that can be unequivocally associated with the**
- 2421 **credential and the identity that it asserts. If the credential is based upon a**
- 2422 **pseudonym this must be indicated in the credential.**
- 2423 **3.7.2.2.3 Subject Key Pair Generation**
- 2424 No stipulation.
- 2425 **3.7.2.2.4 Credential Delivery**
- 2426 An enterprise and its specified service must:
- 2427 **AL2_CM_CRD#010 Notify Subject of Credential Issuance**
- 2428 **Notify the subject of the credential's issuance and, if necessary, confirm the**
- 2429 **Subject's contact information by:**
- 2430 a) **sending notice to the address of record confirmed during identity proofing**
- 2431 **or;**
- 2432 b) **issuing the credential(s) in a manner that confirms the address of record**
- 2433 **supplied by the applicant during identity proofing or;**

2434 c) **issuing the credential(s) in a manner that confirms the ability of the applicant**
2435 **to receive telephone communications at a fixed-line telephone number or**
2436 **postal address supplied by the applicant during identity proofing.**

2437 **AL2_CM_CRD#015 Confirm Applicant's identity (in person)**

2438 **Prior to delivering the credential, require the Applicant to identify themselves in**
2439 **person in any new electronic transaction (beyond the first transaction or encounter)**
2440 **by either:**

2441 (a) **using a secret which was established during a prior transaction or**
2442 **encounter, or sent to the Applicant's phone number, email address, or**
2443 **physical address of record, or;**

2444 (b) **through the use of a biometric that was recorded during a prior**
2445 **encounter.**

2446 **AL2_CM_CRD#016 Confirm Applicant's identity (remotely)**

2447 **Prior to delivering the credential, require the Applicant to identify themselves in any**
2448 **new electronic transaction (beyond the first transaction or encounter) by presenting**
2449 **a temporary secret which was established during a prior transaction or encounter,**
2450 **or sent to the Applicant's phone number, email address, or physical address of**
2451 **record.**

2452
2453

2454 **3.7.2.3 Assurance Level 3**

2455 **3.7.2.3.1 Identity Proofing**

2456 These criteria in this section determine how the enterprise shows compliance with the
2457 criteria for fulfilling identity proofing functions.

2458 The enterprise and its specified service must:

2459 **AL3_CM_IDP#010 Self-managed Identity Proofing**

2460 If the enterprise assumes direct responsibility for identity proofing functions, show, by
2461 direct inclusion, compliance with all applicable identity proofing service assessment
2462 criteria for **AL3 or AL4**.

2463 **AL3_CM_IDP#020 Liberty-Recognized outsourced service**

2464 If the enterprise outsources responsibility for identity proofing functions and uses a
2465 service already Liberty-Recognized, show that the service in question has been certified
2466 at **AL3 or AL4** and that its approval has at least 6 months of remaining validity.

2467 **AL3_CM_IDP#030 Non Liberty-Recognized outsourced service**

2468 **Not use any non- Liberty-Recognized services for identity proofing unless they can**
2469 **be demonstrated to have satisfied equivalently rigorous requirements established by**
2470 **another scheme recognized by IAEG.**

2471 **AL3_CM_IDP#040 Revision to subscriber information**

2472 Provide a means for subscribers to securely amend their stored information after
2473 registration, either by re-proving their identity as in the initial registration process or by
2474 using their credentials to authenticate their revision. **Successful revision must, where**
2475 **necessary, instigate the re-issuance of the credential.**

2476

2477 **3.7.2.3.2 Credential Creation**

2478 These criteria define the requirements for creation of credentials whose highest use is
2479 AL3. Any credentials/tokens that comply with the criteria stipulated at AL4 are also
2480 acceptable at AL3 and below.

2481 Note, however, that a token and credential type required by a higher AL but created
2482 according to these criteria may not necessarily provide that higher level of assurance for
2483 the claimed identity of the subscriber. Authentication can only be provided at the
2484 assurance level at which the identity is proven.

2485 An enterprise and its specified service must:

2486 **AL3_CM_CRN#010** **Authenticated Request**

2487 Only accept a request to generate a credential and bind it to an identity if the source of the
2488 request, i.e., Registration Authority, can be authenticated as being authorized to perform
2489 identity proofing at AL3 or higher.

2490 **AL3_CM_CRN#020** **Unique identity**

2491 Ensure that the identity which relates to a specific applicant is unique within the specified
2492 service, including identities previously used and that are now cancelled other than its re-
2493 assignment to the same applicant.

2494 **Guidance:** This requirement is intended to prevent identities that may exist in a Relying
2495 Party's access control lists from possibly representing a different physical person.

2496

2497 **AL3_CM_CRN#030** **Credential uniqueness**

2498 Allow the subscriber to select a credential (e.g., UserID) that is verified to be unique
2499 within the specified service's community and assigned uniquely to a single identity
2500 subject.

2501 **AL3_CM_CRN#035** **Convey credential**

2502 Be capable of conveying the unique identity information associated with a credential to
2503 Verifiers and Relying Parties.

2504 **AL3_CM_CRN#040** **PIN/Password strength**

2505 **Not use PIN/password tokens.**

2506 **AL3_CM_CRN#050** **One-time password strength**

2507 Only allow one-time password tokens that:

2508 a) **depend on a symmetric key stored on a personal hardware device evaluated**
2509 **against FIPS 140-2 [FIPS140-2] Level 1 or higher, or equivalent, as**
2510 **established by a recognized national technical authority;**

2511 b) **permit at least 10⁶ possible password values;**

2512 c) **require password or biometric activation by the subscriber.**

2513 **AL3_CM_CRN#060** **Software cryptographic token strength**

2514 Ensure that software cryptographic keys stored on general-purpose devices:

- 2515 a) are protected by a key and cryptographic protocol that are evaluated against
2516 FIPS 14-2 [FIPS140-2] Level 2, or equivalent, as established by a recognized
2517 national technical authority;
2518 b) require password or biometric activation by the subscriber or employ a password
2519 protocol when being used for authentication.

2520 **AL3_CM_CRN#070 Hardware token strength**

2521 Ensure that hardware tokens used to store cryptographic keys:

- 2522 a) employ a cryptographic module that is evaluated against FIPS 140-2 [FIPS140-2]
2523 Level 1 or higher, or equivalent, as established by a recognized national technical
2524 authority;
2525 b) require password or biometric activation by the subscriber or also employ a
2526 password when being used for authentication.

2527 **AL3_CM_CRN#080 Binding of key**

2528 **If the specified service generates the subject's key pair, that the key generation**
2529 **process securely and uniquely binds that process to the certificate generation and**
2530 **maintains at all times the secrecy of the private key, until it is accepted by the**
2531 **subject.**

2532 **AL3_CM_CRN#090 Nature of subject**

2533 Record the nature of the subject of the credential (which must correspond to the manner
2534 of identity proofing performed), i.e., private person, a named person acting on behalf of a
2535 corporation or other legal entity, corporation or legal entity, or corporate machine entity,
2536 in a manner that can be unequivocally associated with the credential and the identity that
2537 it asserts. [Omitted]

2538

2539 **3.7.2.3.3 Subject Key Pair Generation**

2540 An enterprise and its specified service must:

2541 **AL3_CM_SKP#010 Key generation by Specified Service**

2542 **If the specified service generates the subject's keys:**

- 2543 a) **use a FIPS 140-2 [FIPS140-2] compliant algorithm, or equivalent, as**
2544 **established by a recognized national technical authority, that is recognized as**
2545 **being fit for the purposes of the service;**
2546 b) **only create keys of a key length and for use with a FIPS 140-2 [FIPS140-2]**
2547 **compliant public key algorithm, or equivalent, as established by a recognized**

- 2548 national technical authority, recognized as being fit for the purposes of the
2549 service;
2550 c) generate and store the keys securely until delivery to and acceptance by the
2551 subject;
2552 d) deliver the subject's private key in a manner that ensures that the privacy of
2553 the key is not compromised and only the subject has access to the private
2554 key.

2555 **AL3_CM_SKP#020 Key generation by Subject**

2556 If the subject generates and presents its own keys, obtain the subject's written
2557 confirmation that it has:

- 2558 a) used a FIPS 140-2 [FIPS140-2] compliant algorithm, or equivalent, as
2559 established by a recognized national technical authority, that is recognized as
2560 being fit for the purposes of the service;
2561 b) created keys of a key length and for use with a FIPS 140-2 [FIPS140-2]
2562 compliant public key algorithm, or equivalent, as established by a recognized
2563 national technical authority, recognized as being fit for the purposes of the
2564 service.
2565

2566 **3.7.2.3.4 Credential Delivery**

2567 An enterprise and its specified service must:

2568 **AL3_CM_CRD#010, Notify Subject of Credential Issuance**

2569 Notify the subject of the credential's issuance and, if necessary, confirm Subject's contact
2570 information by:

- 2571 a) sending notice to the address of record confirmed during identity proofing, and
2572 either:
2573 i) issuing the credential(s) in a manner that confirms the address of
2574 record supplied by the applicant during identity proofing or;
2575 ii) issuing the credential(s) in a manner that confirms the ability of the
2576 applicant to receive telephone communications at a phone number
2577 supplied by the applicant during identity proofing, while recording
2578 the applicant's voice.

