

1

2

3



4

5

6 **Liberty Identity Assurance Framework**

7 **Version:** 1.1

8 **Editor:**

9 Russ Cutler, Confiance Advisors

10 **Contributors:**

11 See the extensive contributors list in Section [7](#).

12 **Abstract:**

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

21

22 **Filename:** liberty-identity-assurance-framework-v1.1.pdf

23

24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66

Notice:

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

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

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

Copyright © 2007-2008 Adobe Systems; Agencia Catalana De Certificacio; America Online, Inc.; Amsoft Systems Pvt Ltd.; BIPAC; BMC Software, Inc.; Bank of America Corporation; Beta Systems Software AG; British Telecommunications plc; Citi; Computer Associates International, Inc.; Dan Combs; Danish National IT & Telecom Agency; Deutsche Telekom AG, T-Com; Diamelle Technologies; Drummond Group Inc.; Entr'ouvert; Ericsson; Falkin Systems LLC; Fidelity Investments; France Télécom; Fugen Solutions, Inc; Fulvens Ltd.; GSA Office of Governmentwide Policy; Gemalto; General Motors; GeoFederation; Giesecke & Devrient GmbH; Guy Huntington; Hewlett-Packard Company; IBM Corporation; Intel Corporation; Kantega; Luminance Consulting Services; Mark Wahl; Mary Ruddy; MedCommons Inc.; Mortgage Bankers Association (MBA); Nanoident Biometrics GmbH; National Emergency Preparedness Coordinating Council (NEPCC); NEC Corporation; Neustar, Inc.; New Zealand Government State Services Commission; NHK (Japan Broadcasting Corporation) Science & Technical Research Laboratories; Nippon Telegraph and Telephone Corporation; Nokia Corporation; Novell, Inc.; OpenNetwork; Oracle Corporation; Ping Identity Corporation; Postsecondary Electronics Standards Council (PESC); RSA Security Inc.; SanDisk Corporation; Sun Microsystems, Inc.; Symlabs, Inc.; Telefónica Móviles, S.A.; Telenor R&D; Thales e-Security; UNINETT AS; VeriSign, Inc.; Vodafone Group Plc.; and Wells Fargo.

All rights reserved.

67 **Contents**

68

69 **1 Introduction5**

70 **2 Assurance Levels7**

71 2.1 Assurance Level Policy Overview7

72 2.2 Description of the Four Assurance Levels8

73 2.2.1 Assurance Level 19

74 2.2.2 Assurance Level 29

75 2.2.3 Assurance Level 310

76 2.2.4 Assurance Level 410

77 **3 Service Assessment Criteria11**

78 3.1 Context and Scope 11

79 3.2 Readership 11

80 3.3 Terminology 12

81 3.4 Criteria Descriptions 12

82 3.5 Common Organizational Service Assessment Criteria 13

83 3.5.1 Assurance Level 1 13

84 3.5.2 Assurance Level 2 14

85 3.5.3 Assurance Level 3 22

86 3.5.4 Assurance Level 4 30

87 3.6 Identity Proofing Service Assessment Criteria 38

88 3.6.1 Assurance Level 1 39

89 3.6.2 Assurance Level 2 41

90 3.6.3 Assurance Level 3 46

91 3.6.4 Assurance Level 4 50

92 3.6.5 Compliance Tables 55

93 3.7 Credential Management Service Assessment Criteria 57

94 3.7.1 Part A--Credential Operating Environment 58

95 3.7.2 Part B--Credential Issuing 67

96 3.7.3 Part C--Credential Revocation 79

97 3.7.4 Part D--Credential Status Management 89

98 3.7.5 Part E--Credential Validation/Authentication 92

99 3.7.6 Compliance Tables 94

100 **4 Accreditation and Certification Rules102**

101 4.1 Assessor Accreditation 102

102 4.1.1 Criteria for Assessor Accreditation 102

103 4.1.2 Assessment 103

104 4.1.3 Accreditation Decision and Appeal 103

105 4.1.4 Maintaining Accreditation 103

106 4.2 Certification of Credential Service Provider Offerings 104

107 4.2.1 Process of Certification 104

108 4.2.2 Criteria for Certification of CSP Line of Business 105

109 4.2.3 Certification Decision 106

110	4.2.4	Appeals Process	106
111	4.2.5	Maintaining Certification.....	106
112	4.3	Process for Handling Non-Compliance	107
113	4.4	Acceptable Public Statements Regarding IAEG Accreditation and Certification ..	107
114	5	Business Rules.....	108
115	5.1	Scope.....	108
116	5.2	Participation	108
117	5.3	Roles and Obligations	109
118	5.3.1	IAEG.....	109
119	5.3.2	CSP Obligations.....	109
120	5.3.3	Relying Party Obligations.....	110
121	5.3.4	Assessor Obligations.....	111
122	5.3.5	General Obligations	112
123	5.4	Enforcement and Recourse	113
124	5.4.1	Breach of Accreditation or Certification Requirements	113
125	5.4.2	Monetary Recourse	113
126	5.4.3	Administrative Recourse.....	114
127	5.5	General Terms	115
128	5.5.1	Governing Law	115
129	5.5.2	Disclaimer	115
130	5.5.3	Assignment and Succession.....	115
131	5.5.4	Hold Harmless	116
132	5.5.5	Severability	116
133	5.6	Interpretation.....	116
134	6	IAEG Glossary.....	117
135	7	Publication Acknowledgements	123
136	8	References	127
137			
138			

139 **1 Introduction**

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

149 The LIAF leverages the EAP Trust Framework [[EAPTrustFramework](#)] and the US E-
150 Authentication Federation Credential Assessment Framework ([[CAF](#)]) as a baseline in
151 forming the criteria for a harmonized, best-of-breed industry identity assurance standard.
152 The LIAF is a framework supporting mutual acceptance, validation, and life cycle
153 maintenance across identity federations. The main components of the LIAF are detailed
154 discussions of Assurance Level criteria, Service and Credential Assessment Criteria, an
155 Accreditation and Certification Model, and the associated business rules.

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. The LIAF
158 defers to the guidance provided by the U.S. National Institute of Standards and
159 Technology (NIST) Special Publication 800-63 version 1.0.1 [[NIST800-63](#)] which
160 outlines four (4) levels of assurance, ranging in confidence level from low to very high.
161 Use of ALs is determined by the level of confidence or trust necessary to mitigate risk in
162 the transaction.

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

170 The LIAF will employ a phased approach to establishing criteria for certification and
171 accreditation, initially focusing on credential service providers (CSPs) and the
172 accreditation of those who will assess and evaluate them. The goal of this phased
173 approach is to initially provide federations and Federation Operators with the means to
174 certify their members for the benefit of inter-federation and streamlining the certification
175 process for the industry. It is anticipated that follow-on phases will target the
176 development of criteria for certification of federations, themselves, and a Best Practice
177 guide for relying parties.

178 Finally, the LIAF will include a discussion of the business rules associated with IAEG
179 participation, certification, and accreditation.

180 2 Assurance Levels

181 2.1 Assurance Level Policy Overview

182 An assurance level (AL) describes the degree to which a relying party in an electronic
183 business transaction can be confident that the identity information being presented by a
184 CSP actually represents the entity named in it and that it is the represented entity who is
185 actually engaging in the electronic transaction. ALs are based on two factors:

- 186 • The extent to which the identity presented by a CSP in an identity assertion can be
187 trusted to actually belong to the entity represented. This factor is generally
188 established through the identity proofing process and identity information
189 management practices.
- 190 • The extent to which the electronic credential presented to a CSP by an individual
191 can be trusted to be a proxy for the entity named in it and not someone else
192 (known as identity binding). This factor is directly related to the integrity and
193 reliability of the technology associated with the credential itself, the processes by
194 which the credential and its verification token are issued, managed, and verified,
195 and the system and security measures followed by the credential service provider
196 responsible for this service.

197 Managing risk in electronic transactions requires authentication and identity information
198 management processes that provide an appropriate level of assurance of identity. Because
199 different levels of risk are associated with different electronic transactions, IAEG has
200 adopted a multi-level approach to ALs. Each level describes a different degree of
201 certainty in the identity of the claimant.

202 The IAEG defines four levels of assurance. The four IAEG ALs are based on the four
203 levels of assurance posited by the U.S. Federal Government and described in OMB M-
204 04-04 [M-04-04] and NIST Special Publication 800-63 [NIST800-63] for use by Federal
205 agencies. The IAEG ALs enable subscribers and relying parties to select appropriate
206 electronic identity trust services. IAEG uses the ALs to define the service assessment
207 criteria to be applied to electronic identity trust service providers when they are
208 demonstrating compliance through the IAEG assessment process. Relying parties should
209 use the assurance level descriptions to map risk and determine the type of credential
210 issuance and authentication services they require. Credential service providers (CSPs)
211 should use the levels to determine what types of credentialing electronic identity trust
212 services they are capable of providing currently and/or aspire to provide in future service
213 offerings.

214

215 **2.2 Description of the Four Assurance Levels**

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

219

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

220

221 The choice of AL is based on the degree of certainty of identity required to mitigate risk
 222 mapped to the level of assurance provided by the credentialing process. The degree of
 223 assurance required is determined by the relying party through risk assessment processes
 224 covering the electronic transaction system. By mapping impact levels to ALs, relying
 225 parties can then determine what level of assurance they require. Further information on
 226 assessing impact levels is provided in Table 2-2:

227

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>				

228

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

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

238 **2.2.1 Assurance Level 1**

239 At AL1, there is minimal confidence in the asserted identity. Use of this level is
240 appropriate when no negative consequences result from erroneous authentication and the
241 authentication mechanism used provides some assurance. A wide range of available
242 technologies and any of the token methods associated with higher ALs, including PINS,
243 can satisfy the authentication requirement. This level does not require use of
244 cryptographic methods.

245 The electronic submission of forms by individuals can be Level 1 transactions when all
246 information flows to the organization from the individual, there is no release of
247 information in return and the criteria for higher assurance levels are not triggered.

248 For example, when an individual uses a web site to pay a parking ticket or tax payment,
249 the transaction can be treated as a Level 1 transaction. Other examples of Level 1
250 transactions include transactions in which a claimant presents a self-registered user ID or
251 password to a merchant's web page to create a customized page, or transactions involving
252 web sites that require registration for access to materials and documentation such as news
253 or product documentation.

254 **2.2.2 Assurance Level 2**

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

261 For example, a transaction in which a beneficiary changes an address of record through
262 an insurance provider's web site can be a Level 2 transaction. The site needs some
263 authentication to ensure that the address being changed is the entitled person's address.
264 However, this transaction involves a relatively low (moderate) risk of inconvenience.
265 Since official notices regarding payment amounts, account status, and records of changes

266 are sent to the beneficiary's address of record, the transaction entails moderate risk of
267 unauthorized release of personally sensitive data.

268 **2.2.3 Assurance Level 3**

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

276 For example, a transaction in which a patent attorney electronically submits confidential
277 patent information to the U.S. Patent and Trademark Office can be a Level 3 transaction.
278 Improper disclosure would give competitors a competitive advantage. Other Level 3
279 transaction examples include online access to a brokerage account that allows the
280 claimant to trade stock, or use by a contractor of a remote system to access potentially
281 sensitive personal client information.

282 **2.2.4 Assurance Level 4**

283 AL4 is appropriate for transactions requiring very high confidence in an asserted identity.
284 This level provides the best practical remote-network authentication assurance, based on
285 proof of possession of a key through a cryptographic protocol. Level 4 is similar to Level
286 3 except that only “hard” cryptographic tokens are allowed. High levels of cryptographic
287 assurance are required for all elements of credential and token management. All sensitive
288 data transfers are cryptographically authenticated using keys bound to the authentication
289 process.

290 For example, access by a law enforcement official to a law enforcement database
291 containing criminal records requires Level 4 protection. Unauthorized access could raise
292 privacy issues and/or compromise investigations. Dispensation by a pharmacist of a
293 controlled drug also requires Level 4 protection. The pharmacist needs full assurance that
294 a qualified doctor prescribed the drug, and the pharmacist is criminally liable for any
295 failure to validate the prescription and dispense the correct drug in the prescribed amount.
296 Finally, approval by an executive of a transfer of funds in excess of \$1 million out of an
297 organization's bank accounts would be a Level 4 transaction.

298

299 **3 Service Assessment Criteria**

300 **3.1 Context and Scope**

301 The IAEG Service Assessment Criteria (SAC) are prepared and maintained by the
302 Identity Assurance Expert Group (IAEG) as part of its Identity Assurance Framework.
303 These criteria set out the requirements for services and their providers at all assurance
304 levels within the Framework. These criteria focus on the specific requirements for IAEG
305 assessment at each assurance level (AL) for the following:

- 306 • The general business and organizational conformity of services and their
307 providers,
- 308 • The functional conformity of identity proofing services, and
- 309 • The functional conformity of credential management services and their providers.

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

312 These criteria have been approved under the IAEG's governance rules as being suitable
313 for use by IAEG-recognized assessors in the performance of their assessments of trust
314 services whose providers are seeking approval by IAEG.

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

318 This document describes the specific criteria that must be met to achieve each of the four
319 ALs supported by the IAEG. To be certified under the IAEG System, services must
320 comply with all criteria at the appropriate level.

321 **3.2 Readership**

322 This description of Service Assessment Criteria is required reading for all IAEG-
323 recognized assessors, since it sets out the requirements with which service functions must
324 comply to obtain IAEG approval.

325 The description of criteria in Sections [3.5](#), [3.6](#) and [3.7](#) is required reading for all providers
326 of services that include identity proofing functions, since providers must be fully aware of
327 the criteria with which their service must comply. It is also recommended reading for
328 those involved in the governance and day-to-day administration of the Identity Assurance
329 Framework.

330 Identity proofing criteria included in Section [3.6](#) is required reading for all Electronic
331 Trust Service Providers whose services include identity proofing functions, since
332 providers must be fully aware of the criteria with which their service must comply.

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

336 3.3 Terminology

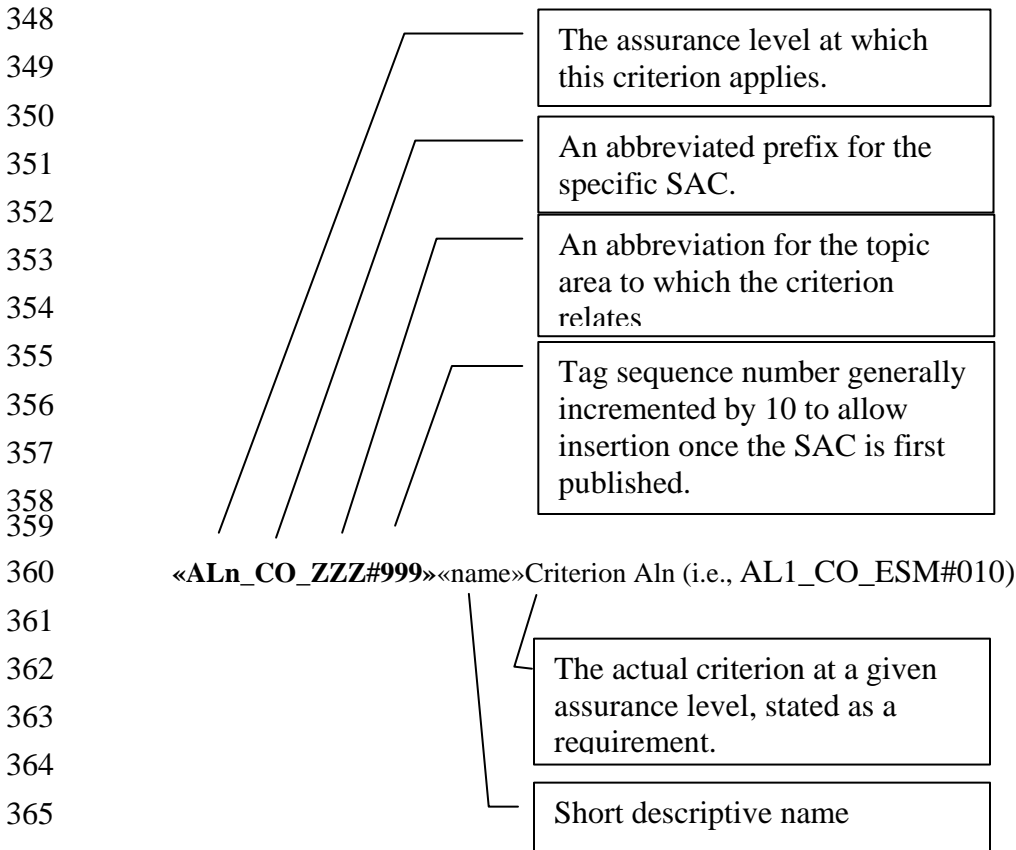
337 All special terms used in this description are defined in the IAEG Glossary.

338 3.4 Criteria Descriptions

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

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

347 The criteria are described as follows:



366

367 **3.5 Common Organizational Service Assessment Criteria**

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

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

374 Note: Some of the SAC-identifying numbers are not used in all of the ALs. In such cases,
375 the particular SAC number has been reserved where not used and skipped.

376 **3.5.1 Assurance Level 1**

377 **3.5.1.1 Enterprise and Service Maturity**

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

381 An enterprise and its specified service must:

382 **AL1_CO_ESM#010 Established enterprise**

383 Be a valid legal entity and a person with legal authority to commit the enterprise must
384 submit the assessment package.

385 **AL1_CO_ESM#020 Established service**

386 Be described in the assessment package as it stands at the time of submission for
387 assessment and must be assessed strictly against that description.

388 **AL1_CO_ESM#030 Legal compliance**

389 Set out and demonstrate that it understands and complies with any legal requirements
390 incumbent on it in connection with operation and delivery of the specified service,
391 accounting for all jurisdictions and countries within which its services may be used.

392

393 **3.5.1.2 Notices and User information**

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

396 An enterprise and its specified service must:

397 **AL1_CO_NUI#010 General Service Definition**

398 Make available to the intended user community a service definition for its specified
399 service that includes all applicable Terms, Conditions, Fees, and Privacy Policy for the
400 service, including any limitations of its usage.

401 **AL1_CO_NUI#030 Due notification**

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

405 **AL1_CO_NUI#040 User Agreement**

406 Through a user agreement:

- 407 a) require the subscriber, or user, to provide full and correct information as required
408 under the terms of their use of the service.
409 b) obtain a record (hard-copy or electronic) of the subscriber's agreement to the
410 terms and conditions of service.
411

412 **3.5.1.3 Information Security Management**

413 No stipulation.

414 **3.5.1.4 Secure Communications**

415 **AL1_CO_SCO#020 Protection of secrets**

416 Ensure that:

- 417 a) access to shared secrets shall be subject to discretionary controls which permit
418 access to those roles/applications which need such access.
419 b) stored shared secrets are not held in their plaintext form.
420 c) any plaintext passwords or secrets are not transmitted across any public or
421 unsecured network.
422

423 **3.5.2 Assurance Level 2**

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

427 **3.5.2.1 Enterprise and Service Maturity**

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

430 An enterprise and its specified service must:

431 **AL2_CO_ESM#010 Established enterprise**

432 Be a valid legal entity and a person with legal authority to commit the enterprise must
433 submit the assessment package.

434 **AL2_CO_ESM#020 Established service**

435 Be described in the assessment package as it stands at the time of submission for
436 assessment and must be assessed strictly against that description.

437 **AL2_CO_ESM#030 Legal compliance**

438 Set out and demonstrate that it understands and complies with any legal requirements
439 incumbent on it in connection with operation and delivery of the specified service,
440 accounting for all jurisdictions within which its services may be offered.

441 **AL2_CO_ESM#040 Financial Provisions**

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

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

446 Specifically set out and demonstrate that it understands and complies with those legal and
447 regulatory requirements incumbent upon it concerning the retention of private (personal
448 and business) information (its secure storage and protection against loss and/or
449 destruction) and the protection of private information (against unlawful or unauthorized
450 access unless permitted by the information owner or required by due process).

451

452 **3.5.2.2 Notices and User Information/Agreements**

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

456 An enterprise and its specified service must:

457 **AL2_CO_NUI#010** **General Service Definition**

458 Make available to the intended user community a service definition for its specified
459 service that includes any specific uses or limitations on its use, all applicable Terms,
460 Conditions, Fees, and Privacy Policy for the service, including any limitations of its usage
461 and definitions of any terms having specific intention or interpretation. Specific
462 provisions are stated in further criteria in this section.

463 **AL2_CO_NUI#020** **Service Definition sections**

464 Publish a service definition for the specified service containing clauses that provide the
465 following information:

- 466 a) The country in or legal jurisdiction under which the service is operated.
- 467 b) if different from the above, the legal jurisdiction under which subscriber and any
468 relying party agreements are entered into.
- 469 c) applicable legislation with which the service complies.
- 470 d) obligations incumbent upon the CSP.
- 471 e) obligations incumbent upon the subscriber.
- 472 f) notifications and guidance for relying parties, especially in respect of actions they
473 are expected to take should they choose to rely upon the service's product.
- 474 g) statement of warranties.
- 475 h) statement of liabilities.
- 476 i) procedures for notification of changes to terms and conditions.
- 477 j) steps the CSP will take in the event that it chooses or is obliged to terminate the
478 service.
- 479 k) full contact details for the CSP (i.e., conventional post, telephone, Internet)
480 including a help desk.
- 481 l) availability of the specified service per se and of its help desk facility.
- 482 m) termination of aspects or all of service.

483 **AL2_CO_NUI#030** **Due notification**

484 Have in place and follow appropriate policy and procedures to ensure that it notifies
485 subscribers in a timely and reliable fashion of any changes to the service definition and
486 any applicable Terms, Conditions, Fees, and Privacy Policy for the specified service and
487 provides a clear means by which subscribers may indicate that they wish to accept the
488 new terms or terminate their subscription.

489 **AL2_CO_NUI#050** **Subscriber Information**

490 Require the subscriber to provide full and correct information as required under the terms
491 of their use of the service.

492 **AL2_CO_NUI#060** **Subscriber Agreement**

493 Obtain a record (hard-copy or electronic) of the subscriber's agreement to the terms and
494 conditions of service.

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

496 Require and provide the mechanisms for the subscriber to provide in a timely manner full
497 and correct amendments should any of their recorded information change, as required
498 under the terms of their use of the service, and only after the subscriber's identity has
499 been authenticated.

500 **AL2_CO_NUI#080** **Helpdesk facility**

501 Ensure that its help desk is available for any queries related to the specified service
502 during the regular business hours of its primary operational location, excepting
503 nationally-recognized holidays.

504

505 **3.5.2.3 Information Security Management**

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

511 An enterprise and its specified service must:

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

513 Have documented all security-relevant administrative, management, and technical
514 policies and procedures. The enterprise must ensure that these are based upon recognized
515 standards or published references, are adequate for the specified service, and are applied
516 in the manner intended.

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

518 Have a clearly defined managerial role, at a senior level, in which full responsibility for
519 the business's security policies is vested and from which promulgation of policy and
520 related procedures is controlled and managed. The policies in place must be properly
521 maintained so as to be effective at all times.

522 **AL2_CO_ISM#030 Risk Management**

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

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

526 Have and shall keep updated a Continuity of Operations Plan that covers disaster
527 recovery and the resilience of the specified service.

528 **AL2_CO_ISM#050 Configuration Management**

529 Demonstrate a configuration management system that at least includes:

- 530 a) version control for software system components.
- 531 b) timely identification and installation of all applicable patches for any software
532 used in the provisioning of the specified service.

533 **AL2_CO_ISM#060 Quality Management**

534 Demonstrate a quality management system that is appropriate for the specified service.

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

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

539 **AL2_CO_ISM#080 Internal Service Audit**

540 Unless it can show that by reason of its size or for other operational reason it is
541 unreasonable, be regularly audited for effective provision of the specified service by
542 internal audit functions independent of the parts of the enterprise responsible for the
543 specified service.

544 **AL2_CO_ISM#090 Independent Audit**

545 Be audited by an independent auditor at least every 24 months to ensure the
546 organization's security-related practices are consistent with the policies and procedures
547 for the specified service and the appointed auditor must have appropriate accreditation or
548 other acceptable experience and qualification.

549 **AL2_CO_ISM#100 Audit Records**

550 Retain full records of all audits, both internal and independent, for a period that, at a
551 minimum, fulfills its legal obligations and otherwise for greater periods either as it may

552 have committed to in its service definition or required by any other obligations it has
553 with/to a subscriber. Such records must be held securely and protected against loss,
554 alteration, or destruction.

555 **AL2_CO_ISM#110 Termination provisions**

556 Have in place a clear plan for the protection of subscribers' private and secret information
557 related to their use of the service which must ensure the ongoing secure preservation and
558 protection of legally required records and for the secure destruction and disposal of any
559 such information whose retention is not legally required. Essential details of this plan
560 must be published.

561

562 **3.5.2.4 Security-relevant Event (Audit) Records**

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

565 An enterprise and its specified service must:

566 **AL2_CO_SER#010 Security event logging**

567 Maintain a log of all security-relevant events concerning the operation of the service,
568 together with a precise record of the time at which the event occurred (time-stamp) , and
569 such records must be retained with appropriate protection, accounting for service
570 definition, risk management requirements, and applicable legislation.

