

1
2
3
4



5
6
7

Liberty Identity Assurance Framework

9 **Version:** 1.0

10 **Editor:**

11 Russ Cutler, Confiance Advisors

12 **Contributors:**

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

14 **Abstract:**

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

23

24 **Filename:** liberty-identity-assurance-framework-v1.0.pdf

25

26 **Notice:**

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

33
34 Implementation of certain elements of this document may require licenses under third
35 party intellectual property rights, including without limitation, patent rights. The
36 Sponsors of and any other contributors to the Specification are not and shall not be held
37 responsible in any manner for identifying or failing to identify any or all such third party
38 intellectual property rights. **This Specification is provided "AS IS," and no**
39 **participant in the Liberty Alliance makes any warranty of any kind, express or**
40 **implied, including any implied warranties of merchantability, non-infringement of**
41 **third party intellectual property rights, and fitness for a particular purpose.**
42 Implementers of this Specification are advised to review the Liberty Alliance Project's
43 website (<http://www.projectliberty.org/>) for information concerning any Necessary
44 Claims Disclosure Notices that have been received by the Liberty Alliance Management
45 Board.

46
47 Copyright © 2007 Adobe Systems; Agencia Catalana De Certificacio; America Online,
48 Inc.; Amsoft Systems Pvt Ltd.; BIPAC; BMC Software, Inc.; Bank of America
49 Corporation; Beta Systems Software AG; British Telecommunications plc; Computer
50 Associates International, Inc.; Dan Combs; Danish National IT & Telecom Agency;
51 Deutsche Telekom AG, T-Com; Diamelle Technologies; Drummond Group Inc.;
52 Entr'ouvert; Ericsson; Falkin Systems LLC; Fidelity Investments; France Télécom; Fugen
53 Solutions, Inc; Fulvens Ltd.; GSA Office of Governmentwide Policy; Gemalto; General
54 Motors; GeoFederation; Giesecke & Devrient GmbH; Guy Huntington; Hewlett-Packard
55 Company; IBM Corporation; Intel Corporation; Kantega; Luminance Consulting
56 Services; Mark Wahl; Mary Ruddy; MedCommons Inc.; Mortgage Bankers Association
57 (MBA); Nanoident Biometrics GmbH; National Emergency Preparedness Coordinating
58 Council (NEPCC); NEC Corporation; Neustar, Inc.; New Zealand Government State
59 Services Commission; NHK (Japan Broadcasting Corporation) Science & Technical
60 Research Laboratories; Nippon Telegraph and Telephone Corporation; Nokia
61 Corporation; Novell, Inc.; OpenNetwork; Oracle Corporation; Ping Identity Corporation;
62 Postsecondary Electronics Standards Council (PESC); RSA Security Inc.; SanDisk
63 Corporation; Sun Microsystems, Inc.; Symlabs, Inc.; Telefónica Móviles, S.A.; Telenor
64 R&D; Thales e-Security; UNINETT AS; VeriSign, Inc.; Vodafone Group Plc.; and Wells
65 Fargo.

66
67 All rights reserved.