2579 **AL3_CM_CRD#020 Subject's acknowledgement**

2580 Receive acknowledgement of receipt of the credential before it is activated and its
2581 directory status record is published (and thereby the subscription becomes active or
2582 re-activated, depending upon the circumstances of issue).

2583

2584

2585 **3.7.2.4 Assurance Level 4**

2586 **3.7.2.4.1 Identity Proofing**

2587 These criteria determine how the enterprise shows compliance with the criteria for
2588 fulfilling identity proofing functions.

2589 An enterprise and its specified service must:

2590 **AL4_CM_IDP#010 Self-managed Identity Proofing**

2591 If the enterprise assumes direct responsibility for identity proofing functions, show, by
2592 direct inclusion, compliance with all applicable identity proofing service assessment
2593 criteria for [omitted] AL4.

2594 **AL4_CM_IDP#020 Liberty-Recognized outsourced service**

2595 If the enterprise outsources responsibility for identity proofing functions and uses a
2596 service already Liberty-Recognized, show that the service in question has been certified
2597 at [omitted] AL4 and that its approval has at least **12** months of remaining validity.

2598 **AL4_CM_IDP#030 Non Liberty-Recognized outsourced service**

2599 Not use any non- Liberty-Recognized outsourced services for identity proofing unless
2600 they can be demonstrated to have satisfied equivalently rigorous requirements established
2601 by another scheme recognized by IAEG.

2602 **AL4_CM_IDP#040 Revision to subscriber information**

2603 Provide a means for subscribers to securely amend their stored information after
2604 registration, either by re-proving their identity as in the initial registration process or by
2605 using their credentials to authenticate their revision. Successful revision must, where
2606 necessary, instigate the re-issuance of the credential.

2607

2608 **3.7.2.4.2 Credential Creation**

2609 These criteria define the requirements for creation of credentials whose highest use is
2610 AL4.

2611 Note, however, that a token and credential created according to these criteria may not
2612 necessarily provide that level of assurance for the claimed identity of the subscriber.
2613 Authentication can only be provided at the assurance level at which the identity is proven.

2614 An enterprise and its specified service must:

2615 **AL4_CM_CRN#010** **Authenticated Request**

2616 Only accept a request to generate a credential and bind it to an identity if the source of the
2617 request, i.e., Registration Authority, can be authenticated as being authorized to perform
2618 identity proofing at AL4.

2619 **AL4_CM_CRN#020** **Unique identity**

2620 Ensure that the identity which relates to a specific applicant is unique within the specified
2621 service, including identities previously used and that are now cancelled, other than its re-
2622 assignment to the same applicant.

2623 **Guidance:** This requirement is intended to prevent identities that may exist in a Relying
2624 Party's access control lists from possibly representing a different physical person.

2625 **AL4_CM_CRN#030** **Credential uniqueness**

2626 Allow the subscriber to select a credential (e.g., UserID) that is verified to be unique
2627 within the specified service's community and assigned uniquely to a single identity
2628 subject.

2629 **AL4_CM_CRN#035** **Convey credential**

2630 Be capable of conveying the unique identity information associated with a credential to
2631 Verifiers and Relying Parties.

2632 **AL4_CM_CRN#040** **PIN/Password strength**

2633 *Not* use PIN/password tokens.

2634 **AL4_CM_CRN#050** **One-time password strength**

2635 *Not* use one-time password tokens.

2636 **AL4_CM_CRN#060** **Software cryptographic token strength**

2637 *Not* use software cryptographic tokens.

2638 **AL4_CM_CRN#070** **Hardware token strength**

2639 Ensure that hardware tokens used to store cryptographic keys:

- 2640 a) employ a cryptographic module that is validated against FIPS 140-2 [[FIPS140-2](#)]
2641 Level 2 or higher, or equivalent, as determined by a recognized national technical
2642 authority;

- 2643 b) are evaluated against FIPS 140-2 Level 3 or higher, or equivalent, as
2644 determined by a recognized national technical authority, for their physical
2645 security;
2646 c) require password or biometric activation by the subscriber [omitted].

2647 **AL4_CM_CRN#080 Binding of key**

2648 If the specified service generates the subject's key pair, that the key generation process
2649 securely and uniquely binds that process to the certificate generation and maintains at all
2650 times the secrecy of the private key, until it is accepted by the subject.

2651 **AL4_CM_CRN#090 Nature of subject**

2652 Record the nature of the subject of the credential [omitted], i.e., private person, a named
2653 person acting on behalf of a corporation or other legal entity, corporation or legal entity,
2654 or corporate machine entity, in a manner that can be unequivocally associated with the
2655 credential and the identity that it asserts.

2656

2657 **3.7.2.4.3 Subject Key Pair Generation**

2658 An enterprise and its specified service must:

2659 **AL4_CM_SKP#010 Key generation by Specified Service**

2660 If the specified service generates the subject's keys:

- 2661 a) use a FIPS 140-2 [FIPS140-2] compliant algorithm, or equivalent, as established
2662 by a recognized national technical authority, that is recognized as being fit for the
2663 purposes of the service;
2664 b) only create keys of a key length and for use with a FIPS 140-2 [FIPS140-2]
2665 compliant public key algorithm, or equivalent, as established by a recognized
2666 national technical authority, recognized as being fit for the purposes of the
2667 service;
2668 c) generate and store the keys securely until delivery to and acceptance by the
2669 subject;
2670 d) deliver the subject's private key in a manner that ensures that the privacy of the
2671 key is not compromised and only the subject has access to the private key.

2672 **AL4_CM_SKP#020 Key generation by Subject**

2673 If the subject generates and presents its own keys, obtain the subject's written
2674 confirmation that it has:

- 2675 a) used a FIPS 140-2 [FIPS140-2] compliant algorithm, or equivalent, as established
2676 by a recognized national technical authority, that is recognized as being fit for the
2677 purposes of the service;
- 2678 b) created keys of a key length and for use with a FIPS 140-2 [FIPS140-2] compliant
2679 public key algorithm, or equivalent, as established by a recognized national
2680 technical authority, recognized as being fit for the purposes of the service.
2681

2682 **3.7.2.4.4 Credential Delivery**

2683 An enterprise and its specified service must:

2684 **AL4_CM_CRD#010 Notify Subject of Credential Issuance**

2685 Notify the subject of the credential's issuance and, if necessary, confirm Subject's contact
2686 information by:

- 2687 a) sending notice to the address of record confirmed during identity proofing;
- 2688 b) **unless the subject presented with a private key, issuing the hardware token**
2689 **to the subject in a manner that confirms the address of record supplied by**
2690 **the applicant during identity proofing;**
- 2691 c) **issuing the certificate to the subject over a separate channel in a manner that**
2692 **confirms either the address of record or the email address supplied by the**
2693 **applicant during identity proofing.**

2694 **AL4_CM_CRD#020 Subject's acknowledgement**

2695 Receive acknowledgement of receipt of the **hardware token** before it is activated and **the**
2696 **corresponding certificate and** its directory status record are published (and thereby the
2697 subscription becomes active or re-activated, depending upon the circumstances of issue).

2698

2699 **3.7.3 Part C - Credential Renewal and Re-issuing**

2700 These criteria apply to the renewal and re-issuing of credentials. They address
2701 requirements levied by the use of various technologies to achieve the appropriate AL⁹.
2702 These criteria include by reference all applicable criteria in Section 3.6 and the renewal
2703 and re-issuing processes shall comply in all practical senses with the applicable criteria
2704 set forth in Part B of this section.

2705

2706 **3.7.3.1 Assurance Level 1**

2707 **3.7.3.1.1 Renewal/Re-issuance Procedures**

2708 These criteria address general renewal and re-issuance functions, to be exercised as
2709 specific controls in these circumstances while continuing to observe the general
2710 requirements established for initial credential issuance.

2711 An enterprise and its specified service must:

2712 **AL1_CM_RNR#010 Changeable PIN/Password**

2713 Permit subjects to change their PINs/passwords.

2714

2715

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

2716 **3.7.3.2 Assurance Level 2**

2717 **3.7.3.2.1 Renewal/Re-issuance Procedures**

2718 These criteria address general renewal and re-issuance functions, to be exercised as
2719 specific controls in these circumstances while continuing to observe the general
2720 requirements established for initial credential issuance.