571

572 **3.5.2.5 Operational infrastructure**

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

576 An enterprise and its specified service must:

577 **AL2_CO_OPN#010 Technical security**

578 Demonstrate that the technical controls employed will provide the level of security
579 required by the risk assessment plan and the ISMS, or other IT security management
580 methodology recognized by a government or professional body, and that these controls
581 are effectively integrated with the appropriate procedural and physical security measures.

582 **AL2_CO_OPN#020** **Defined security roles**

583 Define, by means of a job description, the roles and responsibilities for every security-
584 relevant task, relating it to specific procedures, (which shall be set out in the ISMS, or
585 other IT security management methodology recognized by a government or professional
586 body.) and other job descriptions. Where the role is security-critical or where special
587 privileges or shared duties exist, these must be specifically highlighted, including access
588 privileges relating to logical and physical parts of the service's operations.

589 **AL2_CO_OPN#030** **Personnel recruitment**

590 Demonstrate that it has defined practices for the selection, evaluation, and contracting of
591 all personnel, both direct employees and those whose services are provided by third
592 parties.

593 **AL2_CO_OPN#040** **Personnel skills**

594 Ensure that employees are sufficiently trained, qualified, experienced, and current for the
595 roles they fulfill. Such measures must be accomplished either by recruitment practices or
596 through a specific training program. Where employees are undergoing on-the-job
597 training, they must only do so under the guidance of a mentor with established leadership
598 skills.

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

600 Have sufficient staff to operate the specified service according to its policies and
601 procedures.

602 **AL2_CO_OPN#060** **Physical access control**

603 Apply physical access control mechanisms to ensure that access to sensitive areas is
604 restricted to authorized personnel.

605 **AL2_CO_OPN#070** **Logical access control**

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

608

609 **3.5.2.6 External Services and Components**

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

613 An enterprise and its specified service must:

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

615 Where the enterprise uses the services of external suppliers for specific packaged
616 components of the service or for resources that are integrated with its own operations and
617 under its controls, ensure that those parties are engaged through reliable and appropriate
618 contractual arrangements which stipulate critical policies, procedures, and practices that
619 the subcontractor is required to fulfill.

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

621 Where the enterprise uses the services of external suppliers for specific packaged
622 components of the service or for resources that are integrated with its own operations and
623 under its controls, ensure that contractors' compliance with contractually stipulated
624 policies and procedures, and thus with IAEG assessment criteria, can be proven and
625 subsequently monitored.

626

627 **3.5.2.7 Secure Communications**

628 An enterprise and its specified service must:

629 **AL2_CO_SCO#010 Secure remote communications**

630 If the specific service components are located remotely from and communicate over a
631 public or unsecured network with other service components or other CSP(s) it services,
632 the communications must be cryptographically authenticated by an authentication method
633 that meets, at a minimum, the requirements of AL2 and encrypted using a Federal
634 Information Processing Standard ([FIPS])-approved encryption method or a mechanism
635 of demonstrably equivalent rigor, as established by a recognized national technical
636 authority.

637 **AL2_CO_SCO#020 Protection of secrets**

638 Ensure that:

- 639 a) access to shared secrets shall be subject to discretionary controls that permit
640 access to those roles/applications requiring such access.
641 b) stored shared secrets are not held in their plaintext form.
642 c) any long-term (i.e., not session) shared secrets are revealed only to the subscriber
643 and to CSP's direct agents (bearing in mind item "a" in this list).

644 These roles should be defined and documented by the CSP in accordance to AL
645 2_CO_OPN#020, above.

646

647 **3.5.3 Assurance Level 3**

648 Achieving AL3 requires meeting more stringent criteria in addition to all criteria required
649 to achieve AL2.

650 **3.5.3.1 Enterprise and Service Maturity**

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

653 An enterprise and its specified service must:

654 **AL3_CO_ESM#010 Established enterprise**

655 Be a valid legal entity and a person with legal authority to commit the enterprise must
656 submit the assessment package.

657 **AL3_CO_ESM#020 Established service**

658 Be described in the assessment package as it stands at the time of submission for
659 assessment and must be assessed strictly against that description.

660 **AL3_CO_ESM#030 Legal compliance**

661 Set out and demonstrate that it understands and complies with any legal requirements
662 incumbent on it in connection with operation and delivery of the specified service,
663 accounting for all jurisdictions within which its services may be offered.

664 **AL3_CO_ESM#040 Financial Provisions**

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

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

669 Specifically set out and demonstrate that it understands and complies with those legal and
670 regulatory requirements incumbent upon it concerning the retention of private (personal
671 and business) information (its secure storage and protection against loss and/or
672 destruction) and the protection of private information (against unlawful or unauthorized
673 access unless permitted by the information owner or required by due process).

674 **AL3_CO_ESM#060 Ownership**

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

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

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

682

683 **3.5.3.2 Notices and User Information**

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

687 An enterprise and its specified service must:

688 **AL3_CO_NUI#010 General Service Definition**

689 Make available to the intended user community a service definition for its specified
690 service which includes any specific uses or limitations on its use, all applicable terms,
691 conditions, fees, and privacy policy for the service, including any limitations of its usage
692 and definitions of any terms having specific intention or interpretation. Specific
693 provisions are stated in further criteria in this section.

694 **AL3_CO_NUI#020 Service Definition Sections**

695 Publish a service definition for the specified service containing clauses that provide the
696 following information:

- 697 a) the legal jurisdiction under, or country in, which the service is operated;
- 698 b) if different to the above, the legal jurisdiction under which subscriber and any
699 relying party agreements are entered into;
- 700 c) applicable legislation with which the service complies;
- 701 d) obligations incumbent upon the CSP;
- 702 e) obligations incumbent upon the subscriber;
- 703 f) notifications and guidance for relying parties, especially in respect of actions they
704 are expected to take should they choose to rely upon the service's product;
- 705 g) statement of warranties;
- 706 h) statement of liabilities;
- 707 i) procedures for notification of changes to terms and conditions;

- 708 j) steps the CSP will take in the event that it chooses or is obliged to terminate the
709 service;
710 k) full contact details for the CSP (i.e., conventional post, telephone, Internet)
711 including a help desk;
712 l) availability of the specified service *per se* and of its help desk facility;
713 m) termination of aspects or all of service.

714 **AL3_CO_NUI#030 Due notification**

715 Have in place and follow appropriate policy and procedures to ensure that it notifies
716 subscribers in a timely and reliable fashion of any changes to the service definition and
717 any applicable terms, conditions, fees, and privacy policy for the specified service and
718 provides a clear means by which subscribers may indicate that they wish to accept the
719 new terms or terminate their subscription.

720 **AL3_CO_NUI#050 Subscriber Information**

721 Require the subscriber to provide full and correct information as required under the terms
722 of their use of the service.

723 **AL3_CO_NUI#060 Subscriber Agreement**

724 Obtain a record (hard-copy or electronic) of the subscriber's agreement to the terms and
725 conditions of service.

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

727 Require and provide the mechanisms for the subscriber to provide in a timely manner full
728 and correct amendments should any of their recorded information change, as required
729 under the terms of their use of the service, and only after the subscriber's identity has
730 been authenticated.

731 **AL3_CO_NUI#080 Helpdesk facility**

732 Ensure that its help desk is available for any queries related to the specified service
733 during the regular business hours of its primary operational location, , excepting
734 nationally-recognized holidays.

735

736 **3.5.3.3 Information Security Management**

737 These criteria address the way in which the enterprise manages the security of its
738 business, the specified service, and information it holds relating to its user community.
739 This section focuses on the key components that make up a well-established and effective

740 Information Security Management System (ISMS), or other IT security management
741 methodology recognized by a government or professional body.

742 An enterprise and its specified service must:

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

744 Have documented all security-relevant administrative management and technical policies
745 and procedures. The enterprise must ensure that these are based upon recognized
746 standards or published references, are adequate for the specified service, and are applied
747 in the manner intended.

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

749 Have a clearly defined managerial role, at a senior level, where full responsibility for the
750 business' security policies is vested and from which promulgation of policy and related
751 procedures is controlled and managed. The policies in place must be properly maintained
752 so as to be effective at all times.

753 **AL3_CO_ISM#030 Risk Management**

754 Demonstrate a risk management methodology that adequately identifies and mitigates
755 risks related to the specified service and its user community and must show that a risk
756 assessment review is performed at least once every six months, such as adherence to SAS
757 70 or ISO 27001 methodologies.

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

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

762 **AL3_CO_ISM#050 Configuration Management**

763 Demonstrate a configuration management system that at least includes:

- 764 a) version control for software system components;
- 765 b) timely identification and installation of all applicable patches for any software
766 used in the provisioning of the specified service;
- 767 c) version control and managed distribution for all documentation associated with
768 the specification, management, and operation of the system, covering both
769 internal and publicly available materials.

770 **AL3_CO_ISM#060** **Quality Management**

771 Demonstrate a quality management system that is appropriate for the specified service.

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

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

- 776 a) the software and hardware development environments, for customized
- 777 components;
- 778 b) the procurement process for commercial off-the-shelf (COTS) components;
- 779 c) contracted consultancy/support services;
- 780 d) shipment of system components;
- 781 e) storage of system components;
- 782 f) installation environment security;
- 783 g) system configuration;
- 784 h) transfer to operational status.

785 **AL3_CO_ISM#080** **Internal Service Audit**

786 Unless it can show that by reason of its size or for other arguable operational reason it is
787 unreasonable so to perform, be regularly audited for effective provision of the specified
788 service by internal audit functions independent of the parts of the enterprise responsible
789 for the specified service.

790 **AL3_CO_ISM#090** **Independent Audit**

791 Be audited by an independent auditor at least every 24 months to ensure the
792 organization's security-related practices are consistent with the policies and procedures
793 for the specified service and the appointed auditor must have appropriate accreditation or
794 other acceptable experience and qualification.

795 **AL3_CO_ISM#100** **Audit Records**

796 Retain full records of all audits, both internal and independent, for a period which, as a
797 minimum, fulfils its legal obligations and otherwise for greater periods either as it may
798 have committed to in its service definition or required by any other obligations it has
799 with/to a subscriber. Such records must be held securely and protected against loss,
800 alteration, or destruction.

801 **AL3_CO_ISM#110 Termination provisions**

802 Have in place a clear plan for the protection of subscribers' private and secret information
803 related to their use of the service which must ensure the ongoing secure preservation and
804 protection of legally-required records and for the secure destruction and disposal of any
805 such information whose retention is not legally required. Essential details of this plan
806 must be published.

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

808 Have in place an Information Security Management System (ISMS), or other IT security
809 management methodology recognized by a government or professional body, that follows
810 best practices as accepted by the information security industry and that applies and is
811 appropriate to the CSP in question. All requirements defined by preceding criteria in this
812 section must fall wholly within the scope of this ISMS or selected recognized alternative.

813

814 **3.5.3.4 Security-Relevant Event (Audit) Records**

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

817 An enterprise and its specified service must:

818 **AL3_CO_SER#010 Security Event Logging**

819 Maintain a log of all security-relevant events concerning the operation of the service,
820 together with a precise record of the time at which the event occurred (time-stamp), and
821 such records must be retained with appropriate protection, accounting for service
822 definition risk management requirements, and applicable legislation.

823

824 **3.5.3.5 Operational Infrastructure**

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

828 An enterprise and its specified service must:

829 **AL3_CO_OPN#010 Technical security**

830 Demonstrate that the technical controls employed will provide the level of security
831 required by the risk assessment plan and the ISMS, or other IT security management
832 methodology recognized by a government or professional body, and that these controls
833 are effectively integrated with the appropriate procedural and physical security measures.

834 **AL3_CO_OPN#020** **Defined security roles**

835 Define, by means of a job description, the roles and responsibilities for every security-
836 relevant task, relating it to specific procedures (which shall be set out in the ISMS, or
837 other IT security management methodology recognized by a government or professional
838 body) and other job descriptions. Where the role is security-critical or where special
839 privileges or shared duties exist, these must be specifically highlighted, including access
840 privileges relating to logical and physical parts of the service's operations.

841 **AL3_CO_OPN#030** **Personnel recruitment**

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

847 **AL3_CO_OPN#040** **Personnel skills**

848 Ensure that employees are sufficiently trained, qualified, experienced, and current for the
849 roles they fulfill. Such measures must be accomplished either by recruitment practices or
850 through a specific training program. Where employees are undergoing on-the-job
851 training, they must only do so under the guidance of a mentor with established leadership
852 skills.

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

854 Have sufficient staff to operate the specified service according to its policies and
855 procedures.

856 **AL3_CO_OPN#060** **Physical access control**

857 Apply physical access control mechanisms to ensure access to sensitive areas is restricted
858 to authorized personnel.

859 **AL3_CO_OPN#070** **Logical access control**

860 Employ logical access control mechanisms to ensure access to sensitive system functions
861 and controls is restricted to authorized personnel.

862

863 **3.5.3.6 External Services and Components**

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

867 An enterprise and its specified service must:

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

869 Where the enterprise uses the services of external suppliers for specific packaged
870 components of the service or for resources which are integrated with its own operations
871 and under its controls, ensure that those parties are engaged through reliable and
872 appropriate contractual arrangements which stipulate critical policies, procedures, and
873 practices that the sub-contractor is required to fulfill.

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

875 Where the enterprise uses the services of external suppliers for specific packaged
876 components of the service or for resources which are integrated with its own operations
877 and under its controls, ensure that contractors' compliance with contractually stipulated
878 policies and procedures, and thus with the IAEG's assessment criteria, can be proven and
879 subsequently monitored.

880

881 **3.5.3.7 Secure Communications**

882 An enterprise and its specified service must:

883 **AL3_CO_SCO#010 Secure remote communications**

884 If the specific service components are located remotely from and communicate over a
885 public or unsecured network with other service components or other CSPs it services, the
886 communications must be cryptographically authenticated by an authentication protocol
887 that meets, at a minimum, the requirements of AL3 and encrypted using an Approved
888 Encryption method, as established by a recognized national technical authority.

889 **AL3_CO_SCO#020 Protection of secrets**

890 Ensure that:

- 891 a) access to shared secrets shall be subject to discretionary controls that permit
892 access to those roles/applications requiring such access.
- 893 b) stored shared secrets are encrypted such that:
- 894 i the encryption key for the shared secret file is encrypted under a key held
895 in a FIPS 140-2 [FIPS140-2] Level 2 (or higher) validated hardware

- 896 cryptographic module, or equivalent, as established by a recognized
897 national technical authority, or any FIPS 140-2 Level 3 or 4 cryptographic
898 module, or equivalent, as established by a recognized national technical
899 authority, and decrypted only as immediately required for an
900 authentication operation.
- 901 ii they are protected as a key within the boundary of a FIPS 140-2 Level 2
902 (or higher) validated hardware cryptographic module, or equivalent, as
903 established by a recognized national technical authority, or any FIPS 140-
904 2 Level 3 or 4 cryptographic module, or equivalent, as established by a
905 recognized national technical authority, and are not exported in plaintext
906 from the module.
- 907 iii they are split by an "*n from m*" cryptographic secret-sharing method.
- 908 c) any long-term (i.e., not session) shared secrets are revealed only to the subscriber
909 and CSP direct agents (bearing in mind item "a" in this list).
910

911 **3.5.4 Assurance Level 4**

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

914 **3.5.4.1 Enterprise and Service Maturity**

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

917 An enterprise and its specified service must:

918 **AL4_CO_ESM#010 Established enterprise**

919 Be a valid legal entity and a person with legal authority to commit the enterprise must
920 submit the assessment package.

921 **AL4_CO_ESM#020 Established service**

922 Be described in the assessment package as it stands at the time of submission for
923 assessment and must be assessed strictly against that description.

924 **AL4_CO_ESM#030 Legal compliance**

925 Set out and demonstrate that it understands and complies with any legal requirements
926 incumbent on it in connection with operation and delivery of the specified service,
927 accounting for all jurisdictions within which its services may be offered.

928 **AL4_CO_ESM#040 Financial Provisions**

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

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

933 Specifically set out and demonstrate that it understands and complies with those legal and
934 regulatory requirements incumbent upon it concerning the retention of private (personal
935 and business) information (its secure storage and protection against loss and/or
936 destruction) and the protection of private information (against unlawful or unauthorized
937 access unless permitted by the information owner or required by due process).

938 **AL4_CO_ESM#060 Ownership**

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

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

943 Demonstrate that, for the purposes of providing the specified service, its management and
944 operational structures are distinct, autonomous, have discrete legal accountability, and
945 function according to separate policies, procedures, and controls.

946

947 **3.5.4.2 Notices and User Information/Agreements**

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

951 An enterprise and its specified service must:

952 **AL4_CO_NUI#010 General Service Definition**

953 Make available to the intended user community a service definition for its specified
954 service which includes any specific uses or limitations on its use, all applicable terms,
955 conditions, fees, and privacy policy for the service, including any limitations of its usage
956 and definitions of any terms having specific intention or interpretation. Specific
957 provisions are stated in further criteria in this section.

958 **AL4_CO_NUI#020** **Service Definition Sections**

959 Publish a service definition for the specified service containing clauses that provide the
960 following information:

- 961 a) the country in or legal jurisdiction under which the service is operated;
- 962 b) if different to the above, the legal jurisdiction under which subscriber and any
963 relying party agreements are entered into;
- 964 c) applicable legislation with which the service complies;
- 965 d) obligations incumbent upon the CSP;
- 966 e) obligations incumbent upon the subscriber;
- 967 f) notifications and guidance for relying parties, especially in respect of actions they
968 are expected to take should they choose to rely upon the service's product;
- 969 g) statement of warranties;
- 970 h) statement of liabilities;
- 971 i) procedures for notification of changes to terms and conditions;
- 972 j) steps the CSP will take in the event that it chooses or is obliged to terminate the
973 service;
- 974 k) full contact details for the CSP (i.e., conventional post, telephone, Internet)
975 including a help desk;
- 976 l) availability of the specified service *per se* and of its help desk facility;
- 977 m) termination of aspects or all of service.

978 **AL4_CO_NUI#030** **Due Notification**

979 Have in place and follow appropriate policy and procedures to ensure that it notifies
980 subscribers in a timely and reliable fashion of any changes to the service definition and
981 any applicable terms, conditions, fees, and privacy policy for the specified service and
982 provides a clear means by which subscribers may indicate that they wish to accept the
983 new terms or terminate their subscription.

984 **AL4_CO_NUI#050** **Subscriber Information**

985 Require the subscriber to provide full and correct information as required under the terms
986 of their use of the service.

987 **AL4_CO_NUI#060** **Subscriber Agreement**

988 Obtain a record (hard-copy or electronic) of the subscriber's agreement to the terms and
989 conditions of service.

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

991 Require and provide the mechanisms for the subscriber to provide in a timely manner full
992 and correct amendments should any of their recorded information change, as required

993 under the terms of their use of the service, and only after the subscriber's identity has
994 been authenticated.

995 **AL4_CO_NUI#080 Helpdesk facility**

996 Ensure that its help desk is available for any queries related to the specified service
997 during the regular business hours of its primary operational location, excepting
998 nationally-recognized holidays.

999

1000 **3.5.4.3 Information Security Management**

1001 These criteria address the way in which the enterprise manages the security of its
1002 business, the specified service, and information it holds relating to its user community.
1003 This section focuses on the key components that comprise a well-established and
1004 effective Information Security Management System (ISMS), or other IT security
1005 management methodology recognized by a government or professional body.

1006 An enterprise and its specified service must:

1007 **AL4_CO_ISM#010 Documented policies and procedures**

1008 Have documented all security-relevant administrative, management, and technical
1009 policies and procedures. The enterprise must ensure that these are based upon recognized
1010 standards or published references, are adequate for the specified service, and are applied
1011 in the manner intended.

1012 **AL4_CO_ISM#020 Policy Management and Responsibility**

1013 Have a clearly defined managerial role, at a senior level, where full responsibility for the
1014 business' security policies is vested and from which promulgation of policy and related
1015 procedures is controlled and managed. The policies in place must be properly maintained
1016 so as to be effective at all times.

1017 **AL4_CO_ISM#030 Risk Management**

1018 Demonstrate a risk management methodology that adequately identifies and mitigates
1019 risks related to the specified service and its user community and must show that on-going
1020 risk assessment review is conducted as a part of the business' procedures, such as
1021 adherence to SAS 70 or ISO 27001 methodologies.

1022 **AL4_CO_ISM#040** **Continuity of Operations Plan**

1023 Have and shall keep updated a continuity of operations plan that covers disaster recovery
1024 and the resilience of the specified service and must show that on-going review of this
1025 plan is conducted as a part of the business' procedures.

1026 **AL4_CO_ISM#050** **Configuration Management**

1027 Demonstrate a configuration management system that at least includes:

- 1028 a) version control for software system components;
- 1029 b) timely identification and installation of all applicable patches for any software
1030 used in the provisioning of the specified service;
- 1031 c) version control and managed distribution for all documentation associated with
1032 the specification, management, and operation of the system, covering both
1033 internal and publicly available materials.

1034 **AL4_CO_ISM#060** **Quality Management**

1035 Demonstrate a quality management system that is appropriate for the specified service.

1036 **AL4_CO_ISM#070** **System Installation and Operation Controls**

1037 Apply controls during system development, procurement, installation, and operation that
1038 protect the security and integrity of the system environment, hardware, software, and
1039 communications having particular regard to:

- 1040 a) the software and hardware development environments, for customized
1041 components;
- 1042 b) the procurement process for COTS components;
- 1043 c) contracted consultancy/support services;
- 1044 d) shipment of system components;
- 1045 e) storage of system components;
- 1046 f) installation environment security;
- 1047 g) system configuration;
- 1048 h) transfer to operational status.

1049 **AL4_CO_ISM#080** **Internal Service Audit**

1050 Unless it can show that by reason of its size or for other arguable operational reason it is
1051 unreasonable so to perform, be regularly audited for effective provision of the specified
1052 service by internal audit functions independent of the parts of the enterprise responsible
1053 for the specified service.

1054 **AL4_CO_ISM#090** **Independent Audit**

1055 Be audited by an independent auditor at least every 24 months to ensure the
1056 organization's security-related practices are consistent with the policies and procedures
1057 for the specified service and the appointed auditor must have appropriate accreditation or
1058 other acceptable experience and qualification.

1059 **AL4_CO_ISM#100** **Audit Records**

1060 Retain full records of all audits, both internal and independent, for a period which, as a
1061 minimum, fulfils its legal obligations and otherwise for greater periods either as it may
1062 have committed to in its service definition or required by any other obligations it has
1063 with/to a subscriber. Such records must be held securely and protected against loss,
1064 alteration, or destruction.

1065 **AL4_CO_ISM#110** **Termination provisions**

1066 Have in place a clear plan for the protection of subscribers' private and secret information
1067 related to their use of the service which must ensure the ongoing secure preservation and
1068 protection of legally-required records and for the secure destruction and disposal of any
1069 such information whose retention is not legally required. Essential details of this plan
1070 must be published.

1071 **AL4_CO_ISM#120** **Best Practice Security Management**

1072 Have in place a certified Information Security Management System (ISMS), or other IT
1073 security management methodology recognized by a government or professional body,
1074 that has been assessed and found to be in compliance with the code of practice ISO/IEC
1075 17799 [ISO/IEC17799] through application of practices defined in BS 7799 Part 2
1076 [BSI7799-2] and which applies and is appropriate to the CSP in question. All
1077 requirements expressed in preceding criteria in this "ISM" section must *inter alia* fall
1078 wholly within the scope of this ISMS, or the selected recognized alternative.

1079

1080 **3.5.4.4 Security-Related (Audit) Records**

1081 The criteria in this section are concerned with the need to provide an auditable log of all
1082 events that are pertinent to the correct and secure operation of the service.

1083 An enterprise and its specified service must:

1084 **AL4_CO_SER#010** **Security Event Logging**

1085 Maintain a log of all security-relevant events concerning the operation of the service,
1086 together with a precise record of the time at which the event occurred (time-stamp)

1087 provided by a trusted time-source and such records must be retained with appropriate
1088 protection, accounting for service definition, risk management requirements, and
1089 applicable legislation.

1090

1091 **3.5.4.5 Operational Infrastructure**

1092 The criteria in this section address the infrastructure within which the delivery of the
1093 specified service takes place. It puts particular emphasis upon the personnel involved,
1094 and their selection, training, and duties.

1095 An enterprise and its specified service must:

1096 **AL4_CO_OPN#010 Technical Security**

1097 Demonstrate that the technical controls employed will provide the level of security
1098 required by the risk assessment plan and the ISMS, or other IT security management
1099 methodology recognized by a government or professional body, and that these controls
1100 are effectively integrated with the appropriate procedural and physical security measures.

1101 **AL4_CO_OPN#020 Defined Security Roles**

1102 Define, by means of a job description, the roles and responsibilities for every security-
1103 relevant task, relating it to specific procedures (which shall be set out in the ISMS, or
1104 other IT security management methodology recognized by a government or professional
1105 body) and other job descriptions. Where the role is security-critical or where special
1106 privileges or shared duties exist, these must be specifically highlighted, including access
1107 privileges relating to logical and physical parts of the service's operations.