68

69 **Contents**

70

71 **1 Introduction 5**

72 **2 Assurance Levels 6**

73 2.1 Assurance Level Policy Overview..... 6

74 2.2 Description of the Four Assurance Levels 7

75 2.2.1 Assurance Level 1..... 8

76 2.2.2 Assurance Level 2..... 8

77 2.2.3 Assurance Level 3..... 9

78 2.2.4 Assurance Level 4..... 9

79 **3 Service Assessment Criteria 10**

80 3.1 Context and Scope 10

81 3.2 Readership..... 10

82 3.3 Terminology 11

83 3.4 Criteria Descriptions 11

84 3.5 Common Organizational Service Assessment Criteria 12

85 3.5.1 Assurance Level 1..... 12

86 3.5.2 Assurance Level 2..... 13

87 3.5.3 Assurance Level 3..... 20

88 3.5.4 Assurance Level 4..... 28

89 3.6 Identity Proofing Service Assessment Criteria 36

90 3.6.1 Assurance Level 1..... 37

91 3.6.2 Assurance Level 2..... 38

92 3.6.3 Assurance Level 3..... 43

93 3.6.4 Assurance Level 4..... 47

94 3.6.5 Compliance Tables..... 51

95 3.7 Credential Management Service Assessment Criteria 54

96 3.7.1 Part A--Credential Operating Environment 54

97 3.7.2 Part B--Credential Issuing..... 64

98 3.7.3 Part C--Credential Revocation..... 75

99 3.7.4 Part D--Credential Status Management 84

100 3.7.5 Part E--Credential Validation/Authentication..... 87

101 3.7.6 Compliance Tables..... 89

102 **4 Accreditation and Certification Rules..... 97**

103 4.1 Assessor Accreditation..... 97

104 4.1.1 Criteria for Assessor Accreditation..... 97

105 4.1.2 Assessment..... 98

106 4.1.3 Accreditation Decision and Appeal 98

107 4.1.4 Maintaining Accreditation 98

108 4.2 Certification of Credential Service Provider Offerings 99

109 4.2.1 Process of Certification..... 99

110 4.2.2 Criteria for Certification of CSP Line of BUSINESS 100

111 4.2.3 Certification Decision 101

112	4.2.4	Appeals Process	101
113	4.2.5	Maintaining Certification.....	102
114	4.3	Process for Handling Non-Compliance	102
115	4.3.1	Compliance Determination.....	Error! Bookmark not defined.
116	4.3.2	Period to Cure	Error! Bookmark not defined.
117	4.3.3	Administrative Recourse.....	Error! Bookmark not defined.
118	4.4	Acceptable Public Statements Regarding IAEG Accreditation and Certification	
119		102
120	5	Business Rules.....	103
121	5.1	Scope.....	103
122	5.2	Participation	103
123	5.3	Roles and Obligations	104
124	5.3.1	IAEG.....	104
125	5.3.2	CSP Obligations.....	104
126	5.3.3	Relying Party Obligations.....	105
127	5.3.4	Assessor Obligations.....	106
128	5.3.5	General Obligations	107
129	5.4	Enforcement and Recourse	108
130	5.4.1	Breach of Accreditation or Certification Requirements	108
131	5.4.2	Monetary Recourse	108
132	5.4.3	Administrative Recourse.....	109
133	5.5	General Terms	110
134	5.5.1	Governing Law	110
135	5.5.2	Disclaimer	110
136	5.5.3	Assignment and Succession.....	110
137	5.5.4	Hold Harmless	111
138	5.5.5	Severability	111
139	5.6	Interpretation.....	111
140	6	IAEG Glossary.....	112
141	7	Publication Acknowledgements	118
142	8	References	122
143			
144			

145 **1 Introduction**

146 Liberty Alliance formed the Identity Assurance Expert Group (IAEG) to foster adoption
147 of identity trust services. Utilizing initial contributions from the e-Authentication
148 Partnership (EAP) and the US E-Authentication Federation, the IAEG's objective is to
149 create a framework of baseline policies, business rules, and commercial terms against
150 which identity trust services can be assessed and evaluated. The goal is to facilitate
151 trusted identity federation to promote uniformity and interoperability amongst identity
152 service providers. The primary deliverable of IAEG is the Liberty Identity Assurance
153 Framework (LIAF).

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

161 Assurance Levels (ALs) are the levels of trust associated with a credential as measured by
162 the associated technology, processes, and policy and practice statements. The LIAF
163 defers to the guidance provided by the National Institute of Standards and Technology
164 (NIST) Special Publication 800-63 version 1.0.1 [[NIST800-63](#)] which outlines four (4)
165 levels of assurance, ranging in confidence level from low to very high. Use of ALs is
166 determined by the level of confidence or trust necessary to mitigate risk in the
167 transaction.

168 The Service and Credential Assessment Criteria section in the LIAF will establish
169 baseline criteria for general organizational conformity, identity proofing services,
170 credential strength, and credential management services against which all CSPs will be
171 evaluated. The LIAF will also establish Credential Assessment Profiles (CAPs) for each
172 level of assurance that will be published and updated as needed to account for
173 technological advances and preferred practice and policy updates.

174 The LIAF will employ a phased approach to establishing criteria for certification and
175 accreditation, first focusing on the certification of credential service providers (CSPs) and
176 the accreditation of those who will assess and evaluate them. The goal of this phased
177 approach is to initially provide federations and Federation Operators with the means to
178 certify their members for the benefit of inter-federation and streamlining the certification
179 process for the industry. Follow-on phases will target the development of criteria for
180 certification of relying parties and federations, themselves.