2721 An enterprise and its specified service must:

2722 **AL2_CM_RNR#010 Changeable PIN/Password**

2723 Permit subjects to change their [omitted] passwords, **but employ reasonable practices**
2724 **with respect to password resets and repeated password failures.**

2725 **AL2_CM_RNR#020 Proof-of-possession on Renewal/Re-issuance**

2726 **Subjects wishing to change their passwords must demonstrate that they are in**
2727 **possession of the unexpired current token prior to the CSP proceeding to renew or**
2728 **re-issue it.**

2729 **AL2_CM_RNR#030 Renewal/Re-issuance limitations**

- 2730 **a. not renew but may re-issue Passwords;**
2731 **b. neither renew nor re-issue expired tokens;**
2732 **c. conduct all renewal / re-issuance interactions with the Subject over a**
2733 **protected channel such as SSL/TLS.**

2734 Guidance: Renewal is considered as an extension of usability, whereas re-issuance
2735 requires a change.

2736

2737

2738 **3.7.3.3 Assurance Level 3**

2739 **3.7.3.3.1 Renewal/Re-issuance Procedures**

2740 These criteria address general renewal and re-issuance functions, to be exercised as
2741 specific controls in these circumstances while continuing to observe the general
2742 requirements established for initial credential issuance.

2743 An enterprise and its specified service must:

2744 **AL3_CM_RNR#010 Changeable PIN/Password**

2745 Permit subjects to change **the passwords used to activate their credentials.**

2746

2747 *Further criteria may be determined after AL3 comparability assessment against Federal*
2748 *CAF and NIST SP 800-63.*

2749

2750 **3.7.3.4 Assurance Level 4**

2751 **3.7.3.4.1 Renewal/Re-issuance Procedures**

2752 These criteria address general renewal and re-issuance functions, to be exercised as
2753 specific controls in these circumstances while continuing to observe the general
2754 requirements established for initial credential issuance.

2755 An enterprise and its specified service must:

2756 **AL4_CM_RNR#010 Changeable PIN/Password**

2757 Permit subjects to change the passwords used to activate their credentials.

2758

2759 *Further criteria may be determined after AL4 comparability assessment against Federal*
2760 *CAF and NIST SP 800-63.*

2761

2762

2763 **3.7.4 Part D - Credential Revocation**

2764 These criteria deal with credential revocation and the determination of the legitimacy of a
2765 revocation request.

2766 **3.7.4.1 Assurance Level 1**

2767 An enterprise and its specified service must:

2768 **3.7.4.1.1 Not used**

2769 **3.7.4.1.2 Not used**

2770 **3.7.4.1.3 Secure Revocation Request**

2771 This criterion applies when revocation requests between remote components of a service
2772 are made over a secured communication.

2773 An enterprise and its specified service must:

2774 **AL1_CM_SRR#010 Submit Request**

2775 Submit a request for revocation to the Credential Issuer service (function), using a
2776 secured network communication, if necessary.

2777

2778

2779 **3.7.4.2 Assurance Level 2**

2780 **3.7.4.2.1 Revocation Procedures**

2781 These criteria address general revocation functions, such as the processes involved and
2782 the basic requirements for publication.

2783 An enterprise and its specified service must:

2784 **AL2_CM_RVP#010 Revocation procedures**

- 2785 a) **State the conditions under which revocation of an issued credential may**
2786 **occur;**
- 2787 b) **State the processes by which a revocation request may be submitted;**
- 2788 c) **State the persons and organizations from which a revocation request will be**
2789 **accepted;**
- 2790 d) **State the validation steps that will be applied to ensure the validity (identity)**
2791 **of the Revocant, and;**
- 2792 e) **State the response time between a revocation request being accepted and the**
2793 **publication of revised certificate status.**

2794 **AL2_CM_RVP#020 Secure status notification**

2795 **Ensure that published credential status notification information can be relied upon**
2796 **in terms of the enterprise of its origin (i.e., its authenticity) and its correctness (i.e.,**
2797 **its integrity).**

2798 **AL2_CM_RVP#030 Revocation publication**

2799 **Unless the credential will expire automatically within 72 hours:**

2800 **ensure that published credential status notification is revised within 72 hours of the**
2801 **receipt of a valid revocation request, such that any subsequent attempts to use that**
2802 **credential in an authentication shall be unsuccessful.**

2803 **AL2_CM_RVP#040 Verify revocation identity**

2804 **Establish that the identity for which a revocation request is received is one that was**
2805 **issued by the specified service.**

2806 **AL2_CM_RVP#050 Revocation Records**

2807 **Retain a record of any revocation of a credential that is related to a specific identity**
2808 **previously verified, solely in connection to the stated credential. At a minimum,**
2809 **records of revocation must include:**

- 2810 **a) the Revocant's full name;**
- 2811 **b) the Revocant's authority to revoke (e.g., subscriber themselves, someone**
2812 **acting with the subscriber's power of attorney, the credential issuer, law**
2813 **enforcement, or other legal due process);**
- 2814 **c) the Credential Issuer's identity (if not directly responsible for the identity**
2815 **proofing service);**
- 2816 **d) the identity associated with the credential (whether the subscriber's name or**
2817 **a pseudonym);**
- 2818 **e) the reason for revocation.**

2819 **AL2_CM_RVP#060 Record Retention**

2820 **Retain, securely, the record of the revocation process for the duration of the**
2821 **subscriber's account plus 7.5 years.**

2822

2823 **3.7.4.2.2 Verify Revocant's Identity**

2824 Revocation of a credential requires that the requestor and the nature of the request be
2825 verified as rigorously as the original identity proofing. The enterprise should not act on a
2826 request for revocation without first establishing the validity of the request (if it does not,
2827 itself, determine the need for revocation).

2828 In order to do so, the enterprise and its specified service must:

2829 **AL2_CM_RVR#010 Verify revocation identity**

2830 **Establish that the credential for which a revocation request is received was one that**
2831 **was issued by the specified service, applying the same process and criteria as would**
2832 **be applied to an original identity proofing.**

2833 **AL2_CM_RVR#020 Revocation reason**

2834 **Establish the reason for the revocation request as being sound and well founded, in**
2835 **combination with verification of the Revocant, according to AL2_ID_RVR#030,**
2836 **AL2_ID_RVR#040, or AL2_ID_RVR#050.**

2837 **AL2_CM_RVR#030 Verify Subscriber as Revocant**

2838 **When the subscriber seeks revocation of the subscriber's own credential, the**
2839 **enterprise must:**

- 2840 a) **if in person, require presentation of a primary Government Picture ID**
- 2841 **document that shall be electronically verified by a record check against the**
- 2842 **provided identity with the specified issuing authority's records;**
- 2843 b) **if remote:**
 - 2844 i. **electronically verify a signature against records (if available),**
 - 2845 **confirmed with a call to a telephone number of record, or;**
 - 2846 ii. **authenticate an electronic request as being from the same subscriber,**
 - 2847 **supported by a credential at Assurance Level 2 or higher.**

2848 **AL2_CM_RVR#040 CSP as Revocant**

2849 **Where a CSP seeks revocation of a subscriber's credential, the enterprise must**
2850 **establish that the request is either:**

- 2851 a) **from the specified service itself, with authorization as determined by**
- 2852 **established procedures, or;**
- 2853 b) **from the client Credential Issuer, by authentication of a formalized request**
- 2854 **over the established secure communications network.**

2855 **AL2_CM_RVR#050 Verify Legal Representative as Revocant**

2856 **Where the request for revocation is made by a law enforcement officer or**
2857 **presentation of a legal document, the enterprise must:**

- 2858 a) **if in person, verify the identity of the person presenting the request;**
- 2859 b) **if remote:**
 - 2860 i. **in paper/facsimile form, verify the origin of the legal document by a**
 - 2861 **database check or by telephone with the issuing authority, or;**
 - 2862 ii. **as an electronic request, authenticate it as being from a recognized**
 - 2863 **legal office, supported by a credential at Assurance Level 2 or higher.**
 - 2864

2865 **3.7.4.2.3 Secure Revocation Request**

2866 This criterion applies when revocation requests must be communicated between remote
2867 components of the service organization.

2868 An enterprise and its specified service must:

2869 **AL2_CM_SRR#010 Submit Request**

2870 Submit a request for the revocation to the Credential Issuer service (function), using a
2871 secured network communication.

2872

2873 **3.7.4.3 Assurance Level 3**

2874 **3.7.4.3.1 Revocation Procedures**

2875 These criteria address general revocation functions, such as the processes involved and
2876 the basic requirements for publication.

2877 An enterprise and its specified service must:

2878 **AL3_CM_RVP#010 Revocation procedures**

2879 a) State the conditions under which revocation of an issued credential may occur;

2880 b) State the processes by which a revocation request may be submitted;

2881 c) State the persons and organizations from which a revocation request will be
2882 accepted;

2883 d) State the validation steps that will be applied to ensure the validity (identity) of
2884 the Revocant, and;

2885 e) State the response time between a revocation request being accepted and the
2886 publication of revised certificate status.

2887 **AL3_CM_RVP#020 Secure status notification**

2888 Ensure that published credential status notification information can be relied upon in
2889 terms of the enterprise being its origin (i.e., its authenticity) and its correctness (i.e., its
2890 integrity).