1108 **AL4_CO_OPN#030 Personnel Recruitment**

1109 Demonstrate that it has defined practices for the selection, vetting, and contracting of all
1110 personnel, both direct employees and those whose services are provided by third parties.
1111 Full records of all searches and supporting evidence of qualifications and past
1112 employment must be kept for the duration of the individual's employment plus the longest
1113 lifespan of any credential issued under the service policy.

1114 **AL4_CO_OPN#040 Personnel skills**

1115 Ensure that employees are sufficiently trained, qualified, experienced, and current for the
1116 roles they fulfill. Such measures must be accomplished either by recruitment practices or
1117 through a specific training program. Where employees are undergoing on-the-job
1118 training, they must only do so under the guidance of a mentor with established leadership
1119 skills.

1120 **AL4_CO_OPN#050 Adequacy of Personnel resources**

1121 Have sufficient staff to operate the specified service according to its policies and
1122 procedures.

1123 **AL4_CO_OPN#060 Physical access control**

1124 Apply physical access control mechanisms to ensure access to sensitive areas is restricted
1125 to authorized personnel.

1126 **AL4_CO_OPN#070 Logical access control**

1127 Employ logical access control mechanisms to ensure access to sensitive system functions
1128 and controls is restricted to authorized personnel.

1129

1130 **3.5.4.6 External Services and Components**

1131 This section addresses the relationships and obligations upon contracted parties both to
1132 apply the policies and procedures of the enterprise and also to be available for assessment
1133 as critical parts of the overall service provision.

1134 An enterprise and its specified service must:

1135 **AL4_CO_ESC#010 Contracted Policies and Procedures**

1136 Where the enterprise uses the services of external suppliers for specific packaged
1137 components of the service or for resources which are integrated with its own operations
1138 and under its controls, ensure that those parties are engaged through reliable and
1139 appropriate contractual arrangements which stipulate critical policies, procedures, and
1140 practices that the sub-contractor is required to fulfill.

1141 **AL4_CO_ESC#020 Visibility of Contracted Parties**

1142 Where the enterprise uses the services of external suppliers for specific packaged
1143 components of the service or for resources which are integrated with its own operations
1144 and under its controls, ensure that contractors' compliance with contractually stipulated
1145 policies and procedures, and thus with the IAEG's assessment criteria, can be proven and
1146 subsequently monitored.

1147

1148 **3.5.4.7 Secure Communications**

1149 An enterprise and its specified service must:

1150 **AL4_CO_SCO#010** **Secure remote communications**

1151 If the specific service components are located remotely from and communicate over a
1152 public or unsecured network with other service components or other CSP(s) it services,
1153 the communications must be cryptographically authenticated by an authentication
1154 protocol that meets the requirements of AL4 and encrypted using an approved encryption
1155 method, as established by a national technical authority.

1156 **AL4_CO_SCO#020** **Protection of secrets**

1157 Ensure that:

- 1158 a) access to shared secrets shall be subject to discretionary controls which permit
1159 access to those roles/applications which need such access;
- 1160 b) stored shared secrets are encrypted such that:
 - 1161 i the encryption key for the shared secret file is encrypted under a key held
1162 in a FIPS 140-2 [FIPS140-2] Level 2 (or higher) validated hardware
1163 cryptographic module, or equivalent, as established by a recognized
1164 national technical authority, or any FIPS 140-2 Level 3 or 4 cryptographic
1165 module, or equivalent, as established by a recognized national technical
1166 authority, and decrypted only as immediately required for an
1167 authentication operation.
 - 1168 ii they are protected as a key within the boundary of a FIPS 140-2 Level 2
1169 (or higher) validated hardware cryptographic module, or equivalent, as
1170 established by a recognized national technical authority, or any FIPS 140-
1171 2 Level 3 or 4 cryptographic module, or equivalent, as established by a
1172 recognized national technical authority, and are not exported in plaintext
1173 from the module.
 - 1174 iii they are split by an "*n from m*" cryptographic secret-sharing method.
- 1175 c) any long-term (i.e., not session) shared secrets are revealed only to the subscriber
1176 and the CSP's direct agents (bearing in mind (a) above).
- 1177

1178 **3.6 Identity Proofing Service Assessment Criteria**

1179 The Service Assessment Criteria in this section establish the requirements for the
1180 technical conformity of identity proofing services at all ALs defined in Section 2. These
1181 criteria apply to a particular kind of electronic trust service (ETS) recognized by the
1182 IAEG and to the related credential service provider (CSP)—an identity proofing service

1183 for both individual identity and institutional identity credentials¹. (For definitions of
1184 terms used in this section, see Section 6). These criteria are generally referred to
1185 elsewhere within IAEG documentation as ID-SAC [ID-SAC].

1186 These criteria do not address the delivery of a credential to the applicant/subscriber,
1187 which is dealt with by the Credential Management SAC (CM-SAC), described in Section
1188 3.7.

1189 These criteria may only be used in an assessment in one of the following circumstances:

- 1190 • In conjunction with the Common Organizational SAC (CO-SAC), described in
1191 Section 3.5, for a standalone identity proofing service.
- 1192 • In combination with one or more other SACs that must include the CO-SAC and
1193 where the identity proofing functions that these criteria address form part of a
1194 larger service offering.

1195 Note: Some of the SAC-identifying numbers are not used in all of the ALs. In such cases,
1196 the particular SAC number has been reserved where not used and skipped.

1197 **3.6.1 Assurance Level 1**

1198 **3.6.1.1 Policy**

1199 An enterprise or specified service must:

1200 **AL1_ID_POL#010 Unique service identity**

1201 Ensure that a unique identity is attributed to the specific service, such that credentials
1202 issued by it can be distinguishable from those issued by other services, including services
1203 operated by the same enterprise.

1204 **AL1_ID_POL#020 Unique subject identity**

1205 Ensure that each applicant's identity is unique within the service's community of subjects
1206 and uniquely associable with tokens and/or credentials issued to that identity.

1207

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.

1208 **3.6.1.2 Identity Verification**

1209 **3.6.1.2.1 In-Person Public Verification**

1210 An enterprise or specified service must:

1211 **AL1_ID_IPV#010 Required evidence**

1212 Accept a self-assertion of identity.

1213 **AL1_ID_IPV#020 Evidence checks**

1214 Accept self-attestation of evidence.

1215

1216 **3.6.1.2.2 Remote Public Verification**

1217 If the specific service offers remote identity proofing to applicants with whom it has no
1218 previous relationship, then it must comply with the criteria in this section.

1219 An enterprise or specified service must:

1220 **AL1_ID_RPV#010 Required evidence**

1221 Require the applicant to provide a contact telephone number or email address.

1222 **AL1_ID_RPV#020 Evidence checks**

1223 Verify the provided information by either:

1224 a) confirming the request by calling the number.

1225 b) successfully sending a confirmatory email and receiving a positive
1226 acknowledgement.

1227

1228 **3.6.1.2.3 Secondary Verification**

1229 In each of the above cases, an enterprise or specified service must:

1230 **AL1_ID_SCV#010 Secondary checks**

1231 Have in place additional measures (e.g., require additional documentary evidence, delay
1232 completion while out-of-band checks are undertaken) to deal with any anomalous
1233 circumstances that can be reasonably anticipated (e.g., a legitimate and recent change of
1234 address that has yet to be established as the address of record).

1235

1236 **3.6.1.3 Verification Records**

1237 No criteria.

1238 **3.6.2 Assurance Level 2**

1239 **3.6.2.1 Policy**

1240 The specific service must show that it applies identity proofing policies and procedures
1241 and that it retains appropriate records of identity proofing activities and evidence.

1242 The enterprise or specified service must:

1243 **AL2_ID_POL#010 Unique service identity**

1244 Ensure that a unique identity is attributed to the specific service, such that credentials
1245 issued by it can be distinguishable from those issued by other services, including services
1246 operated by the same enterprise.

1247 **AL2_ID_POL#020 Unique subject identity**

1248 Ensure that each applicant's identity is unique within the service's community of subjects
1249 and uniquely associable with tokens and/or credentials issued to that identity.

1250 **AL2_ID_POL#030 Published Proofing Policy**

1251 Publish the Identity Proofing Policy under which it verifies the identity of applicants² in
1252 form, language, and media accessible to the declared community of users.

1253 **AL2_ID_POL#040 Adherence to Proofing Policy**

1254 Perform all identity proofing strictly in accordance with its published Identity Proofing
1255 Policy, through application of the procedures and processes set out in its Identity Proofing
1256 Practice Statement.

1257

1258 **3.6.2.2 Identity Verification**

1259 The specific service must offer at least one of the following classes of identity proofing
1260 service and may offer any additional sets it chooses, subject to the nature and the
1261 entitlement of the CSP concerned.

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 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.

1262 **3.6.2.2.1 In-Person Public Verification**

1263 If the specific service offers in-person identity proofing to applicants with whom it has no
1264 previous relationship, then it must comply with the criteria in this section.

1265 The enterprise or specified service must:

1266 **AL2_ID_IPV#010 Required evidence**

1267 Ensure that the applicant is in possession of a primary Government Picture ID document
1268 that bears a photographic image of the holder.

1269 **AL2_ID_IPV#020 Evidence checks**

1270 Ensure that the presented document:

- 1271 a) appears to be a genuine document properly issued by the claimed issuing
1272 authority and valid at the time of application;
 - 1273 b) bears a photographic image of the holder that matches that of the applicant;
 - 1274 c) states an address at which the applicant can be contacted.
- 1275

1276 **3.6.2.2.2 Remote Public Verification**

1277 If the specific service offers remote identity proofing to applicants with whom it has no
1278 previous relationship, then it must comply with the criteria in this section.

1279 An enterprise or specified service must:

1280 **AL2_ID_RPV#010 Required evidence**

1281 Ensure that the applicant submits the references of and attests to current possession of at
1282 least one primary Government Picture ID document, and either a second Government ID
1283 or

- 1284 a) an employee or student ID number; or
- 1285 b) a financial account number (e.g., checking account, savings account, loan or
1286 credit card); or
- 1287 c) a utility service account number (e.g., electricity, gas, or water) for an address
1288 matching that in the primary document.

1289 Ensure that the applicant provides additional verifiable personal information that at a
1290 minimum must include:

- 1291 a) a name that matches the referenced photo-ID;
- 1292 b) date of birth; and
- 1293 c) current address or personal telephone number.

1294 Additional information may be requested so as to ensure a unique identity, and alternative
1295 information may be sought where the enterprise can show that it leads to at least the same
1296 degree of certitude when verified.

1297 **AL2_ID_RPV#020 Evidence checks**

1298 Inspection and analysis of records against the provided identity references with the
1299 specified issuing authorities/institutions or through similar databases:

- 1300 a) the existence of such records with matching name and reference numbers;
1301 b) corroboration of date of birth, current address of record, and other personal
1302 information sufficient to ensure a unique identity.

1303

1304

1305 Confirm address of record by at least one of the following means:

- 1306 a) RA sends notice to an address of record confirmed in the records check and
1307 receives a mailed or telephonic reply from applicant; or
1308 b) RA issues credentials in a manner that confirms the address of record supplied by
1309 the applicant, for example by requiring applicant to enter on-line some
1310 information from a notice sent to the applicant; or
1311 c) RA issues credentials in a manner that confirms ability of the applicant to receive
1312 telephone communications at telephone number or email at email address
1313 associated with the applicant in records. Any secret sent over an unprotected
1314 channel shall be reset upon first use.

1315

1316 Additional checks may be performed so as to establish the uniqueness of the claimed
1317 identity, and alternative checks may be performed where the enterprise can show that they
1318 lead to at least the same degree of certitude.

1319

1320 **3.6.2.2.3 Current Relationship Verification**

1321 If the specific service offers identity proofing to applicants with whom it has a current
1322 relationship, then it must comply with the criteria in this section.

1323 The enterprise or specified service must:

1324 **AL2_ID_CRV#010 Required evidence**

1325 Ensure that it has previously exchanged a shared secret (e.g., a PIN or password) that
1326 meets entropy requirements for the AL with the applicant.

1327 **AL2_ID_CRV#020 Evidence checks**

1328 Ensure that it has:

- 1329 a) only issued the shared secret after originally establishing the applicant's identity
1330 with a degree of rigor equivalent to that required under either the AL2 (or higher)
1331 requirements for in-person or remote public verification
1332 b) an ongoing business relationship sufficient to satisfy the enterprise of the
1333 applicant's continued personal possession of the shared secret.
1334

1335 **3.6.2.2.4 Affiliation Verification**

1336 If the specific service offers identity proofing to applicants on the basis of some form of
1337 affiliation, then it must comply with the criteria in this section for the purposes of
1338 establishing that affiliation, in addition to the previously stated requirements for the
1339 verification of the individual's identity.

1340 The enterprise or specified service must:

1341 **AL2_ID_AFV#010 Required evidence**

1342 Ensure that the applicant possesses:

- 1343 a) identification from the organization with which it is claiming affiliation;
1344 b) agreement from the organization that the applicant may be issued a credential
1345 indicating that an affiliation exists.

1346 **AL2_ID_AFV#020 Evidence checks**

1347 Ensure that the presented documents:

- 1348 a) each appear to be a genuine document properly issued by the claimed issuing
1349 authorities and valid at the time of application;
1350 b) refer to an existing organization with a contact address;
1351 c) indicate that the applicant has some form of recognizable affiliation with the
1352 organization;
1353 d) appear to grant the applicant an entitlement to obtain a credential indicating its
1354 affiliation with the organization.
1355

1356 **3.6.2.2.5 Secondary Verification**

1357 In each of the above cases, the enterprise or specified service must:

1358 **AL2_ID_SCV#010 Secondary checks**

1359 Have in place additional measures (e.g., require additional documentary evidence, delay
1360 completion while out-of-band checks are undertaken) to deal with any anomalous
1361 circumstances that can be reasonably anticipated (e.g., a legitimate and recent change of
1362 address that has yet to be established as the address of record).

1363

1364 **3.6.2.3 Verification Records**

1365 The specific service must retain records of the identity proofing (verification) that it
1366 undertakes.

1367 An enterprise or specified service must:

1368 **AL2_ID_VRC#010 Verification Records for Personal Applicants**

1369 Log, taking account of all applicable legislative and policy obligations, a record of the
1370 facts of the verification process. At a minimum, records of identity information must
1371 include:

- 1372 a) the applicant's full name as shown on the government-issued ID;
- 1373 b) the applicant's date of birth;
- 1374 c) the applicant's current address of record;
- 1375 d) the subscriber's current telephone or email address of record;
- 1376 e) type, issuing authority, and reference number(s) of all documents checked in the
1377 identity proofing process;
- 1378 f) where required, a telephone or email address for related contact and/or delivery of
1379 credentials/notifications;
- 1380 g) any pseudonym used by the applicant in lieu of the verified identity;
- 1381 h) date and time of verification.

1382 **AL2_ID_VRC#020 Verification Records for Affiliated Applicants**

1383 In addition to the foregoing, log, taking account of all applicable legislative and policy
1384 obligations, a record of the additional facts of the verification process. At a minimum,
1385 records of identity information must include:

- 1386 a) the subscriber's full name;
- 1387 b) the subscriber's current address of record;
- 1388 c) the subscriber's current telephone or email address of record;
- 1389 d) the subscriber's acknowledgement for issuing the subject with a credential;
- 1390 e) type, issuing authority, and reference number(s) of all documents checked in the
1391 identity proofing process.

1392 **AL2_ID_VRC#030 Record Retention**

1393 Either retain, securely, the record of the verification process for the duration of the
1394 subscriber account plus 7.5 years, or submit same record to a client CSP that has
1395 undertaken to retain the record for the requisite period or longer.

1396 **3.6.3 Assurance Level 3**

1397 **3.6.3.1 Policy**

1398 The specific service must show that it applies identity proofing policies and procedures
1399 and that it retains appropriate records of identity proofing activities and evidence.

1400 The enterprise or specified service must:

1401 **AL3_ID_POL#010 Unique service identity**

1402 Ensure that a unique identity is attributed to the specific service, such that credentials
1403 issued by it can be distinguishable from those issued by other services, including services
1404 operated by the same enterprise.

1405 **AL3_ID_POL#020 Unique subject identity**

1406 Ensure that each applicant's identity is unique within the service's community of subjects
1407 and uniquely associable with tokens and/or credentials issued to that identity.

1408 **AL3_ID_POL#030 Published Proofing Policy**

1409 Publish the Identity Proofing Policy under which it verifies the identity of applicants³ in
1410 form, language, and media accessible to the declared community of Users.

1411 **AL3_ID_POL#040 Adherence to Proofing Policy**

1412 Perform all identity proofing strictly in accordance with its published Identity Proofing
1413 Policy, applying the procedures and processes set out in its Identity Proofing Practice
1414 Statement.

1415

1416 **3.6.3.2 Identity Verification**

1417 The specific service must offer at least one of the following classes of identity proofing
1418 services and may offer any additional services it chooses, subject to the nature and the
1419 entitlement of the CSP concerned.

³ 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.

1420 **3.6.3.2.1 In-Person Public Verification**

1421 A specific service that offers identity proofing to applicants with whom it has no previous
1422 relationship must comply with the criteria in this section.

1423 The enterprise or specified service must:

1424 **AL3_ID_IPV#010 Required evidence**

1425 Ensure that the applicant is in possession of a primary Government Picture ID document
1426 that bears a photographic image of the holder.

1427 **AL3_ID_IPV#020 Evidence checks**

1428 Ensure that the presented document:

- 1429 a) appears to be a genuine document properly issued by the claimed issuing
1430 authority and valid at the time of application;
- 1431 b) bears a photographic image of the holder that matches that of the applicant;
- 1432 c) states an address at which the applicant can be contacted;
- 1433 d) is electronically verified by a record check with the specified issuing authority or
1434 through similar databases that:
- 1435 i) establishes the existence of such records with matching name and
1436 reference numbers;
- 1437 ii) corroborates date of birth, current address of record, and other personal
1438 information sufficient to ensure a unique identity.
- 1439

1440 **3.6.3.2.2 Remote Public Verification**

1441 A specific service that offers remote identity proofing to applicants with whom it has no
1442 previous relationship must comply with the criteria in this section.

1443 The enterprise or specified service must:

1444 **AL3_ID_RPV#010 Required evidence**

1445 Ensure that the applicant submits the references of and attests to current possession of at
1446 least one primary Government Picture ID document, and either a second Government ID
1447 or

- 1448 a) an employee or student ID number; or
- 1449 b) a financial account number (e.g., checking account, savings account, loan or
1450 credit card); or
- 1451 c) a utility service account number (e.g., electricity, gas, or water) for an address
1452 matching that in the primary document.

1453 Ensure that the applicant provides additional verifiable personal information that at a
1454 minimum must include:

- 1455 a) a name that matches the referenced photo-ID;
- 1456 b) date of birth;
- 1457 c) current address or personal telephone number

1458 **AL3_ID_RPV#020 Evidence checks**

1459 Electronically verify by a record check against the provided identity references with the
1460 specified issuing authorities/institutions or through similar databases:

- 1461 a) the existence of such records with matching name and reference numbers;
- 1462 b) corroboration of date of birth, current address of record or personal telephone
1463 number, and other personal information sufficient to ensure a unique identity;
- 1464 c) dynamic verification of personal information previously provided by or likely to
1465 be known only by the applicant.

1466
1467

1468 Confirm address of record by at least one of the following means:

- 1469 a) RA sends notice to an address of record confirmed in the records check and
1470 receives a mailed or telephonic reply from applicant; or
- 1471 b) RA issues credentials in a manner that confirms the address of record supplied by
1472 the applicant, for example by requiring applicant to enter on-line some
1473 information from a notice sent to the applicant; or
- 1474 c) RA issues credentials in a manner that confirms ability of the applicant to receive
1475 telephone communications at telephone number or e mail at e mail address
1476 associated with the applicant in records. Any secret sent over an unprotected
1477 channel shall be reset upon first use.

1478

1479 Additional checks may be performed so as to establish the uniqueness of the claimed
1480 identity, and alternative checks may be performed where the enterprise can show that they
1481 lead to at least the same degree of certitude.

1482 **3.6.3.2.3 Affiliation Verification**

1483 A specific service that offers identity proofing to applicants on the basis of some form of
1484 affiliation must comply with the criteria in this section to establish that affiliation and
1485 with the previously stated requirements to verify the individual's identity.

1486 The enterprise or specified service must:

1487 **AL3_ID_AFV#010 Required evidence**

1488 Ensure that the applicant possesses:

- 1489 a) identification from the organization with which it is claiming affiliation;
1490 b) agreement from the organization that the applicant may be issued a credential
1491 indicating that an affiliation exists.

1492 **AL3_ID_AFV#020 Evidence checks**

1493 Ensure that the presented documents:

- 1494 a) each appear to be a genuine document properly issued by the claimed issuing
1495 authorities and valid at the time of application;
1496 b) refer to an existing organization with a contact address;
1497 c) indicate that the applicant has some form of recognizable affiliation with the
1498 organization;
1499 d) appear to grant the applicant an entitlement to obtain a credential indicating an
1500 affiliation with the organization.
1501

1502 **3.6.3.2.4 Secondary Verification**

1503 In each of the above cases, the enterprise or specified service must also meet the
1504 following criteria:

1505 **AL3_ID_SCV#010 Secondary checks**

1506 Have in place additional measures (e.g., require additional documentary evidence, delay
1507 completion while out-of-band checks are undertaken) to deal with any anomalous
1508 circumstance that can reasonably be anticipated (e.g., a legitimate and recent change of
1509 address that has yet to be established as the address of record).

1510 **3.6.3.3 Verification Records**

1511 The specific service must retain records of the identity proofing (verification) that it
1512 undertakes.

1513 The enterprise or specified service must:

1514 **AL3_ID_VRC#010 Verification Records**

1515 Log, taking account of all applicable legislative and policy obligations, a record of the
1516 facts of the verification process. At a minimum, records of identity information must
1517 include:

- 1518 a) the applicant's full name as stated on the primary Government Picture ID
1519 documents;
1520 b) the applicant's date and place of birth (as declared, but not necessarily verified);
1521 c) the applicant's current address of record;
1522 d) the subscriber's current telephone or email address of record;

- 1523 e) type, issuing authority, and reference number(s) of all documents checked in the
- 1524 identity proofing process;
- 1525 f) any pseudonym used by the applicant in lieu of the verified identity;
- 1526 g) date and time of verification;
- 1527 h) identity of the registrar;
- 1528 i) identity of the CSP providing the verification service or the location at which the
- 1529 (in-house) verification was performed.

1530 **AL3_ID_VRC#020 Verification Records for Affiliated Applicants**

1531 In addition to the foregoing, log, taking account of all applicable legislative and policy
1532 obligations, a record of the additional facts of the verification process. At a minimum,
1533 records of identity information must include:

- 1534 a) the subscriber's full name;
- 1535 b) the subscriber's current address of record;
- 1536 c) the subscriber's current telephone or email address of record;
- 1537 d) the subscriber's acknowledgement of issuing the subject with a credential;
- 1538 e) type, issuing authority, and reference number(s) of all documents checked in the
- 1539 identity proofing process;
- 1540 f) where required, a telephone or email address for related contact and/or delivery of
- 1541 credentials/notifications.

1542 **AL3_ID_VRC#030 Record Retention**

1543 Either retain, securely, the record of the verification/revocation process for the duration of
1544 the subscriber account plus 7.5 years, or submit the same record to a client CSP that has
1545 undertaken to retain the record for the requisite period or longer.

1546 **3.6.4 Assurance Level 4**

1547 Identity proofing at Assurance Level 4 requires the physical presence of the applicant in
1548 front of the registration officer with photo ID or other readily verifiable biometric identity
1549 information, as well as the requirements set out by the following criteria.

1550 **3.6.4.1 Policy**

1551 The specific service must show that it applies identity proofing policies and procedures
1552 and that it retains appropriate records of identity proofing activities and evidence.

1553 The enterprise or specified service must:

1554 **AL4_ID_POL#010 Unique service identity**

1555 Ensure that a unique identity is attributed to the specific service, such that credentials
1556 issued by it can be distinguishable from those issued by other services, including services
1557 operated by the same enterprise.

1558 **AL4_ID_POL#020 Unique subject identity**

1559 Ensure that each applicant's identity is unique within the service's community of subjects
1560 and uniquely associable with tokens and/or credentials issued to that identity.

1561 **AL4_ID_POL#030 Published Proofing Policy**

1562 Publish the Identity Proofing Policy under which it verifies the identity of applicants⁴ in
1563 form, language, and media accessible to the declared community of users.

1564 **AL4_ID_POL#040 Adherence to Proofing Policy**

1565 Perform all identity proofing strictly in accordance with its published Identity Proofing
1566 Policy, applying the procedures and processes set out in its Identity Proofing Practice
1567 Statement.

1568

1569 **3.6.4.2 Identity Verification**

1570 The specific service may offer only face-to-face identity proofing service. Remote
1571 verification is not allowed at this level.