2891 **AL3_CM_RVP#030 Revocation publication**

2892 **[Omitted]**Ensure that published credential status notification is revised within **24** hours
2893 of the receipt of a valid revocation request, such that any subsequent attempts to use that
2894 credential in an authentication shall be unsuccessful. **The nature of the revocation**
2895 **mechanism shall be in accord with the technologies supported by the service.**

2896 **AL3_CM_RVP_#040 Verify Revocation Identity**

2897 Establish that the identity for which a revocation request is received is one that was
2898 issued by the specified service.

2899 **AL3_CM_RVP#050 Revocation Records**

2900 Retain a record of any revocation of a credential that is related to a specific identity
2901 previously verified, solely in connection to the stated credential. At a minimum, records
2902 of revocation must include:

- 2903 a) the Revocant's full name;
2904 b) the Revocant's authority to revoke (e.g., subscriber themselves, someone acting
2905 with the subscriber's power of attorney, the credential issuer, law enforcement, or
2906 other legal due process);
2907 c) the Credential Issuer's identity (if not directly responsible for the identity proofing
2908 service);
2909 d) the identity associated with the credential (whether the subscriber's name or a
2910 pseudonym);
2911 e) the reason for revocation.

2912 **AL3_CM_RVP#060 Record Retention**

2913 Retain, securely, the record of the revocation process for a period which is in compliance
2914 with:

- 2915 a) the records retention policy required by AL2_CM_CPP#010, and;
2916 b) applicable legislation;

2917 and which, in addition, must be not less than the duration of the subscriber's account plus
2918 7.5 years.

2919

2920 **3.7.4.3.2 Verify Revocant's Identity**

2921 Revocation of a credential requires that the requestor and the nature of the request be
2922 verified as rigorously as the original identity proofing. The enterprise should not act on a
2923 request for revocation without first establishing the validity of the request (if it does not,
2924 itself, determine the need for revocation).

2925 In order to do so, the enterprise and its specified service must:

2926 **AL3_CM_RVR#010 Verify revocation identity**

2927 Establish that the credential for which a revocation request is received is one that was
2928 initially issued by the specified service, applying the same process and criteria as would
2929 be applied to an original identity proofing.

2930 **AL3_CM_RVR#020 Revocation reason**

2931 Establish the reason for the revocation request as being sound and well founded, in
2932 combination with verification of the Revocant, according to AL3_ID_RVR#030,
2933 AL3_ID_RVR#040, or AL3_ID_RVR#050.

2934 **AL3_CM_RVR#030 Verify Subscriber as Revocant**

2935 When the subscriber seeks revocation of the subscriber's own credential:

- 2936 a) if in-person, require presentation of a primary Government Picture ID document
2937 that shall be electronically verified by a record check against the provided identity
2938 with the specified issuing authority's records;
2939 b) if remote:
2940 i. electronically verify a signature against records (if available), confirmed
2941 with a call to a telephone number of record, or;
2942 ii. as an electronic request, authenticate it as being from the same subscriber,
2943 supported by a credential at Assurance Level **3** or higher.

2944 **AL3_CM_RVR#040 Verify CSP as Revocant**

2945 Where a CSP seeks revocation of a subscriber's credential, establish that the request is
2946 either:

- 2947 a) from the specified service itself, with authorization as determined by established
2948 procedures, or;
2949 b) from the client Credential Issuer, by authentication of a formalized request over
2950 the established secure communications network.

2951 **AL3_CM_RVR#050 Verify Legal Representative as Revocant**

2952 Where the request for revocation is made by a law enforcement officer or presentation of
2953 a legal document:

- 2954 a) if in person, verify the identity of the person presenting the request, or;
2955 b) if remote:
2956 i. in paper/facsimile form, verify the origin of the legal document by a
2957 database check or by telephone with the issuing authority, or
2958 ii. as an electronic request, authenticate it as being from a recognized legal
2959 office, supported by a credential at Assurance Level **3** or higher.
2960

2961 **3.7.4.3.3 Secure Revocation Request**

2962 This criterion applies when revocation requests must be communicated between remote
2963 components of the service organization.

2964 An enterprise and its specified service must:

2965 **AL3_CM_SRR#010 Submit Request**

2966 Submit a request for the revocation to the Credential Issuer service (function), using a
2967 secured network communication.

2968

2969 **3.7.4.4 Assurance Level 4**

2970 **3.7.4.4.1 Revocation Procedures**

2971 These criteria address general revocation functions, such as the processes involved and
2972 the basic requirements for publication.

2973 An enterprise and its specified service must:

2974 **AL4_CM_RVP#010 Revocation procedures**

2975 a) State the conditions under which revocation of an issued certificate may occur;

2976 b) State the processes by which a revocation request may be submitted;

2977 c) State the persons and organizations from which a revocation request will be
2978 accepted;

2979 d) State the validation steps that will be applied to ensure the validity (identity) of
2980 the Revocant, and;

2981 e) State the response time between a revocation request being accepted and the
2982 publication of revised certificate status.

2983 **AL4_CM_RVP#020 Secure status notification**

2984 Ensure that published credential status notification information can be relied upon in
2985 terms of the enterprise of its origin (i.e., its authenticity) and its correctness (i.e., its
2986 integrity).

2987 **AL4_CM_RVP#030 Revocation publication**

2988 Ensure that published credential status notification is revised within **18** hours of the
2989 receipt of a valid revocation request, such that any subsequent attempts to use that
2990 credential in an authentication shall be unsuccessful. The nature of the revocation
2991 mechanism shall be in accordance with the technologies supported by the service.

2992 **AL4_CM_RVP#040 No stipulation**

2993 **AL4_CM_RVP#050 Revocation Records**

2994 Retain a record of any revocation of a credential that is related to a specific identity
2995 previously verified, solely in connection to the stated credential. At a minimum, records
2996 of revocation must include:

2997 a) the Revocant's full name;

- 2998 b) the Revocant's authority to revoke (e.g., subscriber themselves, someone acting
2999 with the subscriber's power of attorney, the credential issuer, law enforcement, or
3000 other legal due process);
3001 c) the Credential Issuer's identity (if not directly responsible for the identity proofing
3002 service);
3003 d) the identity associated with the credential (whether the subscriber's name or a
3004 pseudonym);
3005 e) the reason for revocation.

3006 **AL4_CM_RVP#060 Record Retention**

3007 Retain, securely, the record of the revocation process for a period which is in compliance
3008 with:

- 3009 c) the records retention policy required by AL2_CM_CPP#010, and;
3010 d) applicable legislation;

3011 and which, in addition, must be not less than the duration of the subscriber's account plus
3012 7.5 years.

3013

3014 **3.7.4.4.2 Verify Revocant's Identity**

3015 Revocation of a credential requires that the requestor and the nature of the request be
3016 verified as rigorously as the original identity proofing. The enterprise should not act on a
3017 request for revocation without first establishing the validity of the request (if it does not,
3018 itself, determine the need for revocation).

3019 In order to do so, the enterprise and its specified service must:

3020 **AL4_CM_RVR#010 Verify revocation identity**

3021 Establish that the credential for which a revocation request is received is one that was
3022 initially issued by the specified service, applying the same process and criteria as would
3023 apply to an original identity proofing.

3024 **AL4_CM_RVR#020 Revocation reason**

3025 Establish the reason for the revocation request as being sound and well founded, in
3026 combination with verification of the Revocant, according to AL4_CM_RVR#030,
3027 AL4_CM_RVR#040, or AL4_CM_RVR#050.

3028 **AL4_CM_RVR#030 Verify Subscriber as Revocant**

3029 Where the subscriber seeks revocation of the subscriber's own credential:

- 3030 a) if in person, require presentation of a primary Government Picture ID document
3031 that shall be [Omitted]«but unclear why, since 'electronically' imposes greater
3032 rigour than not??? Cf. AL3» verified by a record check against the provided
3033 identity with the specified issuing authority's records;
3034 b) if remote:
3035 i. verify a signature against records (if available), confirmed with a call to a
3036 telephone number of record, or;
3037 ii. as an electronic request, authenticate it as being from the same subscriber,
3038 supported by a **different** credential at **Assurance Level 4**.

3039 **AL4_CM_RVR#040 Verify CSP as Revocant**

3040 Where a CSP seeks revocation of a subscriber's credential, establish that the request is
3041 either:

- 3042 a) from the specified service itself, with authorization as determined by established
3043 procedures, or;
3044 b) from the client Credential Issuer, by authentication of a formalized request over
3045 the established secure communications network.

3046 **AL4_CM_RVR#050 Verify Legal Representative as Revocant**

3047 Where the request for revocation is made by a law enforcement officer or presentation of
3048 a legal document:

- 3049 a) if in person, verify the identity of the person presenting the request, or;
3050 b) if remote:
3051 i. in paper/facsimile form, verify the origin of the legal document by a
3052 database check or by telephone with the issuing authority;
3053 ii. as an electronic request, authenticate it as being from a recognized legal
3054 office, supported by a different credential at **Assurance Level 4**.