1572 The enterprise or specified service must:

1573 **3.6.4.2.1 In-Person Public Verification**

1574 **AL4_ID_IPV#010 Required evidence**

1575 Ensure that the applicant is in possession of:

- 1576 a) a primary Government Picture ID document that bears a photographic image of
1577 the holder and either
1578 i) secondary Government Picture ID or an account number issued by a
1579 regulated financial institution, or

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 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.

1615 **AL4_ID_IPV#050** **Applicant knowledge checks**

1616 Where the applicant is unable to satisfy any of the above requirements, that the applicant
1617 can provide a unique identifier, such as a Social Security Number (SSN), that matches the
1618 claimed identity.

1619

1620 **3.6.4.2.2 Affiliation Verification**

1621 A specific service that offers identity proofing to applicants on the basis of some form of
1622 affiliation must comply with the criteria in this section to establish that affiliation, in
1623 addition to complying with the previously stated requirements for verifying the
1624 individual's identity.

1625 The enterprise or specified service must:

1626 **AL4_ID_AJV#010** **Required evidence**

1627 Ensure that the applicant possesses:

- 1628 a) identification from the organization with which the applicant is claiming
1629 affiliation;
- 1630 b) agreement from the organization that the applicant may be issued a credential
1631 indicating that an affiliation exists.

1632 **AL4_ID_AJV#020** **Evidence checks**

1633 Ensure that the presented documents:

- 1634 a) each appear to be a genuine document properly issued by the claimed issuing
1635 authorities and valid at the time of application;
- 1636 b) refer to an existing organization with a contact address;
- 1637 c) indicate that the applicant has some form of recognizable affiliation with the
1638 organization;
- 1639 d) appear to grant the applicant an entitlement to obtain a credential indicating an
1640 affiliation with the organization.

1641

1642 **3.6.4.2.3 Secondary Verification**

1643 In each of the above cases, the enterprise or specified service must also meet the
1644 following criteria:

1645 **AL4_ID_SCV#010** **Secondary checks**

1646 Have in place additional measures (e.g., require additional documentary evidence, delay
1647 completion while out-of-band checks are undertaken) to deal with any anomalous

1648 circumstances that can reasonably be anticipated (e.g., a legitimate and recent change of
1649 address that has yet to be established as the address of record).

1650

1651 **3.6.4.3 Verification Records**

1652 The specific service must retain records of the identity proofing (verification) that it
1653 undertakes.

1654 The enterprise or specified service must:

1655 **AL4_ID_VRC#010 Verification Records for Personal Applicants**

1656 Log, taking account of all applicable legislative and policy obligations, a record of the
1657 facts of the verification process. At a minimum, records of identity information must
1658 include:

- 1659 a) the applicant's full name, as stated on a Government-issued ID document,
- 1660 b) the applicant's date and place of birth (as declared, but not necessarily verified),
- 1661 c) the applicant's current address of record,
- 1662 d) the type, issuing authority, and reference number(s) of all documents checked in
1663 the identity proofing process,
- 1664 e) a telephone or email address for related contact and/or delivery of
1665 credentials/notifications,
- 1666 f) any pseudonym used by the applicant in lieu of the verified identity,
- 1667 g) a biometric record of the applicant (e.g., a photograph, fingerprint, voice
1668 recording),
- 1669 h) date and time of verification issued by a trusted time-source,
- 1670 i) the signature of the applicant,
- 1671 j) identity of the registrar,
- 1672 k) identity of the CSP providing the verification service or the location at which the
1673 (in-house) verification was performed.

1674 **AL4_ID_VRC#020 Verification Records for Affiliated Applicants**

1675 In addition to the foregoing, log, taking account of all applicable legislative and policy
1676 obligations, a record of the additional facts of the verification process. At a minimum,
1677 records of identity information must include:

- 1678 a) the subscriber's full name,
- 1679 b) the subscriber's current address of record,
- 1680 c) the subscriber's current telephone or email address of record,
- 1681 d) the subscriber's authorization for issuing the subject a credential,
- 1682 e) type, issuing authority, and reference number(s) of all documents checked in the
1683 identity proofing process,

- 1684 f) a biometric record of each required representative of the affiliating organization
 1685 (e.g., a photograph, fingerprint, voice recording), as determined by that
 1686 organization's governance rules/charter.

1687 **AL4_ID_VRC#030 Record Retention**

1688 Either retain, securely, the record of the verification/revocation process for the duration of
 1689 the subscriber account plus 10.5 years, or submit the record to a client CSP that has
 1690 undertaken to retain the record for the requisite period or longer.

1691 **3.6.5 Compliance Tables**

1692 Use the following tables to correlate criteria for a particular AL and the evidence offered
 1693 to support compliance.

1694 CSPs preparing for an assessment can use the table appropriate to the level at which they
 1695 are seeking approval to correlate evidence with criteria or to justify non-applicability
 1696 (e.g., "specific service types not offered"). Assessors can use the tables to record
 1697 assessment steps and their determination of compliance or failure.

1698 **Table 3-1. 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	

1699 **Table 3-2. 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_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#010	Required evidence	
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	

1700

1701

Table 3-3. 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_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#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	

1702

1703

Table 3-4. 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	
AL4_ID_IPV#010	Required evidence	
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#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	

1704

1705 3.7 Credential Management Service Assessment Criteria

1706 The Service Assessment Criteria in this section establish requirements for the functional
 1707 conformity of credential management services and their providers at all ALs defined in
 1708 Section 2. These criteria are generally referred to elsewhere within IAEG documentation
 1709 as CM-SAC.

1710 The criteria are divided into five parts. Each part deals with a specific functional aspect
 1711 of the overall credential management process.

1712 This SAC must be used in conjunction with the Common Organizational SAC (CO-
 1713 SAC), described in Section 3.5, and, in addition, must either:

- 1714 • explicitly include the criteria of the Identity Proofing SAC ([ID-SAC]) described
 1715 in Section 3.6, or
- 1716 • rely upon the criteria of the ID-SAC [ID-SAC] being fulfilled by the use of an
 1717 IAEG-approved ID-proofing service.

1718 Note: Some of the SAC-identifying numbers are not used in all of the ALs. In such cases,
 1719 the particular SAC number has been reserved where not used and skipped.

1720 **3.7.1 Part A--Credential Operating Environment**

1721 The criteria in this part deal with the overall operational environment in which the
1722 credential life-cycle management is conducted. The credential management service
1723 assessment criteria must be used in conjunction with the common organizational criteria
1724 described in Section 3.5. In addition, they must either explicitly include the identity
1725 proofing service assessment criteria described in Section 3.6 or rely upon those criteria
1726 being fulfilled by the use of an IAEG-approved identity proofing service.

1727 These criteria describe requirements for the overall operational environment in which
1728 credential lifecycle management is conducted. The common organizational criteria
1729 describe broad requirements. The criteria in this section describe implementation
1730 specifics. Implementation depends on the AL. The procedures and processes required to
1731 create a secure environment for management of credentials and the particular
1732 technologies that are considered strong enough to meet the assurance requirements differ
1733 considerably from level to level.

1734 **3.7.1.1 Assurance Level 1**

1735 These criteria apply to PINs and passwords, as well as SAML assertions.

1736 **3.7.1.1.1 Credential Policy and Practices**

1737 These criteria apply to the policy and practices under which credentials are managed.

1738 An enterprise and its specified service must:

1739 **AL1_CM_CPP#010 Credential Policy and Practice Statement**

1740 No stipulation.

1741

1742 **3.7.1.1.2 Security Controls**

1743 An enterprise and its specified service must:

1744 **AL1_CM_CTR#010 Secret revelation**

1745 No stipulation.

1746 **AL1_CM_CTR#020 Protocol threat risk assessment and controls**

1747 Account for the following protocol threats and apply appropriate controls:

1748 a) password guessing,

1749 b) message replay.

1750 **AL1_CM_CTR#030** **System threat risk assessment and controls**

1751 Account for the following system threats and apply appropriate controls:

- 1752 a) the introduction of malicious code,
- 1753 b) compromised authentication arising from insider action,
- 1754 c) out-of-band attacks by other users and system operators (e.g., shoulder-surfing),
- 1755 d) spoofing of system elements/applications,
- 1756 e) malfeasance on the part of subscribers and subjects.

1757

1758 **3.7.1.1.3 Storage of Long-term Secrets**

1759 An enterprise and its specified service must:

1760 **AL1_CM_STS#010** **Stored Secrets**

1761 *Not* store secrets (such as passwords) as plain text and apply discretionary access controls
1762 that limit access to administrators and those applications that require access.

1763

1764 **3.7.1.1.4 Security-relevant Event (Audit) Records**

1765 No stipulation.

1766 **3.7.1.1.5 Subject Options**

1767 An enterprise and its specified service must:

1768 **AL1_CM_OPN#010** **Changeable PIN/Password**

1769 Permit subjects to change their PINs/passwords.

1770

1771 **3.7.1.2 Assurance Level 2**

1772 These criteria apply to passwords, as well as acceptable SAML assertions.

1773 **3.7.1.2.1 Credential Policy and Practices**

1774 These criteria apply to the policy and practices under which credentials are managed.

1775 An enterprise and its specified service must:

1776 **AL2_CM_CPP#010** **Credential Policy and Practice Statement**

1777 Include in its service definition a description of the policy against which it issues
1778 credentials and the corresponding practices it applies in their management. At a
1779 minimum, the Credential Policy and Practice Statement must specify:

- 1780 a) if applicable, any OIDs related to the Practice and Policy Statement;
1781 b) how users may subscribe to the service/apply for credentials and how users'
1782 credentials will be delivered to them;
1783 c) how subscribers acknowledge receipt of tokens and credentials and what
1784 obligations they accept in so doing (including whether they consent to publication
1785 of their details in credential status directories);
1786 d) how credentials may be renewed, modified, revoked, and suspended, including
1787 how requestors are authenticated or their identity re-proven;
1788 e) what actions a subscriber must take to terminate a subscription.

1789 **AL2_CM_CPP#030 Management Authority**

1790 Have a nominated management body with authority and responsibility for approving the
1791 Credential Policy and Practice Statement and for its implementation.

1792

1793 **3.7.1.2.2 Security Controls**

1794 An enterprise and its specified service must:

1795 **AL2_CM_CTR#010 Secret revelation**

1796 Use communication and authentication protocols that minimize the duration of any clear-
1797 text disclosure of long-term secrets, even when disclosed to trusted parties.

1798 **AL2_CM_CTR#020 Protocol threat risk assessment and controls**

1799 Account for the following protocol threats in its risk assessment and apply controls that
1800 reduce them to acceptable risk levels:

- 1801 a) password guessing,
1802 b) message replay,
1803 c) eavesdropping.

1804 **AL2_CM_CTR#030 System threat risk assessment and controls**

1805 Account for the following system threats in its risk assessment and apply controls that
1806 reduce them to acceptable risk levels:

- 1807 a) the introduction of malicious code;
1808 b) compromised authentication arising from insider action;
1809 c) out-of-band attacks by both users and system operators (e.g., the ubiquitous
1810 shoulder-surfing);
1811 d) spoofing of system elements/applications;
1812 e) malfeasance on the part of subscribers and subjects;
1813 f) intrusions leading to information theft.

1814 **AL2_CM_CTR#040 Specified Service's Key Management**

1815 Specify and observe procedures and processes for the generation, storage, and destruction
1816 of its own cryptographic keys used for securing the specific service's assertions and other
1817 publicized information. At a minimum, these should address:

- 1818 a) the physical security of the environment;
- 1819 b) access control procedures limiting access to the minimum number of authorized
1820 personnel;
- 1821 c) public-key publication mechanisms;
- 1822 d) application of controls deemed necessary as a result of the service's risk
1823 assessment;
- 1824 e) destruction of expired or compromised private keys in a manner that prohibits
1825 their retrieval, or their archival in a manner that prohibits their reuse.

1826

1827 **3.7.1.2.3 Storage of Long-term Secrets**

1828 An enterprise and its specified service must:

1829 **AL2_CM_STS#010 Stored Secrets**

1830 *Not* store secrets (such as passwords) as plain text and apply discretionary access controls
1831 that limit access to administrators and to those applications requiring access.

1832

1833 **3.7.1.2.4 Security-Relevant Event (Audit) Records**

1834 These criteria describe the need to provide an auditable log of all events that are pertinent
1835 to the correct and secure operation of the service. The common organizational criteria
1836 applying to provision of an auditable log of all events pertinent to the correct and secure
1837 operation of the service must also be considered carefully. These criteria carry
1838 implications for credential management operations.

1839 **3.7.1.2.5 Subject Options**

1840 An enterprise and its specified service must:

1841 **AL2_CM_OPN#010 Changeable PIN/Password**

1842 Permit subjects to change their passwords, but employ reasonable practices with respect
1843 to password resets and repeated password failures.

1844

1845 **3.7.1.3 Assurance Level 3**

1846 These criteria apply to one-time password devices and soft crypto applications protected
1847 by passwords or biometric controls, as well as cryptographically-signed SAML
1848 assertions.

1849 **3.7.1.3.1 Credential Policy and Practices**

1850 These criteria apply to the policy and practices under which credentials are managed.

1851 An enterprise and its specified service must:

1852 **AL3_CM_CPP#010 Credential Policy and Practice Statement**

1853 Include in its service definition a full description of the policy against which it issues
1854 credentials and the corresponding practices it applies in their issuance. At a minimum,
1855 the Credential Policy and Practice Statement must specify:

- 1856 a) if applicable, any OIDs related to the Credential Policy and Practice Statement;
- 1857 b) how users may subscribe to the service/apply for credentials and how the users'
1858 credentials will be delivered to them;
- 1859 c) how subscribers acknowledge receipt of tokens and credentials and what
1860 obligations they accept in so doing (including whether they consent to publication
1861 of their details in credential status directories);
- 1862 d) how credentials may be renewed, modified, revoked, and suspended, including
1863 how requestors are authenticated or their identity -proven;
- 1864 e) what actions a subscriber must take to terminate a subscription.

1865 **AL3_CM_CPP#030 Management Authority**

1866 Have a nominated or appointed high-level management body with authority and
1867 responsibility for approving the Certificate Policy and Certification Practice Statement,
1868 including ultimate responsibility for its proper implementation.

1869

1870 **3.7.1.3.2 Security Controls**

1871 **AL3_CM_CTR#020 Protocol threat risk assessment and controls**

1872 Account for the following protocol threats in its risk assessment and apply controls that
1873 reduce them to acceptable risk levels:

- 1874 a) password guessing,
- 1875 b) message replay,
- 1876 c) eavesdropping,
- 1877 d) relying party (verifier) impersonation,
- 1878 e) man-in-the-middle attack.

1879 **AL3_CM_CTR#030 System threat risk assessment and controls**

1880 Account for the following system threats in its risk assessment and apply controls that
1881 reduce them to acceptable risk levels:

- 1882 a) the introduction of malicious code;
- 1883 b) compromised authentication arising from insider action;
- 1884 c) out-of-band attacks by both users and system operators (e.g., shoulder-surfing);
- 1885 d) spoofing of system elements/applications;
- 1886 e) malfeasance on the part of subscribers and subjects;
- 1887 f) intrusions leading to information theft.

1888 **AL3_CM_CTR#040 Specified Service's Key Management**

1889 Specify and observe procedures and processes for the generation, storage, and destruction
1890 of its own cryptographic keys used for securing the specific service's assertions and other
1891 publicized information. At a minimum, these should address:

- 1892 a) the physical security of the environment;
- 1893 b) access control procedures limiting access to the minimum number of authorized
1894 personnel;
- 1895 c) public-key publication mechanisms;
- 1896 d) application of controls deemed necessary as a result of the service's risk
1897 assessment;
- 1898 e) destruction of expired or compromised private keys in a manner that prohibits
1899 their retrieval **or** their archival in a manner that prohibits their reuse.

1900

1901 **3.7.1.3.3 Storage of Long-term Secrets**

1902 An enterprise and its specified service must:

1903 **AL3_CM_STS#010 Stored Secrets**

1904 *Not* store secrets (such as passwords) as plain text and apply discretionary access controls
1905 that limit access to administrators and to those applications that require access.

1906 **AL3_CM_STS#020 Stored Secret Encryption**

1907 Encrypt such shared secret files so that:

- 1908 a) the encryption key for the shared secret file is encrypted under a key held in a
1909 FIPS 140-2 [FIPS140-2] Level 2 or higher validated hardware or software
1910 cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module, or
1911 equivalent, as established by a recognized national technical authority,;
- 1912 b) the shared secret file is decrypted only as immediately required for an
1913 authentication operation;

- 1914 c) shared secrets are protected as a key within the boundary of a FIPS 140-2 Level 2
1915 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or
1916 4 cryptographic module and are not exported from the module in plain text, or
1917 equivalent, as established by a recognized national technical authority,;
1918 d) shared secrets are split by an "*n from m*" cryptographic secret sharing method.
1919

1920 **3.7.1.3.4 Security-relevant Event (Audit) Records**

1921 These criteria describe the need to provide an auditable log of all events that are pertinent
1922 to the correct and secure operation of the service. The common organizational criteria
1923 applying to provision of an auditable log of all security-related events pertinent to the
1924 correct and secure operation of the service must also be considered carefully. These
1925 criteria carry implications for credential management operations.

1926 In the specific context of a certificate management service, an enterprise and its specified
1927 service must:

1928 **AL3_CM_SER#010 Security event logging**

1929 Ensure that such audit records include:

- 1930 a) the identity of the point of registration (irrespective of whether internal or
1931 outsourced);
1932 b) generation of the subscriber's keys or the evidence that the subscriber was in
1933 possession of both parts of their own key-pair;
1934 c) generation of the subscriber's certificate;
1935 d) dissemination of the subscriber's certificate;
1936 e) any revocation or suspension associated with the subscriber's certificate.
1937

1938 **3.7.1.3.5 Subject options**

1939 An enterprise and its specified service must:

1940 **AL3_CM_OPN#010 Changeable PIN/Password**

1941 Permit subjects to change the password used to activate their credentials.
1942

1943 **3.7.1.4 Assurance Level 4**

1944 These criteria apply exclusively to cryptographic technology deployed through a Public
1945 Key Infrastructure. This technology requires hardware tokens protected by password or
1946 biometric controls. No other forms of credential are permitted at AL4.

1947 **3.7.1.4.1 Certification Policy and Practices**

1948 These criteria apply to the policy and practices under which certificates are managed.

1949 An enterprise and its specified service must:

1950 **AL4_CM_CPP#020 Certificate Policy/Certification Practice Statement**

1951 Include in its service definition its full Certificate Policy and the corresponding
1952 Certification and Practice Statement. The Certificate Policy and Certification Practice
1953 Statement must conform to IETF RFC 3647 (2003-11) [[RFC 3647](#)] in their content and
1954 scope or be demonstrably consistent with the content or scope of that RFC. At a
1955 minimum, the Certificate Policy must specify:

- 1956 a) applicable OIDs for each certificate type issued;
- 1957 b) how users may subscribe to the service/apply for certificates, and how certificates
1958 will be issued to them;
- 1959 c) if users present their own keys, how they will be required to demonstrate
1960 possession of the private key;
- 1961 d) if users' keys are generated for them, how the private keys will be delivered to
1962 them;
- 1963 e) how subscribers acknowledge receipt of tokens and credentials and what
1964 obligations they accept in so doing (including whether they consent to publication
1965 of their details in certificate status directories);
- 1966 f) how certificates may be renewed, re-keyed, modified, revoked, and suspended,
1967 including how requestors are authenticated or their identity proven;
- 1968 g) what actions a subscriber must take to terminate their subscription.

1969 **AL4_CM_CPP#030 Management Authority**

1970 Have a nominated or appointed high-level management body with authority and
1971 responsibility for approving the Certificate Policy and Certification Practice Statement,
1972 including ultimate responsibility for its proper implementation.

1973

1974 **3.7.1.4.2 Security Controls**

1975 An enterprise and its specified service must:

1976 **AL4_CM_CTR#020 Protocol threat risk assessment and controls**

1977 Account for the following protocol threats in its risk assessment and apply controls that
1978 reduce them to acceptable risk levels:

- 1979 a) Password guessing,
- 1980 b) Message replay,
- 1981 c) Eavesdropping
- 1982 d) Relying party (verifier) impersonation,
- 1983 e) Man-in-the-middle attack,

1984 f) Session hijacking.

1985 **AL4_CM_CTR#030 System threat risk assessment and controls**

1986 Account for the following system threats in its risk assessment and apply controls that
1987 reduce them to acceptable risk levels:

- 1988 a) the introduction of malicious code;
- 1989 b) compromised authentication arising from insider action;
- 1990 c) out-of-band attacks by both users and system operators (e.g., shoulder-surfing);
- 1991 d) spoofing of system elements/applications;
- 1992 e) malfeasance on the part of subscribers and subjects;
- 1993 f) intrusions leading to information theft.

1994 **AL4_CM_CTR#040 Specified Service's Key Management**

1995 Specify and observe procedures and processes for the generation, storage, and destruction
1996 of its own cryptographic keys used for securing the specific service's assertions and other
1997 publicized information. At a minimum, these should address:

- 1998 a) the physical security of the environment;
- 1999 b) access control procedures limiting access to the minimum number of authorized
2000 personnel;
- 2001 c) public-key publication mechanisms;
- 2002 d) application of controls deemed necessary as a result of the service's risk
2003 assessment;
- 2004 e) destruction of expired or compromised private keys in a manner that prohibits
2005 their retrieval, or their archival in a manner which prohibits their reuse;
- 2006

2007 **3.7.1.4.3 Storage of Long-term Secrets**

2008 The enterprise and its specified service must meet the following criteria:

2009 **AL4_CM_STS#010 Stored Secrets**

- 2010 a) *Not* store secrets (such as private keys) as plain text, and
- 2011 b) apply discretionary access controls that limit access to trusted administrators and
2012 to those applications that require access.

2013 **AL4_CM_STS#020 Stored Secret Encryption**

2014 Encrypt such secret files so that:

- 2015 a) the encryption key for the secret file is encrypted under a key held in a FIPS 140-
2016 2 [FIPS140-2] Level 2 or higher validated hardware cryptographic module or any

- 2017 FIPS 140-2 Level 3 or 4 cryptographic module, or equivalent, as established by a
2018 recognized national technical authority;
- 2019 b) the secret file is decrypted only as immediately required for a key recovery
2020 operation;
- 2021 c) secrets are protected as a key within the boundary of a FIPS 140-2 Level 2 or
2022 higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4
2023 cryptographic module and are not exported from the module in plaintext, or
2024 equivalent, as established by a recognized national technical authority;
- 2025 d) escrowed secrets are split by an "*n from m*" cryptographic secret storing method.
2026

2027 **3.7.1.4.4 Security-relevant Event (Audit) Records**

2028 These criteria describe the need to provide an auditable log of all events that are pertinent
2029 to the correct and secure operation of the service. The common organizational criteria
2030 relating to the recording of all security-related events must also be considered carefully.

2031 These criteria carry implications for credential management operations.

2032 An enterprise and its specified service must:

2033 **AL4_CM_SER#010 Security event logging**

2034 Ensure that such audit records include:

- 2035 a) the identity of the point of registration (whether internal or outsourced);
2036 b) generation of the subscriber's keys or evidence that the subscriber was in
2037 possession of both parts of the key-pair;
- 2038 c) generation of the subscriber's certificate;
2039 d) dissemination of the subscriber's certificate;
2040 e) any revocation or suspension associated with the subscriber's credential.

2041

2042 **3.7.1.4.5 Subject Options**

2043 An enterprise and its specified service must:

2044 **AL4_CM_OPN#010 Changeable PIN/Password**

2045 Permit subjects to change the passwords used to activate their credentials.

2046 **3.7.2 Part B--Credential Issuing**

2047 These criteria apply to the verification of the identity of the subject of a credential and
2048 with token strength and credential delivery mechanisms. They address requirements

2049 levied by the use of various technologies to achieve the appropriate AL⁵. These criteria
2050 include by reference all applicable criteria in Section 3.6.

2051 **3.7.2.1 Assurance Level 1**

2052 **3.7.2.1.1 Identity Proofing**

2053 These criteria determine how the enterprise shows compliance with the criteria for
2054 fulfilling identity proofing functions.

2055 The enterprise and its specified service must:

2056 **AL1_CM_IDP#010 Self-managed Identity Proofing**

2057 If the enterprise assumes direct responsibility for identity proofing functions, show, by
2058 direct inclusion, compliance with all applicable identity proofing service assessment
2059 criteria⁶ ([ID-SAC]) for AL1 or higher.

2060 **AL1_CM_IDP#020 IAEG-approved outsourced service**

2061 If the enterprise outsources responsibility for identity proofing functions and uses a
2062 service already operating under an IAEG Identity Proofing Approval, show that the
2063 service in question has been approved at AL1 or higher.

2064 **AL1_CM_IDP#030 Non IAEG-approved outsourced service**

2065 If the enterprise outsources responsibility for identity proofing functions, ensure that each
2066 provider of such a service demonstrates compliance with all applicable identity proofing
2067 service assessment criteria for AL1 or higher, and that the enterprise, itself, has in place
2068 controls to ensure the continued fulfillment of those criteria by the provider to which the
2069 functions have been outsourced.

2070 **AL1_CM_IDP#040 Revision to subscriber information**

2071 Provide a means for subscribers to amend their stored information after registration.
2072

⁵ Largely driven by the guidance in NIST SP 800-63 [NIST800-63].

⁶ 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.

2073 **3.7.2.1.2 Credential Creation**

2074 These criteria address the requirements for creation of credentials that can only be used at
2075 AL1. Any credentials/tokens that comply with the criteria stipulated for AL2 and higher
2076 are acceptable at AL1.

2077 An enterprise and its specified service must:

2078 **AL1_CM_CRN_#010 Authenticated Request**

2079 Only accept a request to generate a credential and bind it to an identity if the source of the
2080 request can be authenticated as being authorized to perform identity proofing at AL1 or
2081 higher.

2082 **AL1_CM_CRN_#020 Unique identity**

2083 Ensure that the identity to which a credential refers is unique within the specified
2084 service's community, including identities previously used and that are now cancelled.
2085 This requirement is intended to prevent identities that may exist in a Relying Party's
2086 access control list from possibly representing a different physical person.

2087 **AL1_CM_CRN_#030 Credential uniqueness**

2088 Allow the subscriber to select a credential (e.g., UserID) that is verified to be unique
2089 within the specified service's community and assigned uniquely to a single identity
2090 subject.

2091

2092 **3.7.2.2 Assurance Level 2**

2093 **3.7.2.2.1 Identity Proofing**

2094 These criteria determine how the enterprise shows compliance with the criteria for
2095 fulfilling identity proofing functions.

2096 The enterprise and its specified service must:

2097 **AL2_CM_IDP#010 Self-managed Identity Proofing**

2098 If the enterprise assumes direct responsibility for identity proofing functions, show, by
2099 direct inclusion, compliance with all applicable identity proofing service assessment
2100 criteria for AL2 or higher.

2101 **AL2_CM_IDP#020 IAEG-approved outsourced service**

2102 If the enterprise outsources responsibility for identity proofing functions and uses a
2103 service already operating under an IAEG Identity Proofing Approval, show that the

2104 service in question has been approved at AL2 or higher and that its approval has at least 6
2105 months of remaining validity.

2106 **AL2_CM_IDP#030 Non IAEG-approved outsourced service**

2107 If the enterprise outsources responsibility for identity proofing functions, ensure that each
2108 provider of such a service demonstrates compliance with all applicable identity proofing
2109 service assessment criteria for AL2 or higher, and that the enterprise, itself, has in place
2110 controls to ensure the continued fulfillment of those criteria by the provider to which the
2111 functions have been outsourced.

2112 **AL2_CM_IDP#040 Revision to subscriber information**

2113 Provide a means for subscribers to securely amend their stored information after
2114 registration, either by re-proving their identity, as in the initial registration process, or by
2115 using their credentials to authenticate their revision.

2116

2117 **3.7.2.2 Credential Creation**

2118 These criteria define the requirements for creation of credentials whose highest use is at
2119 AL2. Credentials/tokens that comply with the criteria stipulated at AL3 and higher are
2120 also acceptable at AL2 and below.

2121 Note, however, that a token and credential required by a higher AL but created according
2122 to these criteria may not necessarily provide that higher level of assurance for the claimed
2123 identity of the subscriber. Authentication can only be provided at the assurance level at
2124 which the identity is proven.

2125 An enterprise and its specified service must:

2126 **AL2_CM_CRN_#010 Authenticated Request**

2127 Only accept a request to generate a credential and bind it to an identity if the source of the
2128 request can be authenticated, i.e., Registration Authority, as being authorized to perform
2129 identity proofing at AL2 or higher.

2130 **AL2_CM_CRN_#020 Unique identity**

2131 Ensure that the identity to which a credential refers is unique within the specified
2132 service's community, including identities previously used and that are now cancelled.
2133 This requirement is intended to prevent identities that may exist in a Relying Party's
2134 access control list from possibly representing a different physical person.

2135 **AL2_CM_CRN_#030** **Credential uniqueness**

2136 Allow the subscriber to select a credential (e.g., UserID) that is verified to be unique
2137 within the specified service's community and assigned uniquely to a single identity
2138 subject.

2139 **AL2_CM_CRN_#040** **Password strength**

2140 Only allow passwords that, over the life of the password, have resistance to an on-line
2141 guessing attack against a selected user/password of at least 1 in 2^{14} (16,384), accounting
2142 for state-of-the-art attack strategies.

2143 **AL2_CM_CRN_#050** **One-time password strength**

2144 Only allow password tokens that have a resistance to online guessing attack against a
2145 selected user/password of at least 1 in 2^{14} (16,384), accounting for state-of-the-art attack
2146 strategies.

2147 **AL2_CM_CRN_#060** **Software cryptographic token strength**

2148 Ensure that software cryptographic keys stored on general-purpose devices:

- 2149 a) are protected by a key and cryptographic protocol that are evaluated against FIPS
2150 140-2 Level 2, or equivalent, as established by a recognized national technical
2151 authority;
- 2152 b) require password or biometric activation by the subscriber or employ a password
2153 protocol when being used for authentication.
2154

2155 **AL2_CM_CRN_#070** **Hardware token strength**

2156 Ensure that hardware tokens used to store cryptographic keys:

- 2157 a) employ a cryptographic module that is evaluated against FIPS 140-2 Level 1 or
2158 higher, or equivalent, as established by a recognized national technical authority;
- 2159 b) require password or biometric activation by the subscriber or also employ a
2160 password when being used for authentication.
2161

2162 **AL2_CM_CRN_#080** **Binding of key**

2163 No stipulation.

2164 **AL2_CM_CRN_#090 Nature of subject**

2165 Record the nature of the subject of the credential (which must correspond to the manner
2166 of identity proofing performed), i.e., physical person, a named person acting on behalf of
2167 a corporation or other legal entity, corporation or legal entity, or corporate machine entity,
2168 in a manner that can be unequivocally associated with the credential and the identity that
2169 it asserts.

2170 **3.7.2.2.3 Credential Delivery**

2171 An enterprise and its specified service must:

2172 **AL2_CM_CRD_#010 Notify Subject of Credential Issuance**

2173 Notify the subject of the credential's issuance and, if necessary, confirm the Subject's
2174 contact information by:

- 2175 a) sending notice to the address of record confirmed during identity proofing or
- 2176 b) issuing the credential(s) in a manner that confirms the address of record supplied
2177 by the applicant during identity proofing or
- 2178 c) issuing the credential(s) in a manner that confirms the ability of the applicant to
2179 receive telephone communications at a telephone number or email at an email
2180 address supplied by the applicant during identity proofing.

2182 **3.7.2.3 Assurance Level 3**

2183 **3.7.2.3.1 Identity Proofing**

2184 These criteria in this section determine how the enterprise shows compliance with the
2185 criteria for fulfilling identity proofing functions.

2186 The enterprise and its specified service must:

2187 **AL3_CM_IDP#010 Self-managed Identity Proofing**

2188 If the enterprise assumes direct responsibility for identity proofing functions, show, by
2189 direct inclusion, compliance with all applicable identity proofing service assessment
2190 criteria for AL3 or AL4.

2191 **AL3_CM_IDP#020 IAEG-approved outsourced service**

2192 If the enterprise outsources responsibility for identity proofing functions and uses a
2193 service already operating under an IAEG Identity Proofing Approval, show that the
2194 service in question has been approved at AL3 or AL4 and that its approval has at least 6
2195 months of remaining validity.

2196 **AL3_CM_IDP#030 Non IAEG-approved outsourced service**

2197 *Not* use any non-IAEG-approved outsourced services for identity proofing unless they
2198 can be demonstrated to have satisfied equivalently rigorous requirements established by
2199 another scheme recognized by IAEG.

2200 **AL3_CM_IDP#040 Revision to subscriber information**

2201 Provide a means for subscribers to securely amend their stored information after
2202 registration, either by re-proving their identity as in the initial registration process or by
2203 using their credentials to authenticate their revision. Successful revision must, where
2204 necessary, instigate the re-issuance of the credential.

2205

2206 **3.7.2.3.2 Credential Creation**

2207 These criteria define the requirements for creation of credentials whose highest use is
2208 AL3. Any credentials/tokens that comply with the criteria stipulated at AL4 are also
2209 acceptable at AL3 and below.

2210 Note, however, that a token and credential type required by a higher AL but created
2211 according to these criteria may not necessarily provide that higher level of assurance for
2212 the claimed identity of the subscriber. Authentication can only be provided at the
2213 assurance level at which the identity is proven.

2214 An enterprise and its specified service must:

2215 **AL3_CM_CRN_#010 Authenticated Request**

2216 Only accept a request to generate a credential and bind it to an identity if the source of the
2217 request, i.e., Registration Authority, can be authenticated as being authorized to perform
2218 identity proofing at AL3 or higher.

2219 **AL3_CM_CRN_#020 Unique identity**

2220 Ensure that the identity to which a credential refers is unique within the specified
2221 service's intended community, including identities previously used and that are now
2222 cancelled. This requirement is intended to prevent identities that may exist in a Relying
2223 Party's access control lists from possibly representing a different physical person.

2224 **AL3_CM_CRN_#030 Credential uniqueness**

2225 Allow the subscriber to select a credential (e.g., UserID) that is verified to be unique
2226 within the specified service's community and assigned uniquely to a single identity.

2227 **AL3_CM_CRN_#040 PIN/Password strength**

2228 Not use PIN/password tokens.

2229 **AL3_CM_CRN_#050 One-time password strength**

2230 Only allow one-time password tokens that:

- 2231 a) depend on a symmetric key stored on a personal hardware device evaluated
- 2232 against FIPS 140-2 [FIPS140-2] Level 1 or higher, or equivalent, as established
- 2233 by a recognized national technical authority;
- 2234 b) permit at least 10^6 possible password values;
- 2235 c) require password or biometric activation by the subscriber.

2236 **AL3_CM_CRN_#060 Software cryptographic token strength**

2237 Ensure that software cryptographic keys stored on general-purpose devices:

- 2238 c) are protected by a key and cryptographic protocol that are evaluated against FIPS
- 2239 140-2 Level 2, or equivalent, as established by a recognized national technical
- 2240 authority;
- 2241 d) require password or biometric activation by the subscriber or employ a password
- 2242 protocol when being used for authentication.

2243 **AL3_CM_CRN_#070 Hardware token strength**

2244 Ensure that hardware tokens used to store cryptographic keys:

- 2245 a) employ a cryptographic module that is evaluated against FIPS 140-2 Level 1 or
- 2246 higher, or equivalent, as established by a recognized national technical authority;
- 2247 b) require password or biometric activation by the subscriber or also employ a
- 2248 password when being used for authentication.

2249 **AL3_CM_CRN_#080 Binding of key**

2250 If the specified service generates the subject's key pair, that the key generation process

2251 securely and uniquely binds that process to the certificate generation and maintains at all

2252 times the secrecy of the private key, until it is accepted by the subject.

2253 **AL3_CM_CRN_#090 Nature of subject**

2254 Record the nature of the subject of the credential (which must correspond to the manner

2255 of identity proofing performed), i.e., private person, a named person acting on behalf of a

2256 corporation or other legal entity, corporation or legal entity, or corporate machine entity,

2257 in a manner that can be unequivocally associated with the credential and the identity that

2258 it asserts.

2259

2260 **3.7.2.3.3 Subject Key Pair Generation**

2261 An enterprise and its specified service must:

2262 **AL3_CM_SKP_#010 Key generation by Specified Service**

2263 If the specified service generates the subject's keys:

- 2264 a) use a FIPS-approved [FIPS] algorithm, or equivalent, as established by a
- 2265 recognized national technical authority, that is recognized as being fit for the
- 2266 purposes of the service;
- 2267 b) only create keys of a key length and for use with a FIPS-approved public key
- 2268 algorithm, or equivalent, as established by a recognized national technical
- 2269 authority, recognized as being fit for the purposes of the service;
- 2270 c) generate and store the keys securely until delivery to and acceptance by the
- 2271 subject;
- 2272 d) deliver the subject's private key in a manner that ensures that the privacy of the
- 2273 key is not compromised and only the subject has access to the private key.

2274 **AL3_CM_SKP_#020 Key generation by Subject**

2275 If the subject generates and presents its own keys, obtain the subject's written
2276 confirmation that it has:

- 2277 a) used a FIPS-approved algorithm, or equivalent, as established by a recognized
- 2278 national technical authority, that is recognized as being fit for the purposes of the
- 2279 service;
- 2280 b) created keys of a key length and for use with a FIPS-approved public key
- 2281 algorithm, or equivalent, as established by a recognized national technical
- 2282 authority, recognized as being fit for the purposes of the service.
- 2283

2284 **3.7.2.3.4 Credential Delivery**

2285 An enterprise and its specified service must:

2286 **AL3_CM_CRD_#010 Notify Subject of Credential Issuance**

2287 Notify the subject of the credential's issuance and, if necessary, confirm Subject's contact
2288 information by:

- 2289 a) sending notice to the address of record confirmed during identity proofing, and
- 2290 either
- 2291 i) issuing the credential(s) in a manner that confirms the address of record
- 2292 supplied by the applicant during identity proofing; or
- 2293 ii) issuing the credential(s) in a manner that confirms the ability of the
- 2294 applicant to receive telephone communications at a phone number

2295 supplied by the applicant during identity proofing while recording the
2296 applicant's voice.

2297 **AL3_CM_CRD_#020 Subject's acknowledgement**

2298 Receive acknowledgement of receipt of the credential before it is activated and its
2299 directory status record is published (and thereby the subscription becomes active or re-
2300 activated, depending upon the circumstances of issue).

2301

2302 **3.7.2.4 Assurance Level 4**

2303 **3.7.2.4.1 Identity Proofing**

2304 These criteria determine how the enterprise shows compliance with the criteria for
2305 fulfilling identity proofing functions.

2306 An enterprise and its specified service must:

2307 **AL4_CM_IDP#010 Self-managed Identity Proofing**

2308 If the enterprise assumes direct responsibility for identity proofing functions, show, by
2309 direct inclusion, compliance with all applicable identity proofing service assessment
2310 criteria for AL4.

2311 **AL4_CM_IDP#020 IAEG-approved outsourced service**

2312 If the enterprise outsources responsibility for identity proofing functions and uses a
2313 service already operating under an IAEG Identity Proofing Approval, show that the
2314 service in question has been approved at AL4 and that its approval has at least 12 months
2315 of remaining validity.

2316 **AL4_CM_IDP#030 Non IAEG-approved outsourced service**

2317 Not use any non-IAEG-approved outsourced services for identity proofing unless they
2318 can be demonstrated to have satisfied equivalently rigorous requirements established by
2319 another scheme recognized by IAEG.

2320 **AL4_CM_IDP#040 Revision to subscriber information**

2321 Provide a means for subscribers to securely amend their stored information after
2322 registration, either by re-proving their identity as in the initial registration process or by
2323 using their credentials to authenticate their revision. Successful revision must, where
2324 necessary, instigate the re-issuance of the credential.

2325 **3.7.2.4.2 Credential Creation**

2326 These criteria define the requirements for creation of credentials whose highest use is
2327 AL4.

2328 Note, however, that a token and credential created according to these criteria may not
2329 necessarily provide that level of assurance for the claimed identity of the subscriber.
2330 Authentication can only be provided at the assurance level at which the identity is proven.

2331 An enterprise and its specified service must:

2332 **AL4_CM_CRN_#010 Authenticated Request**

2333 Only accept a request to generate a credential and bind it to an identity if the source of the
2334 request, i.e., Registration Authority, can be authenticated as being authorized to perform
2335 identity proofing at AL4.

2336 **AL4_CM_CRN_#020 Unique identity**

2337 Ensure that the identity to which a credential refers is unique within the specified
2338 service's community, including identities previously used and that are now cancelled.
2339 This requirement is intended to prevent identities that may exist in a Relying Party's
2340 access control lists from possibly representing a different physical person.

2341 **AL4_CM_CRN_#030 Credential uniqueness**

2342 Allow the subscriber to select a credential (e.g., UserID) that is verified to be unique
2343 within the specified service's community and assigned uniquely to a single identity
2344 subject.

2345 **AL4_CM_CRN_#040 PIN/Password strength**

2346 *Not* use PIN/password tokens.

2347 **AL4_CM_CRN_#050 One-time password strength**

2348 *Not* use one-time password tokens.

2349 **AL4_CM_CRN_#060 Software cryptographic token strength**

2350 *Not* use software cryptographic tokens.

2351 **AL4_CM_CRN_#070 Hardware token strength**

2352 Ensure that hardware tokens used to store cryptographic keys:

- 2353 a) employ a cryptographic module that is evaluated against FIPS 140-2 [FIPS140-2]
2354 Level 2 or higher, or equivalent, as determined by a recognized national technical
2355 authority;
2356 b) are evaluated against FIPS 140-2 Level 3 or higher, or equivalent, as determined
2357 by a recognized national technical authority, for their physical security;
2358 c) require password or biometric activation by the subscriber.

2359 **AL4_CM_CRN_#080 Binding of key**

2360 If the specified service generates the subject's key pair, that the key generation process
2361 securely and uniquely binds that process to the certificate generation and maintains at all
2362 times the secrecy of the private key, until it is accepted by the subject.

2363 **AL4_CM_CRN_#090 Nature of subject**

2364 Record the nature of the subject of the credential, i.e., private person, a named person
2365 acting on behalf of a corporation or other legal entity, corporation or legal entity, or
2366 corporate machine entity, in a manner that can be unequivocally associated with the
2367 credential and the identity that it asserts.

2368

2369 **3.7.2.4.3 Subject Key Pair Generation**

2370 An enterprise and its specified service must:

2371 **AL4_CM_SKP_#010 Key generation by Specified Service**

2372 If the specified service generates the subject's keys:

- 2373 a) use a FIPS-approved [FIPS] algorithm, or equivalent, as established by a
2374 recognized national technical authority, that is recognized as being fit for the
2375 purposes of the service;
2376 b) only create keys of a key length and for use with a FIPS-approved public key
2377 algorithm, or equivalent, as established by a recognized national technical
2378 authority, recognized as being fit for the purposes of the service;
2379 c) generate and store the keys securely until delivery to and acceptance by the
2380 subject;
2381 d) deliver the subject's private key in a manner that ensures that the privacy of the
2382 key is not compromised and only the subject has access to the private key.

2383 **AL4_CM_SKP_#020 Key generation by Subject**

2384 If the subject generates and presents its own keys, obtain the subject's written
2385 confirmation that it has:

- 2386 a) used a FIPS-approved algorithm, or equivalent, as established by a recognized
2387 national technical authority, that is recognized as being fit for the purposes of the
2388 service;
2389 b) created keys of a key length and for use with a FIPS-approved public key
2390 algorithm, or equivalent, as established by a recognized national technical
2391 authority, recognized as being fit for the purposes of the service.
2392

2393 **3.7.2.4.4 Credential Delivery**

2394 An enterprise and its specified service must:

2395 **AL4_CM_CRD_#010 Notify Subject of Credential Issuance**

2396 Notify the subject of the credential's issuance and, if necessary, confirm Subject's contact
2397 information by:

- 2398 a) sending notice to the address of record confirmed during identity proofing;
2399 b) unless the subject presented with a private key, issuing the hardware token to the
2400 subject in a manner that confirms the address of record supplied by the applicant
2401 during identity proofing;
2402 c) issuing the certificate to the subject over a separate channel in a manner that
2403 confirms either the address of record or the email address supplied by the
2404 applicant during identity proofing.

2405 **AL4_CM_CRD_#020 Subject's acknowledgement**

2406 Receive acknowledgement of receipt of the hardware token before it is activated and the
2407 corresponding certificate and its directory status record are published (and thereby the
2408 subscription becomes active or re-activated, depending upon the circumstances of issue).

2409 **3.7.3 Part C--Credential Revocation**

2410 These criteria deal with credential revocation and the determination of the legitimacy of a
2411 revocation request.

2412 **3.7.3.1 Assurance Level 1**

2413 An enterprise and its specified service must:

2414 **3.7.3.1.1 Not used**

2415 **3.7.3.1.2 Not used**

2416 **3.7.3.1.3 Secure Revocation Request**

2417 This criterion applies when revocation requests between remote components of a service
2418 are made over a secured communication.

2419 An enterprise and its specified service must:

2420 **AL1_CM_SRR#010 Submit Request**

2421 Submit a request for revocation to the Credential Issuer service (function), using a
2422 secured network communication, if necessary.

2423

2424 **3.7.3.2 Assurance Level 2**

2425 **3.7.3.2.1 Revocation Procedures**

2426 These criteria address general revocation functions, such as the processes involved and
2427 the basic requirements for publication.

2428 An enterprise and its specified service must:

2429 **AL2_CM_RVP#010 Revocation procedures**

2430 a) State the conditions under which revocation of an issued credential may occur,

2431 b) State the processes by which a revocation request may be submitted,

2432 c) State the persons and organizations from which a revocation request will be
2433 accepted,

2434 d) State the validation steps that will be applied to ensure the validity (identity) of
2435 the Revocant, and

2436 e) State the response time between a revocation request being accepted and the
2437 publication of revised certificate status.

2438 **AL2_CM_RVP#020 Secure status notification**

2439 Ensure that published credential status notification information can be relied upon in
2440 terms of the enterprise of its origin (i.e., its authenticity) and its correctness (i.e., its
2441 integrity).

2442 **AL2_CM_RVP#030 Revocation publication**

2443 Ensure that published credential status notification is revised within 72 hours of the
2444 receipt of a valid revocation request, such that any subsequent attempts to use that
2445 credential in an authentication shall be unsuccessful.

2446 **AL2_CM_RVP#040 Verify revocation identity**

2447 Establish that the identity for which a revocation request is received is one that was
2448 issued by the specified service.

2449 **AL2_CM_RVP#050** **Revocation Records**

2450 Retain a record of any revocation of a credential that is related to a specific identity
2451 previously verified, solely in connection to the stated credential. At a minimum, records
2452 of revocation must include:

- 2453 a) the Revocant's full name;
- 2454 b) the Revocant's authority to revoke (e.g., subscriber themselves, someone acting
2455 with the subscriber's power of attorney, the credential issuer, law enforcement, or
2456 other legal due process);
- 2457 c) the Credential Issuer's identity (if not directly responsible for the identity proofing
2458 service);
- 2459 d) the identity associated with the credential (whether the subscriber's name or a
2460 pseudonym);
- 2461 e) the reason for revocation.

2462 **AL2_CM_RVP#060** **Record Retention**

2463 Retain, securely, the record of the revocation process for the duration of the subscriber's
2464 account plus 7.5 years.

2465 **3.7.3.2.2 Verify Revocant's Identity**

2466 Revocation of a credential requires that the requestor and the nature of the request be
2467 verified as rigorously as the original identity proofing. The enterprise should not act on a
2468 request for revocation without first establishing the validity of the request (if it does not,
2469 itself, determine the need for revocation).

2470 In order to do so, the enterprise and its specified service must:

2471 **AL2_CM_RVR#010** **Verify revocation identity**

2472 Establish that the credential for which a revocation request is received was one that was
2473 issued by the specified service, applying the same process and criteria as would be
2474 applied to an original identity proofing.

2475 **AL2_CM_RVR#020** **Revocation reason**

2476 Establish the reason for the revocation request as being sound and well founded, in
2477 combination with verification of the Revocant, according to AL2_ID_RVR#030,
2478 AL2_ID_RVR#040, or AL2_ID_RVR#050.

2479 **AL2_CM_RVR#030** **Verify Subscriber as Revocant**

2480 When the subscriber seeks revocation of the subscriber's own credential, the enterprise
2481 must:

- 2482 a) if in person, require presentation of a primary Government Picture ID document
2483 that must be electronically verified by a record check against the provided identity
2484 with the specified issuing authority's records, or
2485 b) if remote:
2486 i. electronically verify a signature against records (if available), confirmed
2487 with a call to a telephone number of record, or
2488 ii. authenticate an electronic request as being from the same subscriber,
2489 supported by a credential at Assurance Level 2 or higher.

2490 **AL2_CM_RVR#040 CSP as Revocant**

2491 Where a CSP seeks revocation of a subscriber's credential, the enterprise must establish
2492 that the request is either:

- 2493 a) from the specified service itself, with authorization as determined by established
2494 procedures, or
2495 b) from the client Credential Issuer, by authentication of a formalized request over
2496 the established secure communications network.

2497 **AL2_CM_RVR#050 Verify Legal Representative as Revocant**

2498 Where the request for revocation is made by a law enforcement officer or presentation of
2499 a legal document, the enterprise must:

- 2500 a) if in person, verify the identity of the person presenting the request, or
2501 b) if remote:
2502 i. in paper/facsimile form, verify the origin of the legal document by a
2503 database check or by telephone with the issuing authority, or
2504 ii. authenticate an electronic request as being from a recognized legal office,
2505 supported by a credential at Assurance Level 2 or higher.
2506

2507 **3.7.3.2.3 Secure Revocation Request**

2508 This criterion applies when revocation requests must be communicated between remote
2509 components of the service organization.