3055 **3.7.4.4.3 Re-keying a credential**

3056 Re-key of a credential requires that the requestor be verified as the subject with as much
3057 rigor as was applied to the original identity proofing. The enterprise should not act on a
3058 request for re-key without first establishing that the requestor is identical to the subject.

3059 In order to do so, the enterprise and its specified service must:

3060 **AL4_CM_RKY#010 Verify Requestor as Subscriber**

3061 **Where the subscriber seeks a re-key for the subscriber's own credential:**

- 3062 a) **if in-person, require presentation of a primary Government Picture ID**
3063 **document that shall be verified by a record check against the provided**
3064 **identity with the specified issuing authority's records;**
3065 b) **if remote:**

- 3066 i. **verify a signature against records (if available), confirmed with a call**
3067 **to a telephone number of record, or;**
3068 ii. **authenticate an electronic request as being from the same subscriber,**
3069 **supported by a different credential at Assurance Level 4.**
3070

3071 **AL4_CM_RKY#020 Re-key requests other than subscriber**

3072 **Re-key requests from any parties other than the subscriber must not be accepted.**

3073 **3.7.4.4.4 Secure Revocation/Re-key Request**

3074 This criterion applies when revocation **or re-key** requests must be communicated
3075 between remote components of the service organization.

3076 The enterprise and its specified service must:

3077 **AL4_CM_SRR#010 Submit Request**

3078 Submit a request for the revocation to the Credential Issuer service (function), using a
3079 secured network communication.

3080

3081 **3.7.5 Part E - Credential Status Management**

3082 These criteria deal with credential status management, such as the receipt of requests for
3083 new status information arising from a new credential being issued or a revocation or other
3084 change to the credential that requires notification. They also deal with the provision of
3085 status information to requesting parties (Verifiers, Relying Parties, courts and others
3086 having regulatory authority, ...) having the right to access such information.

3087 **3.7.5.1 Assurance Level 1**

3088 **3.7.5.1.1 Status Maintenance**

3089 An enterprise and its specified service must:

3090 **AL1_CM_CSM#010 Maintain Status Record**

3091 Maintain a record of the status of all credentials issued.

3092 **AL1_CM_CSM#020 No stipulation**

3093 **AL1_CM_CSM#030 No stipulation**

3094 **AL1_CM_CSM#040 Status Information Availability**

3095 Provide, with 95% availability, a secure automated mechanism to allow relying parties to
3096 determine credential status and authenticate the subject's identity.

3097

3098

3099 **3.7.5.2 Assurance Level 2**

3100 **3.7.5.2.1 Status Maintenance**

3101 An enterprise and its specified service must:

3102 **AL2_CM_CSM#010 Maintain Status Record**

3103 Maintain a record of the status of all credentials issued.

3104 **AL2_CM_CSM#020 Validation of Status Change Requests**

3105 **Authenticate all requestors seeking to have a change of status recorded and**
3106 **published and validate the requested change before considering processing the**
3107 **request. Such validation should include:**

- 3108 a) **the requesting source as one from which the specified service expects to**
3109 **receive such requests;**
3110 b) **if the request is not for a new status, the credential or identity as being one**
3111 **for which a status is already held.**

3112 **AL2_CM_CSM#030 Revision to Published Status**

3113 **Process authenticated requests for revised status information and have the revised**
3114 **information available for access within a period of 72 hours.**

3115 **AL2_CM_CSM#040 Status Information Availability**

3116 Provide, with 95% availability, a secure automated mechanism to allow relying parties to
3117 determine credential status and authenticate the subject's identity.

3118 **AL2_CM_CSM#050 Inactive Credentials**

3119 **Disable any credential that has not been successfully used for authentication during**
3120 **a period of 18 months.**

3121

3122

3123 **3.7.5.3 Assurance Level 3**

3124 **3.7.5.3.1 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 subject'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

3146

3147 **3.7.5.4 Assurance Level 4**

3148 **3.7.5.4.1 Status Maintenance**

3149 An enterprise and its specified service must:

3150 **AL4_CM_CSM#010 Maintain Status Record**

3151 Maintain a record of the status of all credentials issued.

3152 **AL4_CM_CSM#020 Validation of Status Change Requests**

3153 Authenticate all requestors seeking to have a change of status recorded and published and
3154 validate the requested change before considering processing the request. Such validation
3155 should include:

- 3156 a) the requesting source as one from which the specified service expects to receive
3157 such requests;
3158 b) if the request is not for a new status, the credential or identity as being one for
3159 which a status is already held.

3160 **AL4_CM_CSM#030 Revision to Published Status**

3161 Process authenticated requests for revised status information and have the revised
3162 information available for access within a period of 72 hours.

3163 **AL4_CM_CSM#040 Status Information Availability**

3164 Provide, with 99% availability, a secure automated mechanism to allow relying parties to
3165 determine credential status and authenticate the subject's identity.

3166 **AL4_CM_CSM#050 Inactive Credentials**

3167 Disable any credential that has not been successfully used for authentication during a
3168 period of 18 months.

3169

3170 **3.7.6 Part F - Credential Validation/Authentication**

3171 These criteria apply to credential validation and identity authentication.

3172 **3.7.6.1 Assurance Level 1**

3173 **3.7.6.1.1 Assertion Security**

3174 An enterprise and its specified service must:

3175 **AL1_CM_ASS#010 Validation and Assertion Security**

3176 Provide validation of credentials to a Relying Party using a protocol that:

- 3177 a) requires authentication of the specified service or of the validation source;
- 3178 b) ensures the integrity of the authentication assertion;
- 3179 c) protects assertions against manufacture, modification and substitution, and
- 3180 secondary authenticators from manufacture;

3181 and which, specifically:

- 3182 d) creates assertions which are specific to a single transaction;
- 3183 e) where assertion references are used, generates a new reference whenever a new
- 3184 assertion is created;
- 3185 f) when an assertion is provided indirectly, either signs the assertion or sends it via a
- 3186 protected channel, using a strong binding mechanism between the secondary
- 3187 authenticator and the referenced assertion;
- 3188 g) requires the secondary authenticator to:
 - 3189 i) be signed when provided directly to Relying Party, or
 - 3190 ii) have a minimum of 64 bits of entropy when provision is indirect (i.e.
 - 3191 through the credential user).

3192 **AL1_CM_ASS#015 No stipulation**

3193 **AL1_CM_ASS#020 No Post Authentication**

3194 *Not* authenticate credentials that have been revoked.

3195 **AL1_CM_ASS#030 Proof of Possession**

3196 Use an authentication protocol that requires the claimant to prove possession and control
3197 of the authentication token.

3198 **AL1_CM_ASS#040 Assertion Lifetime**

3199 Generate assertions so as to indicate and effect their expiration within:

- 3200 a) 12 hours after their creation, where the service shares a common internet domain
- 3201 with the Relying Party;
- 3202 b) five minutes after their creation, where the service does not share a common
- 3203 internet domain with the Relying Party.
- 3204
- 3205

3206 **3.7.6.2 Assurance Level 2**

3207 **3.7.6.2.1 Assertion Security**

3208 An enterprise and its specified service must:

3209 **AL2_CM_ASS#010 Validation and Assertion Security**

3210 Provide validation of credentials to a Relying Party using a protocol that:

- 3211 a) requires authentication of the specified service, itself, or of the validation source;
- 3212 b) ensures the integrity of the authentication assertion;
- 3213 c) protects assertions against manufacture, modification, **substitution and**
- 3214 **disclosure**, and secondary authenticators from manufacture, **capture and replay**;
- 3215 d) **uses approved cryptography techniques**;

3216 and which, specifically:

- 3217 e) creates assertions which are specific to a single transaction;
- 3218 f) where assertion references are used, generates a new reference whenever a new
- 3219 assertion is created;
- 3220 g) when an assertion is provided indirectly, either signs the assertion or sends it via a
- 3221 protected channel, using a strong binding mechanism between the secondary
- 3222 authenticator and the referenced assertion;
- 3223 h) **send assertions either via a channel mutually-authenticated with the Relying**
- 3224 **Party, or signed and encrypted for the Relying Party**;
- 3225 i) requires the secondary authenticator to:
 - 3226 i) be signed when provided directly to Relying Party, or
 - 3227 ii) have a minimum of 64 bits of entropy when provision is indirect (i.e.
 - 3228 through the credential user);
 - 3229 **iii) be transmitted to the Subject through a protected channel which is**
 - 3230 **linked to the primary authentication process in such a way that**
 - 3231 **session hijacking attacks are resisted**;
 - 3232 **iv) not be subsequently transmitted over an unprotected channel or to an**
 - 3233 **unauthenticated party while it remains valid.**

3234 **AL2_CM_ASS#015 No False Authentication**

3235 **Employ techniques which ensure that system failures do not result in ‘false positive**

3236 **authentication’ errors.**

3237 **AL2_CM_ASS#020 No Post Authentication**

3238 *Not* authenticate credentials that have been revoked **unless the time of the transaction**

3239 **for which verification is sought precedes the time of revocation of the credential.**

3240 **AL2_CM_ASS#030 Proof of Possession**

3241 Use an authentication protocol that requires the claimant to prove possession and control
3242 of the authentication token.

3243 **AL2_CM_ASS#040 Assertion Lifetime**

3244 Generate assertions so as to indicate and effect their expiration:

3245 a) 12 hours after their creation, where the service shares a common internet domain
3246 with the Relying Party;

3247 b) five minutes after their creation, where the service does not share a common
3248 internet domain with the Relying Party.

3249

3250

3251 **3.7.6.3 Assurance Level 3**

3252 **3.7.6.3.1 Assertion Security**

3253 An enterprise and its specified service must:

3254 **AL3_CM_ASS#010 Validation and Assertion Security**

3255 Provide validation of credentials to a Relying Party using a protocol that:

- 3256 a) requires authentication of the specified service, itself, or of the validation source;
- 3257 b) ensures the integrity of the authentication assertion.

3258 **AL3_CM_ASS#015 No False Authentication**

3259 Employ techniques which ensure that system failures do not result in 'false positive
3260 authentication' errors.

3261 **AL3_CM_ASS#020 Post Authentication**

3262 *Not* authenticate credentials that have been revoked unless the time of the transaction for
3263 which verification is sought precedes the time of revocation of the credential.

3264 **AL3_CM_ASS#030 Proof of Possession**

3265 Use an authentication protocol that requires the claimant to prove possession and control
3266 of the authentication token.

3267 **AL3_CM_ASS#040 Assertion Lifetime**

3268 **For non-cryptographic credentials**, generate assertions so as to indicate and effect their
3269 expiration 12 hours after their creation; **otherwise, notify the relying party of how often**
3270 **the revocation status sources are updated.**

3271

3272

3273 **3.7.6.4 Assurance Level 4**

3274 **3.7.6.4.1 Assertion Security**

3275 An enterprise and its specified service must:

3276 **AL4_CM_ASS#010 Validation and Assertion Security**

3277 Provide validation of credentials to a Relying Party using a protocol that:

- 3278 a) requires authentication of the specified service, itself, or of the validation source;
- 3279 b) ensures the integrity of the authentication assertion.

3280 **AL4_CM_ASS#015 No False Authentication**

3281 Employ techniques which ensure that system failures do not result in 'false positive
3282 authentication' errors.

3283 **AL4_CM_ASS#020 Post Authentication**

3284 *Not* authenticate credentials that have been revoked unless the time of the transaction for
3285 which verification is sought precedes the time of revocation of the credential.

3286 **AL4_CM_ASS#030 Proof of Possession**

3287 Use an authentication protocol that requires the claimant to prove possession and control
3288 of the authentication token.

3289 **AL4_CM_ASS#040 Assertion Lifetime**

3290 **[Omitted]** Notify the relying party of how often the revocation status sources are
3291 updated.

3292

3293

3294 **3.7.7 Compliance Tables**

3295 Use the following tables to correlate criteria for a particular Assurance Level (AL) and
3296 the evidence offered to support compliance.

3297 Service providers preparing for an assessment can use the table appropriate to the AL at
3298 which they are seeking approval to correlate evidence with criteria or to justify non-
3299 applicability (e.g., "specific service types not offered").

3300 Assessors can use the tables to record the steps in their assessment and their
3301 determination of compliance or failure.

3302 **Table 3-9 CM-SAC - AL1 Compliance**

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

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

3303

3304

3305

Table 3-10 CM-SAC - AL2 Compliance

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

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

3306

3307

3308

Table 3-11 CM-SAC - AL3 Compliance

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

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

3309

3310

Table 3-12 CM-SAC - AL4 Compliance

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

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

3311

3312 4 IAEG Glossary

3313 *Accreditation.* The process used to achieve formal recognition that an organization has
3314 agreed to the IAEG operating rules and is competent to perform assessments using
3315 the Service Assessment Criteria.

3316 *AL.* See *Assurance Level*

3317 *Applicant.* An individual or person acting as a proxy for a machine or corporate entity
3318 who is the subject of an identity proofing process.

3319 *Approval.* The process by which the IAEG Board accepts the compliance of a certified
3320 service and the CSP responsible for that service commits to upholding the IAEG
3321 Rules.

3322 *Approved encryption.* Any cryptographic algorithm or method specified in a FIPS or a
3323 NIST recommendation or equivalent, as established by a recognized national
3324 technical authority. Refer to <http://csrc.nist.gov/cryptval/>

3325 *Approved service.* A certified service which has been granted an approval by the IAEG
3326 Board.

3327 *Assertion.* A statement from a verifier to a relying party that contains identity or other
3328 information about a subscriber.

3329 *Assessment.* A process used to evaluate an electronic trust service and the service
3330 provider using the requirements specified by one or more Service Assessment
3331 Criteria for compliance with all applicable requirements.

3332 *Assessor.* A person or corporate entity who performs an assessment.

3333 *Assurance level (AL).* A degree of certainty that a claimant has presented a credential
3334 that refers to the claimant's identity. Each assurance level expresses a degree of
3335 confidence in the process used to establish the identity of the individual to whom
3336 the credential was issued and a degree of confidence that the individual who uses
3337 the credential is the individual to whom the credential was issued. The four
3338 assurance levels are:

3339 Level 1: Little or no confidence in the asserted identity's validity

3340 Level 2: Some confidence in the asserted identity's validity

3341 Level 3: High confidence in the asserted identity's validity

3342 Level 4: Very high confidence in the asserted identity's validity

3343 *Attack.* An attempt to obtain a subscriber's token or to fool a verifier into believing that
3344 an unauthorized individual possesses a claimant's token.

3345 *Attribute.* A property associated with an individual.

3346 *Authentication.* Authentication simply establishes identity, not what that identity is

- 3347 authorized to do or what access privileges he or she has.
- 3348 *Authentication protocol.* A well-specified message exchange process that verifies
3349 possession of a token to remotely authenticate a claimant. Some authentication
3350 protocols also generate cryptographic keys that are used to protect an entire
3351 session, so that the data transferred in the session is cryptographically protected.
- 3352 *Authorization.* Process of deciding what an individual ought to be allowed to do.
- 3353 *Bit.* A binary digit: 0 or 1
- 3354 *Brand.* See IAEG Branded Credential.
- 3355 *CAP:* Credential Assessment Profile
- 3356 *Certification.* The IAEG's affirmation that a particular credential service provider can
3357 provide a particular credential service at a particular assurance level.
- 3358 *Claimant.* A party whose identity is to be verified.
- 3359 *Certification Body.* An organization which has been deemed competent to perform
3360 assessments of a particular type. Such assessments may be formal evaluations or
3361 testing and be based upon some defined set of standards or other criteria.
- 3362 *Certified service.* An electronic trust service which has been assessed by an IAEG-
3363 recognized certification body and found to be compliant with the applicable
3364 SACs.
- 3365 *Communicate.* Information is communicated to a party if it is passed to them directly, for
3366 example by hand, by email or by post. This is an act of deliberately 'pushing'
3367 information towards a known party. Cf. '**Make available**'
- 3368 *Credential.* An object to be verified when presented in an authentication transaction. A
3369 credential can be bound in some way to the individual to whom it was issued, or it
3370 can be a bearer credential. Electronic credentials are digital documents that bind
3371 an identity or an attribute to a subscriber's token.
- 3372 *Credential management.* A service that supports the lifecycle of identity credentials from
3373 issuance to revocation, including renewal, status checks and authentication
3374 services.
- 3375 *Credential service.* A type of electronic trust service that supports the verification of
3376 identities (identity proofing), the issuance of identity related
3377 assertions/credentials/tokens, and the subsequent management of those credentials
3378 (for example, renewal, revocation and the provision of related status and
3379 authentication services).
- 3380 *Credential service provider (CSP).* An electronic trust service provider that operates one
3381 or more credential services. A CSP can include a Registration Authority.
- 3382 *CSP.* See *credential service provider*.