2510 An enterprise and its specified service must:

2511 **AL2_CM_SRR#010 Submit Request**

2512 Submit a request for the revocation to the Credential Issuer service (function), using a
2513 secured network communication.

2514

2515 **3.7.3.3 Assurance Level 3**

2516 **3.7.3.3.1 Revocation Procedures**

2517 These criteria address general revocation functions, such as the processes involved and
2518 the basic requirements for publication.

2519 An enterprise and its specified service must:

2520 **AL3_CM_RVP#010 Revocation procedures**

2521 a) State the conditions under which revocation of an issued credential may occur,

2522 b) State the processes by which a revocation request may be submitted,

2523 c) State the persons and organizations from which a revocation request will be
2524 accepted,

2525 d) State the validation steps that will be applied to ensure the validity (identity) of
2526 the Revocant, and

2527 e) State the response time between a revocation request being accepted and the
2528 publication of revised certificate status.

2529 **AL3_CM_RVP#020 Secure status notification**

2530 Ensure that published credential status notification information can be relied upon in
2531 terms of the enterprise being its origin (i.e., its authenticity) and its correctness (i.e., its
2532 integrity).

2533 **AL3_CM_RVP#030 Revocation publication**

2534 Ensure that published credential status notification is revised within 24 hours of the
2535 receipt of a valid revocation request, such that any subsequent attempts to use that
2536 credential in an authentication shall be unsuccessful. The nature of the revocation
2537 mechanism shall be in accord with the technologies supported by the service.

2538 **AL3_CM_RVP_#040 Verify Revocation Identity**

2539 Establish that the identity for which a revocation request is received is one that was
2540 issued by the specified service.

2541 **AL3_CM_RVP#050 Revocation Records**

2542 Retain a record of any revocation of a credential that is related to a specific identity
2543 previously verified, solely in connection to the stated credential. At a minimum, records
2544 of revocation must include:

- 2545 a) the Revocant's full name;
- 2546 b) the Revocant's authority to revoke (e.g., subscriber themselves, someone acting
- 2547 with the subscriber's power of attorney, the credential issuer, law enforcement, or
- 2548 other legal due process);
- 2549 c) the Credential Issuer's identity (if not directly responsible for the identity proofing
- 2550 service);
- 2551 d) the identity associated with the credential (whether the subscriber's name or a
- 2552 pseudonym);
- 2553 e) the reason for revocation.

2554 **AL3_CM_RVP#060 Record Retention**

2555 Retain, securely, the record of the revocation process for the duration of the subscriber's

2556 account plus 7.5 years.

2557

2558 **3.7.3.3.2 Verify Revocant's Identity**

2559 Revocation of a credential requires that the requestor and the nature of the request be

2560 verified as rigorously as the original identity proofing. The enterprise should not act on a

2561 request for revocation without first establishing the validity of the request (if it does not,

2562 itself, determine the need for revocation).

2563 In order to do so, the enterprise and its specified service must:

2564 **AL3_CM_RVR#010 Verify revocation identity**

2565 Establish that the credential for which a revocation request is received is one that was

2566 initially issued by the specified service, applying the same process and criteria as would

2567 be applied to an original identity proofing.

2568 **AL3_CM_RVR#020 Revocation reason**

2569 Establish the reason for the revocation request as being sound and well founded, in

2570 combination with verification of the Revocant, according to AL3_ID_RVR#030,

2571 AL3_ID_RVR#040, or AL3_ID_RVR#050.

2572 **AL3_CM_RVR#030 Verify Subscriber as Revocant**

2573 When the subscriber seeks revocation of the subscriber's own credential:

- 2574 a) if in-person, require presentation of a primary Government Picture ID document
- 2575 that must be electronically verified by a record check against the provided identity
- 2576 with the specified issuing authority's records, or
- 2577 b) if remote:

- 2578 i. electronically verify a signature against records (if available), confirmed
2579 with a call to a telephone number of record, or
2580 ii. authenticate an electronic request as being from the same subscriber,
2581 supported by a credential at Assurance Level 3 or higher.

2582 **AL3_CM_RVR#040 Verify CSP as Revocant**

2583 Where a CSP seeks revocation of a subscriber's credential, establish that the request is
2584 either:

- 2585 a) from the specified service itself, with authorization as determined by established
2586 procedures, or
2587 b) from the client Credential Issuer, by authentication of a formalized request over
2588 the established secure communications network.

2589 **AL3_CM_RVR#050 Legal Representative as Revocant**

2590 Where the request for revocation is made by a law enforcement officer or presentation of
2591 a legal document:

- 2592 a) if in person, verify the identity of the person presenting the request, or
2593 b) if remote:
2594 i. in paper/facsimile form, verify the origin of the legal document by a
2595 database check or by telephone with the issuing authority, or
2596 ii. authenticate an electronic request as being from a recognized legal office,
2597 supported by a credential at Assurance Level 3 or higher.
2598

2599 **3.7.3.3.3 Secure Revocation Request**

2600 This criterion applies when revocation requests must be communicated between remote
2601 components of the service organization.

2602 An enterprise and its specified service must:

2603 **AL3_CM_SRR#010 Submit Request**

2604 Submit a request for the revocation to the Credential Issuer service (function), using a
2605 secured network communication.

2606

2607 **3.7.3.4 Assurance Level 4**

2608 **3.7.3.4.1 Revocation Procedures**

2609 These criteria address general revocation functions, such as the processes involved and
2610 the basic requirements for publication.

2611 An enterprise and its specified service must:

2612 **AL4_CM_RVP#010** **Revocation procedures**

- 2613 a) State the conditions under which revocation of an issued certificate may occur,
- 2614 b) State the processes by which a revocation request may be submitted,
- 2615 c) State the persons and organizations from which a revocation request will be
2616 accepted,
- 2617 d) State the validation steps that will be applied to ensure the validity (identity) of
2618 the Revocant, and
- 2619 e) State the response time between a revocation request being accepted and the
2620 publication of revised certificate status.

2621 **AL4_CM_RVP#020** **Secure status notification**

2622 Ensure that published credential status notification information can be relied upon in
2623 terms of the enterprise of its origin (i.e., its authenticity) and its correctness (i.e., its
2624 integrity).

2625 **AL4_CM_RVP#030** **Revocation publication**

2626 Ensure that published credential status notification is revised within 18 hours of the
2627 receipt of a valid revocation request, such that any subsequent attempts to use that
2628 credential in an authentication shall be unsuccessful. The nature of the revocation
2629 mechanism shall be in accordance with the technologies supported by the service.

2630 **AL4_CM_RVP#050** **Revocation Records**

2631 Retain a record of any revocation of a credential that is related to a specific identity
2632 previously verified, solely in connection to the stated credential. At a minimum, records
2633 of revocation must include:

- 2634 a) the Revocant's full name;
- 2635 b) the Revocant's authority to revoke (e.g., subscriber themselves, someone acting
2636 with the subscriber's power of attorney, the credential issuer, law enforcement, or
2637 other legal due process);
- 2638 c) the Credential Issuer's identity (if not directly responsible for the identity proofing
2639 service);
- 2640 d) the identity associated with the credential (whether the subscriber's name or a
2641 pseudonym);
- 2642 e) the reason for revocation.

2643 **AL4_CM_RVP#060 Record Retention**

2644 Retain, securely, the record of the revocation process for the duration of the subscriber's
2645 account plus 7.5 years.

2646

2647 **3.7.3.4.2 Verify Revocant's Identity**

2648 Revocation of a credential requires that the requestor and the nature of the request be
2649 verified as rigorously as the original identity proofing. The enterprise should not act on a
2650 request for revocation without first establishing the validity of the request (if it does not,
2651 itself, determine the need for revocation).

2652 In order to do so, the enterprise and its specified service must:

2653 **AL4_CM_RVR#010 Verify revocation identity**

2654 Establish that the credential for which a revocation request is received is one that was
2655 initially issued by the specified service, applying the same process and criteria as would
2656 apply to an original identity proofing.

2657 **AL4_CM_RVR#020 Revocation reason**

2658 Establish the reason for the revocation request as being sound and well founded, in
2659 combination with verification of the Revocant, according to AL4_CM_RVR#030,
2660 AL4_CM_RVR#040, or AL4_CM_RVR#050.

2661 **AL4_CM_RVR#030 Verify Subscriber as Revocant**

2662 Where the subscriber seeks revocation of the subscriber's own credential:

- 2663 a) if in person, require presentation of a primary Government Picture ID document
2664 that shall be verified by a record check against the provided identity with the
2665 specified issuing authority's records, or
2666 b) if remote:
2667 i. verify a signature against records (if available), confirmed with a call to a
2668 telephone number of record, or
2669 ii. authenticate an electronic request as being from the same subscriber,
2670 supported by a different credential at Assurance Level 4.

2671 **AL4_CM_RVR#040 Verify CSP as Revocant**

2672 Where a CSP seeks revocation of a subscriber's credential, establish that the request is
2673 either:

- 2674 a) from the specified service itself, with authorization as determined by established
2675 procedures, or

- 2676 b) from the client Credential Issuer, by authentication of a formalized request over
2677 the established secure communications network.

2678 **AL4_CM_RVR#050 Legal Representative as Revocant**

2679 Where the request for revocation is made by a law enforcement officer or presentation of
2680 a legal document:

- 2681 a) if in person, verify the identity of the person presenting the request, or
2682 b) if remote:
2683 i. in paper/facsimile form, verify the origin of the legal document by a
2684 database check or by telephone with the issuing authority, or
2685 ii. authenticate an electronic request as being from a recognized legal office,
2686 supported by a different credential at Assurance Level 4.

2687 **3.7.3.4.3 Re-keying a credential**

2688 Re-key of a credential requires that the requestor be verified as the subject with as much
2689 rigor as was applied to the original identity proofing. The enterprise should not act on a
2690 request for re-key without first establishing that the requestor is identical to the subject.

2691 In order to do so, the enterprise and its specified service must:

2692 **AL4_CM_RKY#010 Verify Requestor as Subscriber**

2693 Where the subscriber seeks a re-key for the subscriber's own credential:

- 2694 a) if in-person, require presentation of a primary Government Picture ID document
2695 that shall be verified by a record check against the provided identity with the
2696 specified issuing authority's records, or
2697 b) if remote:
2698 i. verify a signature against records (if available), confirmed with a call to a
2699 telephone number of record, or
2700 ii. authenticate an electronic request as being from the same subscriber,
2701 supported by a different credential at Assurance Level 4.
2702

2703 **AL4_CM_RKY#020 Re-key requests from parties other than the subscriber**

2704 Re-key requests from any other parties must not be accepted

2705 **3.7.3.4.4 Secure Revocation/Re-key Request**

2706 This criterion applies when revocation or re-key requests must be communicated between
2707 remote components of the service organization.

2708 The enterprise and its specified service must:

2709 **AL4_CM_SRR#010** **Submit Request**

2710 Submit a request for the revocation to the Credential Issuer service (function), using a
2711 secured network communication.

2712 **3.7.4 Part D--Credential Status Management**

2713 These criteria deal with credential status management, such as the receipt of requests for
2714 new status information arising from a new credential being issued or a revocation or other
2715 change to the credential that requires notification. They also deal with the provision of
2716 status information to requesting parties having the right to access such information.

2717 **3.7.4.1 Assurance Level 1**

2718 **3.7.4.1.1 Status Maintenance**

2719 An enterprise and its specified service must:

2720 **AL1_CM_CSM#010** **Maintain Status Record**

2721 Maintain a record of the status of all credentials issued.

2722 **AL1_CM_CSM#040** **Status Information Availability**

2723 Provide, with 95% availability, a secure automated mechanism to allow relying parties to
2724 determine credential status and authenticate the subject's identity.

2725

2726 **3.7.4.2 Assurance Level 2**

2727 **3.7.4.2.1 Status Maintenance**

2728 An enterprise and its specified service must:

2729 **AL2_CM_CSM#010** **Maintain Status Record**

2730 Maintain a record of the status of all credentials issued.

2731 **AL2_CM_CSM#020** **Validation of Status Change Requests**

2732 Authenticate all requestors seeking to have a change of status recorded and published and
2733 validate the requested change before considering processing the request. Such validation
2734 should include:

- 2735 a) the requesting source as one from which the specified service expects to receive
2736 such requests;

2737 b) if the request is not for a new status, the credential or identity as being one for
2738 which a status is already held.

2739 **AL2_CM_CSM#030 Revision to Published Status**

2740 Process authenticated requests for revised status information and have the revised
2741 information available for access within a period of 72 hours.

2742 **AL2_CM_CSM#040 Status Information Availability**

2743 Provide, with 95% availability, a secure automated mechanism to allow relying parties to
2744 determine credential status and authenticate the subject's identity.

2745 **AL2_CM_CSM#050 Inactive Credentials**

2746 Disable any credential that has not been successfully used for authentication during a
2747 period of 18 months.

2748

2749 **3.7.4.3 Assurance Level 3**

2750 **3.7.4.3.1 Status Maintenance**

2751 An enterprise and its specified service must:

2752 **AL3_CM_CSM#010 Maintain Status Record**

2753 Maintain a record of the status of all credentials issued.

2754 **AL3_CM_CSM#020 Validation of Status Change Requests**

2755 Authenticate all requestors seeking to have a change of status recorded and published and
2756 validate the requested change before considering processing the request. Such validation
2757 should include:

2758 a) the requesting source as one from which the specified service expects to receive
2759 such requests;

2760 b) if the request is not for a new status, the credential or identity as being one for
2761 which a status is already held.

2762 **AL3_CM_CSM#030 Revision to Published Status**

2763 Process authenticated requests for revised status information and have the revised
2764 information available for access within a period of 72 hours.

2765 **AL3_CM_CSM#040** **Status Information Availability**

2766 Provide, with 95% availability, a secure automated mechanism to allow relying parties to
2767 determine credential status and authenticate the subject's identity.

2768 **AL3_CM_CSM#050** **Inactive Credentials**

2769 Disable any credential that has not been successfully used for authentication during a
2770 period of 18 months.

2771

2772 **3.7.4.4** **Assurance Level 4**

2773 **3.7.4.4.1** **Status Maintenance**

2774 An enterprise and its specified service must:

2775 **AL4_CM_CSM#010** **Maintain Status Record**

2776 Maintain a record of the status of all credentials issued.

2777 **AL4_CM_CSM#020** **Validation of Status Change Requests**

2778 Authenticate all requestors seeking to have a change of status recorded and published and
2779 validate the requested change before considering processing the request. Such validation
2780 should include:

- 2781 a) the requesting source as one from which the specified service expects to receive
- 2782 such requests;
- 2783 b) if the request is not for a new status, the credential or identity as being one for
- 2784 which a status is already held.

2785 **AL4_CM_CSM#030** **Revision to Published Status**

2786 Process authenticated requests for revised status information and have the revised
2787 information available for access within a period of 72 hours.

2788 **AL4_CM_CSM#040** **Status Information Availability**

2789 Provide, with 95% availability, a secure automated mechanism to allow relying parties to
2790 determine credential status and authenticate the subject's identity.

2791 **AL4_CM_CSM#050** **Inactive Credentials**

2792 Disable any credential that has not been successfully used for authentication during a
2793 period of 18 months.

2794 **3.7.5 Part E--Credential Validation/Authentication**

2795 These criteria apply to credential validation and identity authentication.

2796 **3.7.5.1 Assurance Level 1**

2797 **3.7.5.1.1 Assertion Security**

2798 An enterprise and its specified service must:

2799 **AL1_CM_ASS#010 Validation and Assertion Security**

2800 Provide validation of credentials to a relying party using a protocol that:

- 2801 a) requires authentication of the specified service or of the validation source;
- 2802 b) ensures the integrity of the authentication assertion.

2803 **AL1_CM_ASS#020 Post Authentication**

2804 *Not* authenticate credentials that have been revoked.

2805 **AL1_CM_ASS#030 Proof of Possession**

2806 Use an authentication protocol that requires the claimant to prove possession and control
2807 of the authentication token.

2808 **AL1_CM_ASS#040 Assertion Lifetime**

2809 No stipulation.

2810

2811 **3.7.5.2 Assurance Level 2**

2812 **3.7.5.2.1 Assertion Security**

2813 An enterprise and its specified service must:

2814 **AL2_CM_ASS#010 Validation and Assertion Security**

2815 Provide validation of credentials to a relying party using a protocol that:

- 2816 a) requires authentication of the specified service, itself, or of the validation source;
- 2817 b) ensures the integrity of the authentication assertion.

2818 **AL2_CM_ASS#020 Post Authentication**

2819 *Not* authenticate credentials that have been revoked.

2820 **AL2_CM_ASS#030** **Proof of Possession**

2821 Use an authentication protocol that requires the claimant to prove possession and control
2822 of the authentication token.

2823 **AL2_CM_ASS#040** **Assertion Lifetime**

2824 Generate assertions so as to indicate and effect their expiration 12 hours after their
2825 creation.

2826

2827 **3.7.5.3** **Assurance Level 3**

2828 **3.7.5.3.1** **Assertion Security**

2829 An enterprise and its specified service must:

2830 **AL3_CM_ASS#010** **Validation and Assertion Security**

2831 Provide validation of credentials to a relying party using a protocol that:

- 2832 a) requires authentication of the specified service, itself, or of the validation source;
2833 b) ensures the integrity of the authentication assertion.

2834 **AL3_CM_ASS#020** **Post Authentication**

2835 *Not* authenticate credentials that have been revoked.

2836 **AL3_CM_ASS#030** **Proof of Possession**

2837 Use an authentication protocol that requires the claimant to prove possession and control
2838 of the authentication token.

2839 **AL3_CM_ASS#040** **Assertion Lifetime**

2840 For non-cryptographic credentials, generate assertions that indicate and effect their
2841 expiration 12 hours after their creation; otherwise, notify the relying party of how often
2842 the revocation status sources are updated.

2843

2844 **3.7.5.4** **Assurance Level 4**

2845 **3.7.5.4.1** **Assertion Security**

2846 An enterprise and its specified service must:

2847 **AL4_CM_ASS#010 Validation and Assertion Security**

2848 Provide validation of credentials to a relying party using a protocol that:

- 2849 a) requires authentication of the specified service, itself, or of the validation source;
2850 b) ensures the integrity of the authentication assertion.

2851 **AL4_CM_ASS#020 Post Authentication**

2852 *Not* authenticate credentials that have been revoked.

2853 **AL4_CM_ASS#030 Proof of Possession**

2854 Use an authentication protocol that requires the claimant to prove possession and control
2855 of the authentication token.

2856 **AL4_CM_ASS#040 Assertion Lifetime**

2857 Notify the relying party of how often the revocation status sources are updated.

2858

2859 **3.7.6 Compliance Tables**

2860 Use the following tables to correlate criteria and evidence offered/compliance achieved.
2861 A table is provided for each assurance level. The tables are linked to their respective
2862 criteria and vice-versa, to aid referencing between them. Service providers preparing for
2863 an assessment can use the table appropriate to the level at which they are seeking
2864 approval to correlate evidence with criteria or to justify non-applicability of criteria (e.g.,
2865 specific service types not offered): Assessors can use the tables to record the steps they
2866 take in their assessment and their determination of compliance or failure.

2867

2868

Table 3-5 CM-SAC - AL1 Compliance

Clause	Description	Compliance
Part A – Credential Operating Environment		
AL1_CM_CPP#010	Credential Policy and Practice Statement	
AL1_CM_CTR#010	Secret revelation	
AL1_CM_CTR#020	Protocol threat risk assessment and controls	
AL1_CM_CTR#030	System threat risk assessment and controls	
AL1_CM_STS#010	Stored Secrets	
AL1_CM_OPN#010	Changeable PIN/Password	
Part B – Credential Issuing		
AL1_CM_IDP#010	Self-managed identity proofing	
AL1_CM_IDP#020	IAEG-approved outsourced service	
AL1_CM_IDP#030	Non IAEG-approved outsourced service	
AL1_CM_IDP#040	Revision to subscriber information	
AL1_CM_CRN_#010	Authenticated Request	
AL1_CM_CRN_#020	Unique identity	
AL1_CM_CRN_#030	Credential uniqueness	
Part C – Credential Revocation		
AL1_CM_SRR#010	Submit Request	
Part D – Credential Status Management		
AL1_CM_CSM#010	Maintain Status Record	
AL1_CM_CSM#040	Status Information Availability	
Part E – Credential Validation / Authentication		
AL1_CM_ASS#010	Validation and Assertion Security	
AL1_CM_ASS#020	No Post Authentication	
AL1_CM_ASS#030	Proof of Possession	
AL1_CM_ASS#040	Assertion Lifetime	

2869

2870

Table 3-6 CM-SAC - AL2 Compliance

Clause	Description	Compliance
Part A - Credential Operating Environment		
AL2_CM_CPP#010	Credential Policy and Practice Statement	
AL2_CM_CPP#030	Management Authority	
AL2_CM_CTR#010	Secret revelation	
AL2_CM_CTR#020	Protocol threat risk assessment and controls	
AL2_CM_CTR#030	System threat risk assessment and controls	
AL2_CM_CTR#040	Specified Service's Key Management	
AL2_CM_STS#010	Stored Secrets	
AL2_CM_OPN#010	Changeable PIN/Password	
Part B – Credential Issuing		
AL2_CM_IDP#010	Self-managed identity proofing	
AL2_CM_IDP#020	IAEG-approved outsourced service	
AL2_CM_IDP#030	Non IAEG-approved 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_#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	Binding of key	
AL2_CM_CRN_#090	Nature of subject	
AL2_CM_CRD_#010	Subject of Credential's Issuance	
Part C – 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	
Part D – 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 E – Credential Validation / Authentication		
AL2_CM_ASS#010	Validation and Assertion Security	
AL2_CM_ASS#020	No Post Authentication	
AL2_CM_ASS#030	Proof of Possession	
AL2_CM_ASS#040	Assertion Lifetime	

2871

2872

2873

Table 3-7 CM-SAC - AL3 Compliance

Clause	Description	Compliance
Part A – Credential Operating Environment		
AL3_CM_CPP#010	Credential Policy and Practice Statement	
AL3_CM_CPP#030	Management Authority	
AL3_CM_CTR#010	Secret revelation	
AL3_CM_CTR#020	Protocol threat risk assessment and controls	
AL3_CM_CTR#030	System threat risk assessment and controls	
AL3_CM_CTR#040	Specified Service's Key Management	
AL3_CM_STS#010	Stored Secrets	
AL3_CM_STS#020	Stored Secret Encryption	
AL3_CM_SER#010	Security event logging	
AL3_CM_OPN#010	Changeable PIN/Password	
Part B – Credential Issuing		
AL3_CM_IDP#010	Self-managed identity proofing	
AL3_CM_IDP#020	IAEG-approved outsourced service	
AL3_CM_IDP#030	Non IAEG-approved 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_#040	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	Subject of Credential's Issuance	
AL3_CM_CRD_#020	Subject's acknowledgement	
Part C – 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	CSP as Revocant	
AL3_CM_RVR#050	Verify Legal Representative as Revocant	
AL3_CM_SRR#010	Submit Request	
Part D – 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 E – Credential Validation / Authentication		
AL3_CM_ASS#010	Validation and Assertion Security	
AL3_CM_ASS#020	No Post Authentication	
AL3_CM_ASS#030	Proof of Possession	
AL3_CM_ASS#040	Assertion Lifetime	

2874

2875

Table 3-8 CM-SAC - AL4 Compliance

Clause	Description	Compliance
Part A - Credential Operating Environment		
AL4_CM_CPP#020	Credential Policy and Practice Statement	
AL4_CM_CPP#030	Management Authority	
AL4_CM_CTR#010	Secret revelation	
AL4_CM_CTR#020	Protocol threat risk assessment and controls	
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 logging	
AL4_CM_OPN#010	Changeable PIN/Password	
Part B – Credential Issuing		
AL4_CM_IDP#010	Self-managed identity proofing	
AL4_CM_IDP#020	IAEG-approved outsourced service	
AL4_CM_IDP#030	Non IAEG-approved 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_#040	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	Subject of Credential's Issuance	
AL4_CM_CRD_#020	Subject's acknowledgement	
Part C – Credential Revocation		
AL4_CM_RVP#010	Revocation procedures	
AL4_CM_RVP#020	Secure status notification	
AL4_CM_RVP#030	Revocation publication	
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 from non-Subscriber	
AL4_CM_SRR#010	Submit Request	
Part D – 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 E – Credential Validation / Authentication		
AL4_CM_ASS#010	Validation and Assertion Security	
AL4_CM_ASS#020	No Post Authentication	
AL4_CM_ASS#030	Proof of Possession	
AL4_CM_ASS#040	Assertion Lifetime	

2876

2877 **4 Accreditation and Certification Rules**

2878 **4.1 Assessor Accreditation**

2879 IAEG certified services can be offered only by a CSP that is IAEG-certified. IAEG
2880 certification will be granted by a Federation Operator based on an assessment provided
2881 by an IAEG-accredited assessor. Assessor accreditation requires the following steps.

- 2882 a) An assessor submits an application for accreditation.
- 2883 b) The IAEG evaluates the application according to the criteria set for accreditation.
- 2884 c) The applicant is notified of the IAEG decision.
- 2885 d) In the event of a negative decision, the applicant is offered an appeal.