-
- 3383 *Cryptographic token.* A token for which the secret is a cryptographic key.
- 3384 *Electronic credentials.* Digital documents used in authentication that bind an identity or
3385 an attribute to a subscriber's token.
- 3386 *Electronic Trust service (ETS).* A service that enhances trust and confidence in electronic
3387 transactions, typically but not necessarily using cryptographic techniques or
3388 involving confidential material such as PINs and passwords.
- 3389 *Electronic Trust service provider (ETSP).* An entity that provides one or more electronic
3390 trust services.
- 3391 *ETS.* See electronic trust service.
- 3392 *ETSP.* See electronic trust service provider,
- 3393 *Federal Information Processing Standards ([FIPS]).* Standards and guidelines issued by
3394 the National Institute of Standards and Technology (NIST) for use government-
3395 wide in the United States. NIST develops FIPS when the U.S. Federal
3396 government has compelling requirements, such as for security and
3397 interoperability, for which no industry standards or solutions are acceptable.
- 3398 *Federated identity management.* A system that allows individuals to use the same user
3399 name, password, or other personal identification to sign on to the networks of
3400 more than one enterprise in order to conduct transactions.
- 3401 *Federation Operator.* An individual or group that defines standards for its respective
3402 federation, or trust community and evaluates participation in the community or
3403 network to ensure compliance with policy, including the ability to request audits
3404 of participants for verification.
- 3405 *FIPS.* See Federal Information Processing Standards.
- 3406 *IAEG.* See *Identity Assurance Expert Group*
- 3407 *Liberty-Accredited Assessor.* A body that has fulfilled the applicable requirements of the
3408 Liberty Accreditation and Certification Scheme and been granted an accreditation
3409 to perform assessments against Service Assessment Criteria, at the specified
3410 assurance level(s).
- 3411 *Liberty-Recognized Credential Service.* A Credential / Identity Management Service
3412 operated by an Organization that has signed the Liberty Service Provider
3413 Agreement, and that has been Certified by a Liberty-Accredited Assessor as being
3414 conformant to the applicable Service Assessment Criteria, according to the
3415 service type and selected Assurance Level(s).
- 3416 *Identification.* Process of using claimed or observed attributes of an individual to infer
3417 who the individual is.
- 3418 *Identifier.* Something that points to an individual, such as a name, a serial number, or
3419 some other pointer to the party being identified.

- 3420 *Identity*. A unique name for single person. Because a person's legal name is not
3421 necessarily unique, identity must include enough additional information (for
3422 example, an address or some unique identifier such as an employee or account
3423 number) to make a unique name.
- 3424 *Identity Assurance Expert Group (IAEG)*. The multi-industry Liberty Alliance
3425 partnership working on enabling interoperability among public and private
3426 electronic identity authentication systems.
- 3427 *Identity Assurance Framework (IAF)*. The body of work that collectively defines the
3428 industry-led self-regulatory framework for electronic trust services in the United
3429 States and around the globe, as operated by the IAEG. The Identity Assurance
3430 Framework includes descriptions of criteria, rules, procedures, processes, and
3431 other documents.
- 3432 *Identity authentication*. Process of establishing an understood level of confidence that an
3433 identifier refers to an identity. It may or may not be possible to link the
3434 authenticated identity to an individual.
- 3435 *Identity binding*. The extent to which an electronic credential can be trusted to be a proxy
3436 for the entity named in it.
- 3437 *Identity Proofing*. The process by which identity related information is validated so as to
3438 identify a person with a degree of uniqueness and certitude sufficient for the
3439 purposes for which that identity is to be used.
- 3440 *Identity Proofing policy*. A set of rules that defines identity proofing requirements
3441 (required evidence, format, manner of presentation, validation), records actions
3442 required of the registrar, and describes any other salient aspects of the identity
3443 proofing function that are applicable to a particular community or class of
3444 applications with common security requirements. An identity proofing policy is
3445 designed to accomplish a stated assurance level.
- 3446 *Identity Proofing service provider*. An electronic trust service provider which offers, as a
3447 standalone service, the specific electronic trust service of identity proofing. This
3448 service provider is sometimes referred to as a Registration Agent/Authority (RA).
- 3449 *Identity Proofing practice statement*. A statement of the practices that an identity
3450 proofing service provider employs in providing its services in accordance with the
3451 applicable identity proofing policy.
- 3452 *Information Security Management Systems (ISMS)*. A system of management concerned
3453 with information security. The key concept of ISMS is the design, implement,
3454 and maintain a coherent suite of processes and systems for effectively managing
3455 information security, thus ensuring the confidentiality, integrity, and availability
3456 of information assets and minimizing information security risks.
- 3457 *Issuer*. Somebody or something that supplies or distributes something officially.

- 3458 *Level of assurance.* See assurance level.
- 3459 *Make available.* Information is made available to a party if it is published in a form
3460 accessible to the party in a place that the party might reasonably expect to find it,
3461 for example in a clearly identifiable page on the CSP's website. It is also made
3462 available if it is provided promptly on request through a mechanism that is widely
3463 published and easy to find and use. Finally, it is also made available if it is
3464 directly **Communicated** to the party (cf. '**Communicate**').
- 3465 *Network.* An open communications medium, typically, the Internet, that is used to
3466 transport messages between the claimant and other parties.
- 3467 *OID.* Object identifier.
- 3468 *Password.* A shared secret character string used in authentication protocols. In many
3469 cases the claimant is expected to memorize the password.
- 3470 *Practice statement.* A formal statement of the practices followed by an authentication
3471 entity (e.g., RA, CSP, or verifier) that typically defines the specific steps taken to
3472 register and verify identities, issue credentials and authenticate claimants.
- 3473 *Public key.* The public part of the asymmetric key pair that is typically used to verify
3474 signatures or encrypt data.
- 3475 *Public key infrastructure (PKI).* A set of technical and procedural measures used to
3476 manage public keys embedded in digital certificates. The keys in such certificates
3477 can be used to safeguard communication and data exchange over potentially
3478 unsecure networks.
- 3479 *Registration.* An entry in a register, or somebody or something whose name or
3480 designation is entered in a register.
- 3481 *Relying party.* An entity that relies upon a subscriber's credentials, typically to process a
3482 transaction or grant access to information or a system.
- 3483 *Role.* The usual or expected function of somebody or something, or the part somebody or
3484 something plays in a particular action or event.
- 3485 *SAC.* See Service Assessment Criteria.
- 3486 *Security.* A collection of safeguards that ensures the confidentiality of information,
3487 protects the integrity of information, ensures the availability of information,
3488 accounts for use of the system, and protects the system(s) and/or network(s) used
3489 to process the information.
- 3490 *Service Assessment Criteria (SAC).* A set of requirements levied upon specific
3491 organizational and other functions performed by electronic trust services and
3492 service providers. Services and service providers must comply with all applicable
3493 criteria to qualify for IAEG approval.
- 3494 *Signatory.* A party that opts into and agrees to be bound by the IAEG Rules according to

- 3495 the specified procedures.
- 3496 *Specified service.* The electronic trust service which, for the purposes of an IAEG
3497 assessment, is the subject of criteria set out in a particular SAC, or in an
3498 application for assessment, in a grant of an approval or other similar usage as may
3499 be found in various IAEG documentation.
- 3500 *Subject.* An entity that is able to use an electronic trust service subject to agreement with
3501 an associated subscriber. A subject and a subscriber can be the same entity.
- 3502 *Subscriber.* A party that has entered into an agreement to use an electronic trust service.
3503 A subscriber and a subject can be the same entity.
- 3504 *Threat.* An adversary that is motivated and capable to violate the security of a target and
3505 has the capability to mount attacks that will exploit the target's vulnerabilities.
- 3506 *Token.* Something that a claimant possesses and controls (typically a key or password)
3507 that is used to authenticate the claimant's identity.
- 3508 *Verification.* Establishment of the truth or correctness of something by investigation of
3509 evidence.

3510 5 Publication Acknowledgements

3511

3512 The IAEG would like to thank the following working group chairs and vice chairs for
3513 their commitment and dedication to the Liberty Identity Assurance Framework.

3514

3515 IAEG Co-Chair: Myisha Frazier-Mcelveen, CitiGroup

3516 IAEG Co-Chair: Rich Furr, SAFE Bio Pharma

3517 IAEG Co-Chair: Nigel Tedeschi, British Telecom

3518 Previous IAEG Co-Chair: Frank Villavicencio, CitiGroup

3519

3520 Previous IASIG Chair: Peter Alterman, Federal General Services Administration, Office
3521 of Government-Wide Policy