2886 **4.1.1 Criteria for Assessor Accreditation**

2887 The Board of Directors or any committee or other entity the Board may empower by
2888 delegation (the Board) may choose to recognize the accreditation of another body in lieu
2889 of its own accreditation or as a supplement to its own accreditation. The Board shall
2890 apply the following criteria when determining whether to approve the application of an
2891 assessor for accreditation.

2892 **4.1.1.1 Expertise With Relevant Standards**

2893 Prior to accreditation, the assessor must demonstrate expertise in the application of
2894 general controls evaluation standards, such as ISO 27001. In addition, the assessor must
2895 demonstrate competence in the application of specific controls evaluation criteria, such as
2896 WebTrust, formally identified by the IAEG and against which CSPs are to be assessed for
2897 certification by Federation Operators and other trust providers.

2898 **4.1.1.2 Business Expertise**

2899 The assessor must:

- 2900 a) have been in existence for more than 1 month;
- 2901 b) demonstrate that it is financially solvent and stable and reasonably certain to
2902 remain so in the opinion of the CSP for whom services will be provided;
- 2903 c) demonstrate proof of business insurance, or similar instrument, to satisfy the
2904 potential liability of its services, as determined by the parties to the process;
- 2905 d) demonstrate experience and expertise in electronic authentication and identity
2906 assurance methodologies like Web Trust, tScheme, ISO 27001 or other similar
2907 standard approach.
- 2908 e) Successfully complete a Liberty-sponsored IAF examination or similar domain
2909 expertise accreditation program recognized by Liberty;

- 2910 f) *not* have any key personnel or personnel directly involved in assessments or
2911 development and delivery of assessment reports and recommendations to the
2912 IAEG who have been convicted of a crime.

2913 **4.1.2 Assessment**

2914 Prior to accreditation, assessors may be subject to an on-site evaluation by the IAEG or a
2915 designee. This assessment is to determine compliance with the current IAEG criteria for
2916 accreditation and to evaluate expertise, processes and equipment necessary to conduct the
2917 assessment of CSPs according to IAEG certification criteria and rules. Whether an on-
2918 site inspection is scheduled or not, the assessor shall provide information as provided for
2919 in Section 4.1.1.1 and Section 4.1.1.2.

2920 **4.1.3 Accreditation Decision and Appeal**

2921 Within a reasonable time and at the discretion of the IAEG, the IAEG shall make a
2922 determination of accreditation and communicate that determination to the applicant.

2923 In the event of a negative decision, the assessor may request an appeal of the
2924 accreditation decision by the IAEG. Such request shall be considered by a three-member
2925 panel of the IAEG Board of Directors or any committee or other entity the Board may
2926 empower by delegation, composed of people who have been uninvolved with the decision
2927 and are impartial.

2928 **4.1.4 Maintaining Accreditation**

2929 After the initial year of accreditation, assessors may be subject to an on-site or remote
2930 surveillance evaluation. The surveillance assessment shall include review of at least the
2931 following:

- 2932 a) Internal audit reports focusing on Information Technology-related controls audits.
2933 b) Minutes of management review meetings on the topic of Information Technology-
2934 related controls reviews.
2935 c) Results of certification assessments, if any.
2936 d) Any material changes in key personnel, facilities and/or testing process.
2937 e) Information on any other significant changes in the quality system of the assessor.

2938 The IAEG, or a designee, may conduct an on-site reassessment or surveillance assessment
2939 of accredited assessors at a minimum of once every 2 years, for verification of continued
2940 compliance with IAEG accreditation criteria and rules.

2941 **4.2 Certification of Credential Service Provider Offerings**

2942 Only a CSP whose product or line of business is currently IAEG certified can issue or
2943 otherwise purvey certified credentials or validation of IAEG certified credentials under an
2944 IAEG brand or IAEG business rules or for use within the IAEG system.

2945 **4.2.1 Process of Certification**

2946 The process of certification for each product or line of business for which certification is
2947 sought by a CSP includes the following steps.

- 2948 a) A CSP seeking certification for a product or line of business begins the formal
2949 process by reviewing the list of IAEG accredited and approved assessors. The
2950 CSP selects an assessor for commencing formal assessment, for which there shall
2951 be a separate contractual arrangement between the applicant and the chosen
2952 assessor.
- 2953 b) The IAEG accredited assessor selected by the applicant conducts an assessment of
2954 the CSP product or line of business. At the conclusion of the assessment process,
2955 the assessor and the CSP separately submit their respective materials to, and as
2956 required by, the Federation Operator.
- 2957 c) The assessor submits the assessment report and its recommendation regarding
2958 certification to, and as required by, the Federation Operator.
- 2959 d) The CSP submits an application for certification to the Federation Operator,
2960 including agreement to the IAEG business rules, as well as specification of each
2961 line of offerings for which certification is sought, and the assurance level (AL) at
2962 which each certification is sought.
- 2963 e) After receiving the assessment and application materials from the assessor and
2964 CSP, respectively, the Federation Operator evaluates the relevant information and
2965 makes a decision on certification.
- 2966 f) The Federation Operator communicates its decision on certification to the CSP,
2967 the assessor and the IAEG. In the event a certification designation is assigned, it
2968 is incumbent on the Federation Operator to ensure that the CSP operate in a
2969 manner that complies with the IAF guidelines.
- 2970 g) In the event of a negative decision, the CSP is afforded an appeal.
- 2971 h) In the event of a positive decision, the CSP's certified product or line of business
2972 is added to the IAEG Certified CSP offering list.
- 2973 i) A CSP may not be the assessor of its own service or any other credential service
2974 operating in the same federation or network.

2975 **4.2.1.1 Application**

2976 The IAEG shall provide a standard application form for certification by Federation
2977 Operators as an IAEG-certified CSP both on the IAEG web site and in paper form. The
2978 application, to be completed by the CSP and submitted to the Federation Operator, shall
2979 include contact information; an agreement to abide by the IAEG rules and any other
2980 applicable IAEG requirements identified in the application, such as a license agreement
2981 or other terms and conditions; and an IAEG appeal request form to request review of the
2982 final certification determination. In addition, the application shall require the applicant to
2983 specify the precise scope of each line of business for which certification is sought, the AL
2984 at which each certification is sought, and any existing applicable accreditation,
2985 certification or similar approvals granted to each specified line of business.

2986 **4.2.1.2 Initial Evaluation**

2987 Upon receipt of an application for certification, the Federation Operator shall review the
2988 contents and the assessment report.

2989 **4.2.1.3 Assessment**

2990 Prior to submitting an application for certification, CSPs must obtain an assessment by an
2991 IAEG accredited assessor. The assessment shall determine compliance with the current
2992 IAEG Service Assessment Criteria.

2993 An IAEG accredited assessor will conduct an on-site reassessment or surveillance
2994 assessment of a CSP at least 1 year after certification and, at a minimum, once every 2
2995 years thereafter, for verification of continued compliance with IAEG certification
2996 requirements.

2997 **4.2.2 Criteria for Certification of CSP Line of Business**

2998 **4.2.2.1 Standard Evaluation Criteria Used by Assessor**

2999 For each line of business for which certification is sought, the practices, operations,
3000 organization, personnel and other relevant aspects of a CSP must be assessed against the
3001 appropriate Service Assessment Criteria for the specified Assurance Level.

3002 When multiple offerings share one or more assessment criteria, the criteria need only be
3003 considered once per assessment. Such criteria may include management organization,
3004 physical security, or personnel who are common to each line of business for which
3005 certification is sought. In addition, criteria that have been previously assessed positively
3006 by an adequate assessor and assessment process and that are equivalent to IAEG criteria
3007 may be relied upon for purposes of an IAEG assessment. Whether such criteria are
3008 deemed adequate and equivalent must be decided by the IAEG Board. Such
3009 determination by the Board may be triggered by a request by a previously assessed
3010 applicant CSP, an accredited assessor or on the initiative of the Board itself. Such
3011 determinations may be published from time to time as assessment guidance by the IAEG.

3012 **4.2.2.2 Supplemental Criteria Used by Assessor**

3013 The criteria applied by assessors are identified in the IAEG Service Assessment Criteria
3014 (Section 3).

3015 **4.2.3 Certification Decision**

3016 **4.2.3.1 Assessor Delivers Report and Recommendation**

3017 Upon conclusion of the assessment, for each line of business for which certification has
3018 been sought, the assessor shall deliver to the Federation Operator a final assessment
3019 report, including a recommendation on whether to certify the assessed CSP.

3020 **4.2.3.2 Federation Operator Makes Certification Decision**

3021 Upon receipt of each assessment report and recommendation on certification from the
3022 accredited assessor, the Federation Operator shall determine within a reasonable time
3023 whether to deny certification to the CSP, certify the CSP, or take such other action as may
3024 be appropriate, including requesting further information, contractual agreements, or
3025 provable action from the CSP by a certain date.

3026 The decision of the Federation Operator shall be communicated to both the CSP and the
3027 assessor within a reasonable time, to be set by the IAEG Board. The assessor will then
3028 communicate the decision to the IAEG.

3029 **4.2.4 Appeals Process**

3030 Upon receipt of the decision on certification by a Liberty-accredited Federation Operator,
3031 a CSP may request an appeal of that decision. Upon receiving the Appeal Request from a
3032 CSP, the IAEG shall appoint a three-member review panel from among IAEG Board of
3033 Directors or any committee or other entity the Board may empower by delegation. Said
3034 panel shall consider the request and review the assessment of the CSP provided by the
3035 accredited assessor to the Federation Operator. The panel will then provide its review of
3036 the assessment to the Federation Operator for consideration in the appeals process.

3037 **4.2.5 Maintaining Certification**

3038 The CSP must notify the assessor, the Federation Operator and the IAEG of any material
3039 change that may lower the assurance level of the certified product or line of business 60
3040 days before the change is performed or immediately upon the incidence of any unplanned
3041 change. The Federation Operator, in consultation with the accredited assessor, will
3042 determine whether the changes are sufficient to require re-assessment. The re-assessment,
3043 if required, need only cover those elements that have changed.

3044

3045 **4.3 Process for Handling Non-Compliance**

3046 The process for handling non-compliance applies both to accredited assessors and to
3047 certified CSPs, unless otherwise noted, and is outlined in Sec. 5 – Business Rules.

3048

3049 **4.4 Acceptable Public Statements Regarding IAEG**
3050 **Accreditation and Certification**

3051 It is acceptable for a party to indicate that it is an "IAEG Accredited Assessor" or an
3052 "IAEG Certified Credential Service Provider" for any period during which such statement
3053 is true. However, no party may make any public claim, whether to media outlets, in bids
3054 and other proposals, in marketing materials or otherwise, regarding its status as an
3055 applicant for accreditation or certification, nor can it claim that it is in the process of
3056 achieving such status.

3057 **5 Business Rules**

3058 **5.1 Scope**

3059 Signatories to these business rules agree that these rules govern the use and validation of
3060 Liberty Alliance IAEG certified credentials, the certification of such credentials and the
3061 accreditation of those who assess issuers of such credentials. These business rules are
3062 intended to cover use of credentials for purposes of authentication and not specifically for
3063 the application of a legal signature, which may be subject to other rules depending upon
3064 the parties and transactions involved. The IAEG will employ a phased approach to
3065 establishing business rules and assessment criteria for identity trust service providers,
3066 starting with credential service providers, then evolving to include federations and
3067 federation operators.

3068 The IAEG will provide a framework of assessment criteria as a guideline for the
3069 certification of credentials issued by a CSP. The IAEG is responsible for the accreditation
3070 of assessors who evaluate CSPs for purposes of IAEG certification of credentials.
3071 Federations and/or Federation Operators will utilize the assessors' evaluations to provide
3072 certification statements with respect to the individual CSPs. A certification statement
3073 made by a federation or federation operator regarding a CSP's compliance with IAEG
3074 certification criteria may be accepted by other federations in consideration of that CSP.

3075 The foregoing does not prohibit use of an IAEG credential under a different brand,
3076 certification, or set of rules, provided that the credential is clearly being used as a non-
3077 IAEG credential.

3078 Claimants are not direct signatories to these business rules. Claimants may have
3079 contracts with each CSP issuing an IAEG credential to the claimant. The claimant can be
3080 a person, the electronic agent of a person, or any legal entity, including a corporation.
3081 Any issues or conflicts arising from use of IAEG-certified credentials will be directed to
3082 the Federation Operator for resolution.

3083 **5.2 Participation**

3084 Before becoming eligible to become a participant in these rules, a CSP must successfully
3085 complete an assessment by an IAEG-accredited assessor and be awarded IAEG
3086 certification for one or more lines of credentials issued by that CSP. A relying party may
3087 become bound by these business rules by agreeing to accept and rely on credentials
3088 issued by one or more IAEG-certified CSPs. A CSP need not be a member of the IAEG
3089 non-profit corporation in order to become certified to these business rules.

3090 **5.3 Roles and Obligations**

3091 **5.3.1 IAEG**

3092 **5.3.1.1 Promulgation and Amendment of Business Rules and Other Documents**

3093 The IAEG shall formalize and may periodically amend these business rules. The IAEG
3094 shall also formalize and may periodically amend a set of documents governing the
3095 accreditation of assessors of IAEG CSPs and the certification criteria of IAEG
3096 credentials. The IAEG reserves the right, at its discretion, to formalize and periodically
3097 amend such other materials, including policies or guidelines, participation agreements,
3098 handbooks or other documents relevant to the IAEG. Notice of all amendments shall be
3099 given by IAEG by electronic mail to the contact person(s) identified by each signatory for
3100 such purpose and by posting to the IAEG web site. All amendments shall be effective as
3101 of the date specified in such notice. If a signatory objects in writing to an amendment
3102 within 30 days after notice of the amendment is given by IAEG, such objection shall be
3103 deemed to be a notice of termination of such signatory's participation in IAEG under
3104 Section 5.2.

3105 **5.3.1.2 Assessor Accreditation and CSP Certification Requirements**

3106 The IAEG is responsible for accreditation of assessors in the IAEG System. The IAEG
3107 shall formalize and may periodically amend requirements for certification of credentials
3108 issued by a CSP and the accreditation of assessors of CSPs.

3109 **5.3.1.3 IAEG Providers List**

3110 The IAEG will maintain and update as needed a list of current accredited assessors and
3111 IAEG-certified CSPs. To the extent allowable, the IAEG will publish this list as a service
3112 to the industry.

3113 **5.3.1.4 Contact Information**

3114 Current contact information for the IAEG can be found at <http://www.projectliberty.org>.

3115 **5.3.2 CSP Obligations**

3116 **5.3.2.1 CSP Certification**

3117 A CSP is obliged to obtain certification of one or more lines of credentials as a
3118 prerequisite for participation in the IAEG System. Certification of CSPs will be
3119 determined by federations and/or Federation Operators based on their review of an
3120 assessment report provided by an IAEG-accredited assessor upon request.

3121 **5.3.2.2 CSP Participation**

3122 A CSP is obliged to abide by the criteria set forth in this document in order to achieve and
3123 maintain IAEG certification status.

3124 **5.3.2.3 Continued Compliance with Certification Requirements**

3125 Each approved and certified CSP must comply with all certification requirements during
3126 the period of time for which credentials issued by the CSP are certified.

3127 **5.3.2.4 Use of IAEG Trademark**

3128 A CSP may not use or display the IAEG or Liberty Alliance trademark in association with
3129 the issuance, validation or other servicing of an IAEG credential or otherwise use or
3130 display the IAEG or Liberty trademark on or associated with any service, product,
3131 literature or other information unless such use has been approved by the IAEG and/or
3132 Liberty Alliance and the trademark is used in accordance with the applicable agreement
3133 with the IAEG.

3134 **5.3.2.5 Records of IAEG Related Disputes**

3135 A CSP is required to investigate any complaint raised to the CSP from a relying party
3136 regarding an IAEG credential. The CSP is also required to keep auditable records of its
3137 investigation and decisions regarding any complaint.

3138 **5.3.2.6 Validation**

3139 Each CSP must make available a method of validation for each IAEG credential it issues
3140 or is otherwise responsible for validating. Such method must be accessible and reliable.

3141 **5.3.2.7 Privacy Practices**

3142 Each CSP must be able to verify that it is complying with applicable privacy practices, as
3143 stated in Section [5.3.5.4](#) of these business rules.

3144 **5.3.2.8 Relying Party Agreements**

3145 It is advised that each approved CSP shall have in place an agreement governing the
3146 rights and obligations between it and any relying party using, validating or otherwise
3147 relying upon IAEG-certified credentials issued by that CSP. As an example, such
3148 agreement may include a clause for conflict resolution upon which the Federation
3149 Operator can rely in the event a conflict arises. Such agreement may contain such
3150 additional terms as the parties may agree to.

3151 **5.3.3 Relying Party Obligations**

3152 **5.3.3.1 Reasonable Reliance and Level of Assurance**

3153 A relying party is expected through its normal course of business to determine, for itself,
3154 the appropriate level of assurance of the IAEG credential needed for a particular
3155 application, transaction or other session. The IAEG advises a relying party to establish
3156 that a credential is in fact issued by an IAEG-certified CSP in order for the relying party's
3157 reliance upon the asserted identity of the claimant to be deemed reasonable under these
3158 business rules. Additionally, the IAEG advises a relying party to successfully validate an

3159 IAEG credential in order for its reliance upon the asserted identity of the claimant to be
3160 deemed reasonable under these business rules. Any use by or validation of an IAEG
3161 credential by a party that has not entered into an agreement with the CSP that issued the
3162 credential shall be at the sole risk of that party, for which the CSP shall have no liability
3163 whatsoever.

3164 **5.3.3.2 Use of IAEG Trademark**

3165 A relying party may not use or display the IAEG or Liberty Alliance trademark in
3166 association with the acceptance, validation or other use of an IAEG credential or
3167 otherwise use or display the IAEG or Liberty trademark on or associated with any
3168 service, product, literature or other information unless such use has been approved by the
3169 IAEG and/or Liberty Alliance.

3170 **5.3.4 Assessor Obligations**

3171 **5.3.4.1 Assessor Accreditation**

3172 An assessor is not eligible for approval by the IAEG to conduct an assessment for
3173 purposes of IAEG certification of a CSP or otherwise participate as an assessor in the
3174 IAEG System unless that assessor has been and remains accredited by the IAEG.

3175 **5.3.4.2 Assessor Agreement**

3176 An assessor is obliged to execute an IAEG assessor agreement as a prerequisite to being
3177 approved by the IAEG.

3178 **5.3.4.3 Continued Compliance with Accreditation Requirements**

3179 In accordance with the requirements of the IAEG accreditation and certification rules and
3180 any applicable service assessment criteria, approved and accredited assessors must
3181 remain in compliance with all accreditation requirements for the period of time for which
3182 they are accredited.

3183 **5.3.4.4 Use of IAEG Trademark**

3184 An assessor may not use or display the IAEG or Liberty Alliance trademark in association
3185 with an assessment or otherwise use or display the IAEG or Liberty trademark on or
3186 associated with any service, product, literature or other information unless such use has
3187 been approved by the IAEG and/or Liberty Alliance and the trademark is used in
3188 accordance with the applicable agreement with the IAEG.

3189 **5.3.5 General Obligations**

3190 **5.3.5.1 Record Keeping**

3191 Every signatory wishing to avail itself of IAEG resolution of disputes under the terms of
3192 these business rules is obliged to keep records sufficient to preserve evidence of the facts
3193 related to a particular dispute.

3194 **5.3.5.2 System Security and Reliability**

3195 Every signatory agrees to safeguard the security and reliability of the IAEG System.
3196 Specifically, every signatory agrees that the IAEG reserves the right to suspend use of the
3197 IAEG System, in whole or in part, and the participation of any party or parties to the
3198 system without notice and at the sole discretion of the IAEG to protect the integrity and
3199 efficacy of the IAEG System or the rights or property of any party. Agreement to access,
3200 use or rely upon the IAEG System is subject to such terms and conditions as the IAEG
3201 may provide in these business rules, related participation agreements or otherwise.

3202 **5.3.5.3 Third Party Processors**

3203 Any IAEG-certified or -accredited party that is participating in these rules and uses a
3204 third-party processor to perform any processing, transactions or other obligations related
3205 to participation in the IAEG System either must take full responsibility for assuring that
3206 actions of the third-party processor are in compliance with all applicable terms of these
3207 business rules or assure that the third party, itself, becomes a direct signatory of these
3208 business rules.

3209 **5.3.5.4 Claimant Privacy**

3210 Every participant in these business rules must assure that each claimant for which the
3211 participating organization collects or otherwise uses personally identifiable information
3212 has granted informed consent with regard to the sharing of any personally identifiable
3213 information about the claimant by the participant with any other party, whether such
3214 information is contained in a credential, other identity assertion or otherwise. The
3215 informed consent of the individual must be obtained before personally identifiable
3216 information is used for enrollment, authentication or any subsequent uses. Claimants
3217 must be provided with a clear statement about the collection and use of personally
3218 identifiable information upon which to make informed decisions. Participants must
3219 collect only the information necessary to complete the intended authentication function.

3220 Informed consent, for the purposes of this section, is an agreement made by a claimant
3221 with the legal capacity to do so who is so situated as to be able to exercise free power of
3222 choice without the intervention of any element of force, fraud, deceit, duress, over-
3223 reaching, or other form of constraint or coercion and who is given sufficient information
3224 about the subject matter and elements of the transaction involved as to enable him or her
3225 to make an informed and enlightened decision.

3226 Nothing in these business rules shall be construed to authorize or permit the sharing of
3227 any personally identifiable information about an end user other than the information
3228 contained in a certificate or other identity assertion. Such information can be shared only
3229 with an approved relying party to whom the end user has presented credentials or
3230 attempted to access services with an identity assertion operating under the IAEG. If any
3231 other personally identifiable information about a claimant is shared with any party
3232 operating within the IAEG System or any other party, the required consent terms listed in
3233 this section of these business rules must be affirmatively assented to by the claimant.

3234 **5.4 Enforcement and Recourse**

3235 **5.4.1 Breach of Accreditation or Certification Requirements**

3236 **5.4.1.1 Compliance Determination**

3237 Upon receipt by the IAEG of credible information that any IAEG-certified or -accredited
3238 party is not in compliance with the requirements for accreditation or certification, the
3239 IAEG Board or staff or a committee at Board discretion shall make a determination on
3240 whether the party is in fact in material non-compliance with IAEG requirements and shall
3241 communicate the determination to the affected parties. The Board of Directors shall
3242 establish further criteria, as needed, detailing conduct or circumstances constituting
3243 material non-compliance with IAEG rules or standards.

3244 Upon receipt of credible information that a CSP is not in compliance with the
3245 requirements for certification, a Federation Operator may make the determination on
3246 whether the CSP is in fact in material non-compliance with IAEG requirements and shall
3247 communicate the determination to affected parties.

3248 **5.4.1.2 Period to Cure**

3249 An IAEG-certified or -accredited party found to be in material non-compliance shall be
3250 afforded an opportunity and period of time to remedy that material non-compliance,
3251 provided such period does not unduly jeopardize the integrity of the IAEG System or the
3252 rights or property of another party.

3253 **5.4.2 Monetary Recourse**

3254 A CSP may be liable solely under the terms of an existing agreement with a relying party
3255 for losses suffered by the relying party where the cause is attributable to conduct by the
3256 CSP that was carried out in material non-compliance with these business rules or with
3257 certification requirements. Conflict resolution will be directed to the appropriate
3258 Federation Operator.

3259 A CSP may offer credentials at a band of monetary recourse set independently from levels
3260 of assurance. A CSP shall disclose the monetary recourse it will or will not make

3261 available with respect to IAEG credentials and any applicable terms or limitations
3262 governing the recourse according to Table 5-1.

3263

Table 5-1. Bands and Amounts of Monetary Recourse	
Band	Amount
1. No recourse	Zero monetary recourse
2. By agreement	By agreement of the parties

3264

3265 **5.4.2.1 Safe Harbors**

3266 **5.4.2.1.1 Losses Arising From Authorization or Unreasonable Reliance**

3267 In no event shall liability or other recourse specified herein be triggered by unreasonable
3268 reliance on a credential by a relying party or by losses resulting from authorization errors
3269 that have not been caused by errors in authentication of identity of a claimant by means
3270 of an IAEG credential.

3271 **5.4.2.1.2 Conduct in Accordance with Business Rules**

3272 Under these business rules, an approved CSP is not liable for losses suffered by a relying
3273 party where the cause is attributable to conduct by the CSP that was carried out in
3274 accordance with these business rules.

3275 **5.4.2.2 Request for Monetary Recourse**

3276 All requests for monetary recourse and the dispositions of all requests must be directed to
3277 the appropriate Federation Operator or trust provider by each relying party and CSP
3278 involved.

3279 **5.4.2.3 Reporting to the IAEG**

3280 All disputes and monetary requests involving IAEG-certified CSPs will be reported to the
3281 IAEG by the Federation Operator or identity trust provider involved.

3282 **5.4.3 Administrative Recourse**

3283 Based on review of all available data and in light of all relevant circumstances, the IAEG
3284 Board of Directors may take administrative recourse against any participant determined
3285 to be in material non-compliance with these business rules, to include, as needed, any of
3286 the following remedies.