3522

3523 Interim Chair: James Lewis, The Center for Strategic and International Studies

3524 Interim Vice Chair: David Temoshok, U.S. General Services Administration

3525

3526 Business Requirements and Processes Work Group

3527 Chair: Linda G. Elliot, PingID Network

3528 Vice Chair: Thomas Greco, beTRUSTed

3529

3530 Credential Services Assessment Criteria and Levels of Assurance Work Group

3531 Chair: Robert J. Schlecht, Mortgage Bankers Association of America

3532 Vice Chair: Von Harrison, U.S. General Services Administration

3533

3534 Credential Services Assessment Criteria Sub Work

3535 Chair: Nancy Black, HollenGroup

3536 Vice Chair: Richard G. Wilsher, Zygma LLC

3537

3538 Levels of Assurance Sub Work Group

3539 Chair: Peter Alterman, Federal General Services Administration, Office of Government-
3540 Wide Policy

3541 Vice Chair: Noel Nazario, KPMG LLP

3542

3543 Interoperability Sub Work Group

3544 Chair: William E. Burr, National Institute of Standards and Technology

3545 Vice Chair: Kurt Van Etten, eBay, Inc.

3546

3547 Evaluation, Accreditation and Compliance Work Group

3548 Chair: Gary Glickman, Giesecke & Devrient Cardtech, Inc.

3549 Vice Chair: Cornelia Chebinou, National Association of State Auditors, Comptrollers and

- 3550 Treasurers
- 3551
- 3552 EAP Governance Work Group
- 3553 Chair: Paula Arcioni, State of New Jersey, Office of Information Technology
- 3554 Vice Chair: Roger J. Cochetti, CompTIA
- 3555
- 3556 Consultants
- 3557 Russ Cutler, Confiance Advisors, LLC
- 3558 Yuriy Dzambasow, A&N Associates, Inc.
- 3559 Nathan Faut, KPMG
- 3560 Dan Greenwood, Commonwealth of Massachusetts
- 3561 Rebecca Nielsen, Booz Allen Hamilton
- 3562 Richard G. Wilsher, Zyigma LLC
- 3563
- 3564 Members of the various work groups include:
- 3565 Shin Adachi, NTT
- 3566 Khaja Ahmed, Microsoft Corporation
- 3567 Michael A. Aisenberg, VeriSign, Inc.
- 3568 Peter Alterman, National Institutes of Health
- 3569 Paula Arcioni, State of New Jersey, Office of Information Technology
- 3570 Jonathan Askins, ACXIOM Corporation
- 3571 Asaf Awan, Parkweb Associates
- 3572 Stefano Baroni, SETECS
- 3573 Paul Barrett, Real User Corporation
- 3574 Nancy Black, Hollen Group
- 3575 Debb Blanchard, Enspier Technologies/GDT
- 3576 Warren Blosjo, 3Factor
- 3577 Daniel Blum, Burton Group
- 3578 Iana Bohmer, Northrop Grumman Information Technology
- 3579 Christine Borucke, Electronic Data Systems
- 3580 Kirk Brafford, SSP-Litronic, Inc.
- 3581 Mayi Canales, M Squared Strategies, Inc.
- 3582 Richard Carter, American Association of Motor Vehicles Administration
- 3583 Kim Cartwright, Experian
- 3584 James A. Casey, NeuStar, Inc.
- 3585 Ray Cavanaugh, Entegrity Solutions
- 3586 Chuck Chamberlain, U.S. Postal Service
- 3587 Cornelia Chebinou, National Association of State Auditors, Comptrollers and Treasurers
- 3588 Rebecca Chisolm, Sun Microsystems Federal
- 3589 Philippe Clement, France Telecom
- 3590 Roger J. Cochetti, CompTIA
- 3591 Dan Combs, Global Identity Solutions
- 3592 John Cornell, U.S. General Services Administration

3593 Sarah Currier, CheckFree Corporation
3594 Chris Daly, IBM Corporation
3595 Peter Davis, Neustar
3596 Kathy DiMaggio, Sigaba Corporation
3597 Yuriy Dzambasow, A&N Associates, Inc.
3598 Josh Elliott, American Management Systems
3599 Clay Epstein, Indentrus LLC
3600 Irving R. Gilson, Department of Defense
3601 Gary Glickman, Giesecke & Devrient Cardtech, Inc.
3602 James A. Gross, Wells Fargo
3603 Kirk R. Hall, GeoTrust
3604 Von Harrison, U.S. General Services Administration
3605 Christopher Hankin, Sun Microsystems, Inc.
3606 Patrick Harding, Ping Identity
3607 Jane Hennessey, Wells Fargo
3608 Helen Hill, HIMSS
3609 Michael Horkey, Global Identity Solutions
3610 Katherine M. Hollis, Electronic Data Systems
3611 Robert Housel, National City Corporation
3612 Burt Kaliski, RSA Security, Inc.
3613 Shannon Kellog, RSA Security, Inc.
3614 James Kobielus, Burton Group
3615 Patrick Lally, SSP-Litronic, Inc.
3616 Steve Lazerowich, Enspier Technologies/GDT
3617 Phillip S. Lee, SC Solutions, Inc.
3618 Peter Lieberwirth, Authentidate
3619 Rob Lockhart, IEEE-ISTO
3620 Chris Loudon, Enspier Technologies/GDT
3621 J. Scott Lowry, Enspier Technologies/GDT
3622 Lena Kannappan, FuGen Solutions
3623 Paul Madsen, NTT
3624 Adele Marsh, PA Higher Education Assistance Agency
3625 Patty McCarty, Private ID Systems
3626 Doug McCoy, SAFLINK Corporation
3627 Brett McDowell, IEEE-ISTO
3628 Ben Miller, InsideID
3629 Larry Miller, Indentrus LLC
3630 Sead Muftic, SETECS
3631 Noel Nazario, KPMG LLP
3632 Michael R. Nelson, IBM Corporation
3633 Simon Nicholson, Sun Microsystems, Inc.
3634 Pete Palmer, HIMSS NHII Task Force Advisor, Guidant Corporation
3635 Stephen Permission, Standards Based Programs

3636 Bob Pinheiro, Robert Pinheiro Consulting LLC
3637 Alex Popowycz, Fidelity Investments
3638 Hemma Prafullchandra, FuGen Solutions
3639 Stephen L. Ranzini, University Bank
3640 Christiane Reinhold, BearingPoint
3641 Donald E. Rhodes, American Banker Association
3642 Jason Roualt, HP
3643 Randy V. Sabett, Cooley Goodward, LLP
3644 Ravi Sandhu, NSD Security
3645 Dean Sarff, Minerals Management Service
3646 Donald Saxinger, FDIC
3647 Robert J. Schlecht, Mortgage Bankers Association of America
3648 Howard Schmidt, eBay, Inc.
3649 Ari Schwartz, Center for Democracy and Technology
3650 Michael Sessa, PESC
3651 John Shipley, The Shipley Group
3652 Stephen P. Sill, U.S. General Services Administration
3653 Helena G. Sims, NACHA – The Electronic Payments Association
3654 Bill Smith, Sun Microsystems, Inc.
3655 Tadgh Smith, IBM
3656 Judith Spencer, U.S. General Services Administration
3657 William Still, ChoicePoint Public Sector
3658 Michael M. Talley, University Bancorp
3659 David Temoshok, U.S. General Services Administration
3660 Richard Thayer, ComTech, Inc.
3661 John Ticer, NeuStar, Inc.
3662 Richard Trevorah, *tScheme* Limited
3663 Kevin Trilli, VeriSign, Inc.
3664 Matthew Tuttle, beTRUSTed
3665 A. Jerald Varner, U.S. General Services Administration
3666 Martin Wargon, Wave Systems Corporation
3667 Richard G. Wilsher, Zygma LLC
3668 David Weitzel, Mitretek Systems, Inc.
3669 Michael Wolf, Authentidate
3670 Gordon R. Woodrow, ClearTran, Inc.
3671 Steve Worona, EDUCAUSE
3672 David Wasley, Int2

3673 6 References

3674

3675 [CAF] Louden, Chris, Spenser, Judy, Burr, Bill, Hawkins, Kevin, Temoshok, David,
3676 Cornell, John, Wilsher, Richard G., Timchak, Steve, Sill, Stephen, Silver, Dave, Harrison,
3677 Von, eds., "E-Authentication Credential Assessment Framework (CAF)," E-
3678 Authentication Initiative, Version 2.0.0 (March 16, 2005).
3679 <http://www.cio.gov/eauthentication/documents/CAF.pdf>

3680

3681 [EAP CSAC 04011] "EAP working paper: Identity Proofing Service Assessment Criteria
3682 (ID-SAC)," Electronic Authentication Partnership, Draft 0.1.3 (July 20, 2004)
3683 http://eap.projectliberty.org/docs/Jul2004/EAP_CSAC_04011_0-1-3_ID-SAC.doc

3684

3685 [EAPTrustFramework] "Electronic Authentication Partnership Trust Framework"
3686 Electronic Authentication Partnership, Version 1.0. (January 6, 2005)
3687 http://eap.projectliberty.org/docs/Trust_Framework_010605_final.pdf

3688

3689 [FIPS140-2] "Security Requirements for Cryptographic Modules" Federal Information
3690 Processing Standards. (May 25, 2001) [http://csrc.nist.gov/publications/fips/fips140-
3691 2/fips1402.pdf](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)

3692

3693 [IS27001] ISO/IEC 27001:2005 "Information technology - Security techniques -
3694 Requirements for information security management systems" International Organization
3695 for Standardization.
3696 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

3697

3698 [M-04-04] Bolton, Joshua B., eds., "E-Authentication Guidance for Federal Agencies,"
3699 Office of Management and Budget, (December 16, 2003).
3700 <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>

3701

3702 [NIST800-63] Burr, William E., Dodson, Donna F., Polk, W. Timothy, eds., "Electronic
3703 Authentication Guideline: : Recommendations of the National Institute of Standards and
3704 Technology," Version 1.0.2, National Institute of Standards and Technology, (April,
3705 2006). http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

3706

3707 [RFC 3647] Chokhani, S., Ford, W., Sabett, R., Merrill, C., Wu, S., eds., "Internet X.509
3708 Public Key Infrastructure Certificate Policy and Certification Practices Framework," The
3709 Internet Engineering Task Force (November, 2003). <http://www.ietf.org/rfc/rfc3647.txt>
3710
3711