3287 **5.4.3.1 Warning**

3288 The non-complying party may be given a warning. The warning may be confidential or
3289 may be publicized within the IAEG or publicized more broadly, at the discretion of the
3290 IAEG Board of Directors.

3291 **5.4.3.2 Credential Revocation**

3292 The non-complying party may be required to revoke one or more IAEG credentials.

3293 **5.4.3.3 Non-compliance Fees**

3294 The non-complying party may be subject to a schedule of fees, to be specified by the
3295 IAEG Board of Directors. The fees may increase according to the length of time before
3296 the party comes back into compliance.

3297 **5.4.3.4 Suspension**

3298 The non-complying party may have its participation in the IAEG System suspended,
3299 including the suspension of accreditation or certification, pending coming back into
3300 compliance.

3301 **5.4.3.5 Termination**

3302 The non-complying party may have its participation in the IAEG System terminated,
3303 including the termination of accreditation or certification.

3304 **5.5 General Terms**

3305 **5.5.1 Governing Law**

3306 These business rules and any related materials governing the IAEG shall be construed
3307 and adjudicated according to the laws of the state of Delaware, U.S.A.

3308 **5.5.2 Disclaimer**

3309 No signatory may disclaim the warranty of merchantability and fitness for a particular
3310 purpose with respect to the provision of any service or product to any other signatory
3311 under these business rules.

3312 **5.5.3 Assignment and Succession**

3313 No signatory may sell, rent, lease, sublicense, assign, grant a security interest in or
3314 otherwise transfer any right and/or obligation contained in these business rules or the
3315 participation agreement executed by that signatory without the express written consent of
3316 the IAEG.

3317 **5.5.4 Hold Harmless**

3318 All signatories to these business rules agree to hold the IAEG harmless for any losses or
3319 other liability arising out of or in relation to the issuance, use, acceptance, validation, or
3320 other reliance upon an IAEG credential or otherwise arising out of or in relation to
3321 participation in the IAEG System or other conduct subject to these business rules.

3322 **5.5.5 Severability**

3323 If any provision, set of provisions or part of a provision of these business rules is held to
3324 be unenforceable or otherwise invalid in whole or in part, the remaining provisions shall
3325 remain in full force and effect and shall be construed to the maximum extent practicable
3326 as a consistent and reasonable entire agreement.

3327 **5.6 Interpretation**

3328 The terms of these business rules shall be interpreted by the IAEG so as to avoid conflict
3329 or inconsistencies between the various provisions and between these business rules,
3330 applicable participation agreements and other relevant IAEG materials.

3331 **6 IAEG Glossary**

3332 *Accreditation.* The process used to achieve formal recognition that an organization has
3333 agreed to the IAEG operating rules and is competent to perform assessments using
3334 the Service Assessment Criteria.

3335 *AL.* See *assurance level*

3336 *Applicant.* An individual or person acting as a proxy for a machine or corporate entity
3337 who is the subject of an identity proofing process.

3338 *Approval.* The process by which the IAEG Board accepts the compliance of a certified
3339 service and the CSP responsible for that service commits to upholding the IAEG
3340 Rules.

3341 *Approved encryption.* Any cryptographic algorithm or method specified in a FIPS or a
3342 NIST recommendation or equivalent, as established by a recognized national
3343 technical authority. Refer to <http://csrc.nist.gov/cryptval/>

3344 *Approved service.* A certified service which has been granted an approval by the IAEG
3345 Board.

3346 *Assertion.* A statement from a verifier to a relying party that contains identity or other
3347 information about a subscriber.

3348 *Assessment.* A process used to evaluate an electronic trust service and the service
3349 provider using the requirements specified by one or more Service Assessment
3350 Criteria for compliance with all applicable requirements.

3351 *Assessor.* A person or corporate entity who performs an assessment.

3352 *Assurance level (AL).* A degree of certainty that a claimant has presented a credential
3353 that refers to the claimant's identity. Each assurance level expresses a degree of
3354 confidence in the process used to establish the identity of the individual to whom
3355 the credential was issued and a degree of confidence that the individual who uses
3356 the credential is the individual to whom the credential was issued. The four
3357 assurance levels are:

3358 Level 1: Little or no confidence in the asserted identity's validity

3359 Level 2: Some confidence in the asserted identity's validity

3360 Level 3: High confidence in the asserted identity's validity

3361 Level 4: Very high confidence in the asserted identity's validity

3362 *Attack.* An attempt to obtain a subscriber's token or to fool a verifier into believing that
3363 an unauthorized individual possesses a claimant's token.

3364 *Attribute.* A property associated with an individual.

3365 *Authentication.* Authentication simply establishes identity, not what that identity is
3366 authorized to do or what access privileges he or she has.

- 3367 *Authentication protocol.* A well-specified message exchange process that verifies
3368 possession of a token to remotely authenticate a claimant. Some authentication
3369 protocols also generate cryptographic keys that are used to protect an entire
3370 session, so that the data transferred in the session is cryptographically protected.
- 3371 *Authorization.* Process of deciding what an individual ought to be allowed to do.
- 3372 *Bit.* A binary digit: 0 or 1
- 3373 *Brand.* See IAEG Branded Credential.
- 3374 *CAP:* Credential Assessment Profile
- 3375 *Certification.* The IAEG's affirmation that a particular credential service provider can
3376 provide a particular credential service at a particular assurance level.
- 3377 *Claimant.* A party whose identity is to be verified.
- 3378 *Certification Body.* An organization which has been deemed competent to perform
3379 assessments of a particular type. Such assessments may be formal evaluations or
3380 testing and be based upon some defined set of standards or other criteria.
- 3381 *Certified service.* An electronic trust service which has been assessed by an IAEG-
3382 recognized certification body and found to be compliant with the applicable
3383 SACs.
- 3384 *Credential.* An object to be verified when presented in an authentication transaction. A
3385 credential can be bound in some way to the individual to whom it was issued, or it
3386 can be a bearer credential. Electronic credentials are digital documents that bind
3387 an identity or an attribute to a subscriber's token.
- 3388 *Credential management.* A service that supports the lifecycle of identity credentials from
3389 issuance to revocation, including renewal, status checks and authentication
3390 services.
- 3391 *Credential service.* A type of electronic trust service that supports the verification of
3392 identities (identity proofing), the issuance of identity related
3393 assertions/credentials/tokens, and the subsequent management of those credentials
3394 (for example, renewal, revocation and the provision of related status and
3395 authentication services).
- 3396 *Credential service provider (CSP).* An electronic trust service provider that operates one
3397 or more credential services. A CSP can include a Registration Authority.
- 3398 *CSP.* See *credential service provider*.
- 3399 *Cryptographic token.* A token for which the secret is a cryptographic key.
- 3400 *Electronic credentials.* Digital documents used in authentication that bind an identity or
3401 an attribute to a subscriber's token.

- 3402 *Electronic Trust service (ETS)*. A service that enhances trust and confidence in electronic
3403 transactions, typically but not necessarily using cryptographic techniques or
3404 involving confidential material such as PINs and passwords.
- 3405 *Electronic Trust service provider (ETSP)*. An entity that provides one or more electronic
3406 trust services.
- 3407 *ETS*. See electronic trust service.
- 3408 *ETSP*. See electronic trust service provider,
- 3409 *Federal Information Processing Standards ([FIPS])*. Standards and guidelines issued by
3410 the National Institute of Standards and Technology (NIST) for use government-
3411 wide in the United States. NIST develops FIPS when the U.S. Federal government
3412 has compelling requirements, such as for security and interoperability, for which
3413 no industry standards or solutions are acceptable.
- 3414 *Federated identity management*. A system that allows individuals to use the same user
3415 name, password, or other personal identification to sign on to the networks of
3416 more than one enterprise in order to conduct transactions.
- 3417 *Federation Operator*. An individual or group that defines standards for its respective
3418 federation, or trust community and evaluates participation in the community or
3419 network to ensure compliance with policy, including the ability to request audits
3420 of participants for verification.
- 3421 *FIPS*. See Federal Information Processing Standards.
- 3422 *IAEG*. See *Identity Assurance Expert Group*
- 3423 *IAEG assessor*. An organization that has agreed to the IAEG Rules and that has been
3424 accredited to conduct assessments of credential service providers.
- 3425 *IAEG-branded credential*. Information indicating the individual identity of a natural
3426 person, according to a CSP certified by the IAEG to issue, process, validate or
3427 otherwise purvey such credential.
- 3428 *IAEG credential service provider*. Organization that has agreed to the IAEG Operating
3429 Rules and other applicable Rules, and that has been Certified to issue, process,
3430 validate, etc., an IAEG branded credential.
- 3431 *IAEG-recognized assessor*. A body that has been granted an accreditation to perform
3432 assessments against Service Assessment Criteria, at the specified assurance
3433 level(s).
- 3434 *IAEG-recognized certification body*. A certification body which has been accredited by,
3435 or whose qualifications have been otherwise established by, a scheme which the
3436 IAEG Board has deemed to be appropriate for the purposes of determining an
3437 CSP's competence to perform assessments against IAEG's criteria.

- 3438 *Identification.* Process of using claimed or observed attributes of an individual to infer
3439 who the individual is.
- 3440 *Identifier.* Something that points to an individual, such as a name, a serial number, or
3441 some other pointer to the party being identified.
- 3442 *Identity.* A unique name for single person. Because a person's legal name is not
3443 necessarily unique, identity must include enough additional information (for
3444 example, an address or some unique identifier such as an employee or account
3445 number) to make a unique name.
- 3446 *Identity Assurance Expert Group (IAEG).* The multi-industry Liberty Alliance
3447 partnership working on enabling interoperability among public and private
3448 electronic identity authentication systems.
- 3449 *Identity Assurance Framework (IAF).* The body of work that collectively defines the
3450 industry-led self-regulatory framework for electronic trust services in the United
3451 States and around the globe, as operated by the IAEG. The Identity Assurance
3452 Framework includes descriptions of criteria, rules, procedures, processes, and
3453 other documents.
- 3454 *Identity authentication.* Process of establishing an understood level of confidence that an
3455 identifier refers to an identity. It may or may not be possible to link the
3456 authenticated identity to an individual.
- 3457 *Identity binding.* The extent to which an electronic credential can be trusted to be a proxy
3458 for the entity named in it.
- 3459 *Identity Proofing.* The process by which identity related information is validated so as to
3460 identify a person with a degree of uniqueness and certitude sufficient for the
3461 purposes for which that identity is to be used.
- 3462 *Identity Proofing policy.* A set of rules that defines identity proofing requirements
3463 (required evidence, format, manner of presentation, validation), records actions
3464 required of the registrar, and describes any other salient aspects of the identity
3465 proofing function that are applicable to a particular community or class of
3466 applications with common security requirements. An identity proofing policy is
3467 designed to accomplish a stated assurance level.
- 3468 *Identity Proofing service provider.* An electronic trust service provider which offers, as a
3469 standalone service, the specific electronic trust service of identity proofing. This
3470 service provider is sometimes referred to as a Registration Agent/Authority (RA).
- 3471 *Identity Proofing practice statement.* A statement of the practices that an identity
3472 proofing service provider employs in providing its services in accordance with the
3473 applicable identity proofing policy.

- 3474 *Information Security Management Systems (ISMS)*. A system of management concerned
3475 with information security. The key concept of ISMS is the design, implement,
3476 and maintain a coherent suite of processes and systems for effectively managing
3477 information security, thus ensuring the confidentiality, integrity, and availability of
3478 information assets and minimizing information security risks.
- 3479 *Issuer*. Somebody or something that supplies or distributes something officially.
- 3480 *Level of assurance*. See assurance level.
- 3481 *Network*. An open communications medium, typically, the Internet, that is used to
3482 transport messages between the claimant and other parties.
- 3483 *OID*. Object identifier.
- 3484 *Password*. A shared secret character string used in authentication protocols. In many
3485 cases the claimant is expected to memorize the password.
- 3486 *Practice statement*. A formal statement of the practices followed by an authentication
3487 entity (e.g., RA, CSP, or verifier) that typically defines the specific steps taken to
3488 register and verify identities, issue credentials and authenticate claimants.
- 3489 *Public key*. The public part of the asymmetric key pair that is typically used to verify
3490 signatures or encrypt data.
- 3491 *Public key infrastructure (PKI)* . A set of technical and procedural measures used to
3492 manage public keys embedded in digital certificates. The keys in such certificates
3493 can be used to safeguard communication and data exchange over potentially
3494 unsecure networks.
- 3495 *Registration*. An entry in a register, or somebody or something whose name or
3496 designation is entered in a register.
- 3497 *Relying party*. An entity that relies upon a subscriber's credentials, typically to process a
3498 transaction or grant access to information or a system.
- 3499 *Role*. The usual or expected function of somebody or something, or the part somebody or
3500 something plays in a particular action or event.
- 3501 *SAC*. See Service Assessment Criteria.
- 3502 *Security*. A collection of safeguards that ensures the confidentiality of information,
3503 protects the integrity of information, ensures the availability of information,
3504 accounts for use of the system, and protects the system(s) and/or network(s) used
3505 to process the information.
- 3506 *Service Assessment Criteria (SAC)*. A set of requirements levied upon specific
3507 organizational and other functions performed by electronic trust services and
3508 service providers. Services and service providers must comply with all applicable
3509 criteria to qualify for IAEG approval.

- 3510 *Signatory.* A party that opts into and agrees to be bound by the IAEG Rules according to
3511 the specified procedures.
- 3512 *Specified service.* The electronic trust service which, for the purposes of an IAEG
3513 assessment, is the subject of criteria set out in a particular SAC, or in an
3514 application for assessment, in a grant of an approval or other similar usage as may
3515 be found in various IAEG documentation.
- 3516 *Subject.* An entity that is able to use an electronic trust service subject to agreement with
3517 an associated subscriber. A subject and a subscriber can be the same entity.
- 3518 *Subscriber.* A party that has entered into an agreement to use an electronic trust service.
3519 A subscriber and a subject can be the same entity.
- 3520 *Threat.* An adversary that is motivated and capable to violate the security of a target and
3521 has the capability to mount attacks that will exploit the target's vulnerabilities.
- 3522 *Token.* Something that a claimant possesses and controls (typically a key or password)
3523 that is used to authenticate the claimant's identity.
- 3524 *Verification.* Establishment of the truth or correctness of something by investigation of
3525 evidence.

3526 **7 Publication Acknowledgements**

3527 The IAEG would like to thank the following working group chairs and vice chairs for
3528 their commitment and dedication to the Liberty Identity Assurance Framework.

3529

3530 IAEG Co-Chair: Frank Villavicencio, Citi

3531 IAEG Co-Chair: Alex Popowycz, Fidelity Investments

3532

3533 IASIG Co-Chair: Peter Alterman, Federal PKI Policy Authority

3534 IASIG Co-Chair: Hemma Prafullchandra, FuGen Solutions

3535

3536 Interim Chair: James Lewis, The Center for Strategic and International Studies

3537 Interim Vice Chair: David Temoshok, U.S. General Services Administration

3538

3539 Business Requirements and Processes Work Group

3540 Chair: Linda G. Elliot, PingID Network

3541 Vice Chair: Thomas Greco, beTRUSTed

3542

3543 Credential Services Assessment Criteria and Levels of Assurance Work Group

3544 Chair: Robert J. Schlecht, Mortgage Bankers Association of America

3545 Vice Chair: Von Harrison, U.S. General Services Administration

3546

3547 Credential Services Assessment Criteria Sub Work

3548 Chair: Nancy Black, HollenGroup

3549 Vice Chair: Richard Wilsher, The Zygma Partnership

3550

3551 Levels of Assurance Sub Work Group

3552 Chair: Peter Alterman, National Institutes of Health

3553 Vice Chair: Noel Nazario, KPMG LLP

3554

3555 Interoperability Sub Work Group

3556 Chair: William E. Burr, National Institute of Standards and Technology

3557 Vice Chair: Kurt Van Etten, eBay, Inc.

3558

3559 Evaluation, Accreditation and Compliance Work Group

3560 Chair: Gary Glickman, Giesecke & Devrient Cardtech, Inc.

3561 Vice Chair: Cornelia Chebinou, National Association of State Auditors, Comptrollers
3562 and Treasurers

3563

3564 EAP Governance Work Group

3565 Chair: Paula Arcioni, State of New Jersey, Office of Information Technology

3566 Vice Chair: Roger J. Cochetti, CompTIA

3567
3568 Consultants
3569 Russ Cutler, Confiance Advisors, LLC
3570 Yuriy Dzambasow, A&N Associates, Inc.
3571 Nathan Faut, KPMG
3572 Dan Greenwood, Commonwealth of Massachusetts
3573 Rebecca Nielsen, Booz Allen Hamilton
3574 Richard Wilsher, The Zygma Partnership
3575
3576 Members of the various work groups include:
3577 Khaja Ahmed, Microsoft Corporation
3578 Michael A. Aisenberg, VeriSign, Inc.
3579 Peter Alterman, National Institutes of Health
3580 Paula Arcioni, State of New Jersey, Office of Information Technology
3581 Jonathan Askins, ACXIOM Corporation
3582 Asaf Awan, Parkweb Associates
3583 Stefano Baroni, SETECS
3584 Paul Barrett, Real User Corporation
3585 Nancy Black, Hollen Group
3586 Debb Blanchard, Enspier Technologies/GDT
3587 Warren Blosjo, 3Factor
3588 Daniel Blum, Burton Group
3589 Iana Bohmer, Northrop Grumman Information Technology
3590 Christine Borucke, Electronic Data Systems
3591 Kirk Brafford, SSP-Litronic, Inc.
3592 Mayi Canales, M Squared Strategies, Inc.
3593 Richard Carter, American Association of Motor Vehicles Administration
3594 Kim Cartwright, Experian
3595 James A. Casey, NeuStar, Inc.
3596 Ray Cavanaugh, Entegrity Solutions
3597 Chuck Chamberlain, U.S. Postal Service
3598 Cornelia Chebinou, National Association of State Auditors, Comptrollers and Treasurers
3599 Rebecca Chisolm, Sun Microsystems Federal
3600 Roger J. Cochetti, CompTIA
3601 Dan Combs, Global Identity Solutions
3602 John Cornell, U.S. General Services Administration
3603 Sarah Currier, CheckFree Corporation
3604 Chris Daly, IBM Corporation
3605 Peter Davis, Neustar
3606 Kathy DiMaggio, Sigaba Corporation
3607 Yuriy Dzambasow, A&N Associates, Inc.
3608 Josh Elliott, American Management Systems
3609 Clay Epstein, Indentrus LLC

3610 Irving R. Gilson, Department of Defense
3611 Gary Glickman, Giesecke & Devrient Cardtech, Inc.
3612 James A. Gross, Wells Fargo
3613 Kirk R. Hall, GeoTrust
3614 Von Harrison, U.S. General Services Administration
3615 Christopher Hankin, Sun Microsystems, Inc.
3616 Jane Hennessey, Wells Fargo
3617 Michael Horkey, Global Identity Solutions
3618 Katherine M. Hollis, Electronic Data Systems
3619 Robert Housel, National City Corporation
3620 Burt Kaliski, RSA Security, Inc.
3621 Shannon Kellog, RSA Security, Inc.
3622 James Kobielus, Burton Group
3623 Patrick Lally, SSP-Litronic, Inc.
3624 Steve Lazerowich, Enspier Technologies/GDT
3625 Phillip S. Lee, SC Solutions, Inc.
3626 Peter Lieberwirth, Authentidate
3627 Rob Lockhart, IEEE-ISTO
3628 Chris Loudon, Enspier Technologies/GDT
3629 J. Scott Lowry, Enspier Technologies/GDT
3630 Lena Kannappan, FuGen Solutions
3631 Paul Madsen, NTT
3632 Adele Marsh, PA Higher Education Assistance Agency
3633 Patty McCarty, Private ID Systems
3634 Doug McCoy, SAFLINK Corporation
3635 Ben Miller, InsideID
3636 Larry Miller, Identrus LLC
3637 Sead Muftic, SETECS
3638 Noel Nazario, KPMG LLP
3639 Michael R. Nelson, IBM Corporation
3640 Simon Nicholson, Sun Microsystems, Inc.
3641 Pete Palmer, HIMSS NHII Task Force Advisor, Guidant Corporation
3642 Stephen Permison, Standards Based Programs
3643 Bob Pinheiro, , Robert Pinheiro Consulting LLC
3644 Alex Popowycz, Fidelity Investments
3645 Hemma Prafullchandra, FuGen Solutions
3646 Stephen L. Ranzini, University Bank
3647 Christiane Reinhold, BearingPoint
3648 Donald E. Rhodes, American Banker Association
3649 Jason Roualt, HP
3650 Randy V. Sabett, Cooley Goodward, LLP
3651 Ravi Sandhu, NSD Security
3652 Dean Sarff, Minerals Management Service

3653 Donald Saxinger, FDIC
3654 Robert J. Schlecht, Mortgage Bankers Association of America
3655 Howard Schmidt, eBay, Inc.
3656 Ari Schwartz, Center for Democracy and Technology
3657 Michael Sessa, PESC
3658 John Shipley, The Shipley Group
3659 Stephen P. Sill, U.S. General Services Administration
3660 Helena G. Sims, NACHA – The Electronic Payments Association
3661 Bill Smith, Sun Microsystems, Inc.
3662 Tadgh Smith, IBM
3663 Judith Spencer, U.S. General Services Administration
3664 William Still, ChoicePoint Public Sector
3665 Michael M. Talley, University Bancorp
3666 David Temoshok, U.S. General Services Administration
3667 Richard Thayer, ComTech, Inc.
3668 John Ticer, NeuStar, Inc.
3669 Kevin Trilli, VeriSign, Inc.
3670 Matthew Tuttle, beTRUSTed
3671 A. Jerald Varner, U.S. General Services Administration
3672 Martin Wargon, Wave Systems Corporation
3673 Richard Wilsher, The Zyigma Partnership
3674 David Weitzel, Mitretek Systems, Inc.
3675 Michael Wolf, Authentidate
3676 Gordon R. Woodrow, ClearTran, Inc.
3677 Steve Worona, EDUCAUSE
3678 David Wasley, Int2

3679 8 References

- 3680 [BSI7799-2] "BS 7799-2:2002 Information security management. Specification with
3681 guidance for use," BSI Group (September 05, 2002). [http://www.bsi-](http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030049529)
3682 [global.com/en/Shop/Publication-Detail/?pid=000000000030049529](http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030049529)
- 3683
- 3684 [CAF] Louden, Chris, Spenser, Judy, Burr, Bill, Hawkins, Kevin, Temoshok, David,
3685 Cornell, John, Wilsher, Richard G., Timchak, Steve, Sill, Stephen, Silver, Dave, Harrison,
3686 Von, eds., "E-Authentication Credential Assessment Framework (CAF)," E-
3687 Authentication Initiative, Version 2.0.0 (March 16, 2005).
3688 <http://www.cio.gov/eauthentication/documents/CAF.pdf>
- 3689
- 3690 [EAP CSAC 04011] "EAP working paper: Identity Proofing Service Assessment Criteria
3691 (ID-SAC)," Electronic Authentication Partnership, Draft 0.1.3 (July 20, 2004)
3692 http://eap.projectliberty.org/docs/Jul2004/EAP_CSAC_04011_0-1-3_ID-SAC.doc
- 3693
- 3694 [EAPTrustFramework] "Electronic Authentication Partnership Trust Framework"
3695 Electronic Authentication Partnership, Version 1.0. (January 6, 2005)
3696 http://eap.projectliberty.org/docs/Trust_Framework_010605_final.pdf
- 3697
- 3698 [FIPS] "Federal Information Processing Standards Publications" Federal Information
3699 Processing Standards. <http://www.itl.nist.gov/fipspubs/>
- 3700
- 3701 [FIPS140-2] "Security Requirements for Cryptographic Modules" Federal Information
3702 Processing Standards. (May 25, 2001) [http://csrc.nist.gov/publications/fips/fips140-](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)
3703 [2/fips1402.pdf](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)
- 3704
- 3705 [ISO/IEC17799] "ISO/IEC 17799:2005 Information technology -- Security techniques --
3706 Code of practice for information security management" International Organization for
3707 Standardization.
3708 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39612
- 3709
- 3710 [M-04-04] Bolton, Joshua B., eds., "E-Authentication Guidance for Federal Agencies,"
3711 Office of Management and Budget, (December 16, 2003).
3712 <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>
- 3713

- 3714 [NIST800-63] Burr, William E., Dodson, Donna F., Polk, W. Timothy, eds., "Electronic
3715 Authentication Guideline: : Recommendations of the National Institute of Standards and
3716 Technology," Version 1.0.2, National Institute of Standards and Technology, (April,
3717 2006). http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
3718
- 3719 [RFC 3647] Chokhani, S., Ford, W., Sabett, R., Merrill, C., Wu, S., eds., "Internet X.509
3720 Public Key Infrastructure Certificate Policy and Certification Practices Framework," The
3721 Internet Engineering Task Force (November, 2003). <http://www.ietf.org/rfc/rfc3647.txt>
3722