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

183 2 Assurance Levels

184 2.1 Assurance Level Policy Overview

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

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

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

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

217

218 **2.2 Description of the Four Assurance Levels**

219 The four ALs describe the degree of certainty associated with an identity. The levels are
 220 identified by both a number and a text label. The levels are defined as shown in Table 2-
 221 1:

222

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

223

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

230

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 agency programs or public interests	N/A	Min	Mod	High
Unauthorized release of sensitive information	N/A	Min	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>				

231

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

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

241 **2.2.1 Assurance Level 1**

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

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

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

257 **2.2.2 Assurance Level 2**

258 At AL2, there is confidence that an asserted identity is accurate. Moderate risk is
259 associated with erroneous authentication. Single-factor remote network authentication is
260 appropriate. Successful authentication requires that the claimant prove control of the
261 token through a secure authentication protocol. Eavesdropper, replay, and online
262 guessing attacks are prevented. Although the identity proofing requirements may be
263 similar to those for AL1, the authentication mechanisms must be more secure.

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

269 beneficiary's address of record, the transaction entails moderate risk of unauthorized
270 release of personally sensitive data.

271 **2.2.3 Assurance Level 3**

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

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

285 **2.2.4 Assurance Level 4**

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

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

301 **3 Service Assessment Criteria**

302 **3.1 Context and Scope**

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

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

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

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

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

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

323 **3.2 Readership**

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

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

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

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

338 3.3 Terminology

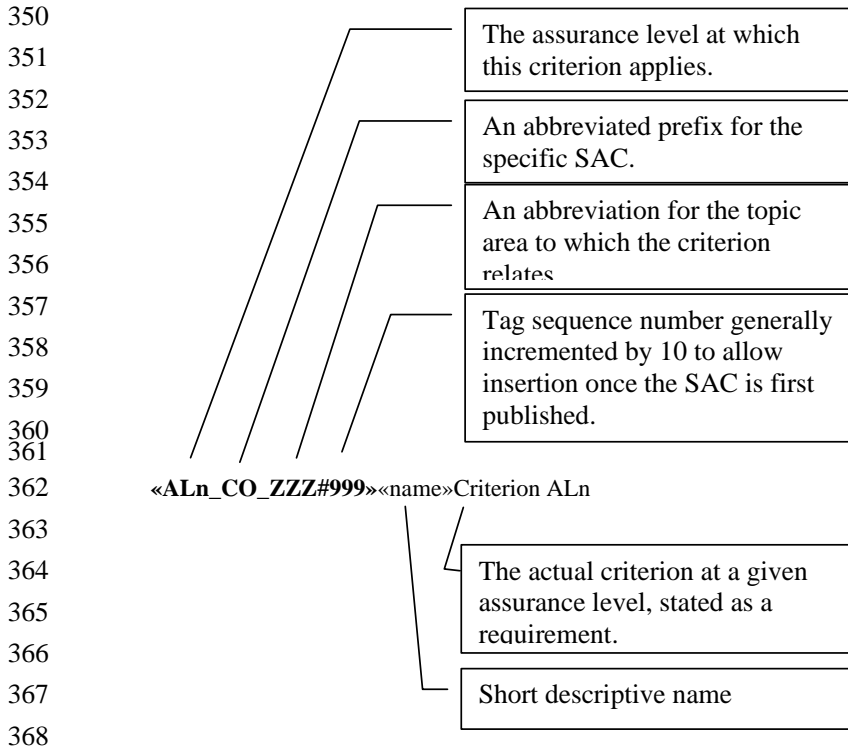
339 All special terms used in this description are defined in the IAEG Glossary.

340 3.4 Criteria Descriptions

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

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

349 The criteria are described as follows:



369 **3.5 Common Organizational Service Assessment Criteria**

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

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

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

378 **3.5.1 Assurance Level 1**

379 **3.5.1.1 Enterprise and Service Maturity**

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

383 An enterprise and its specified service must:

384 **AL1_CO_ESM#010 Established enterprise**

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

387 **AL1_CO_ESM#020 Established service**

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

390 **AL1_CO_ESM#030 Legal compliance**

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

394

395 **3.5.1.2 Notices and User information**

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

398 An enterprise and its specified service must:

399 **AL1_CO_NUI#010** **General Service Definition**

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

403 **AL1_CO_NUI#030** **Due notification**

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

407 **AL1_CO_NUI#040** **User Agreement**

408 Through a user agreement:

- 409 a) require the subscriber to provide full and correct information as required under the
- 410 terms of their use of the service.
- 411 b) obtain a record (hard-copy or electronic) of the subscriber's agreement to the
- 412 terms and conditions of service.
- 413

414 **3.5.1.3** **Information Security Management**

415 No stipulation.

416 **3.5.1.4** **Secure Communications**

417 **AL1_CO_SCO#020** **Protection of secrets**

418 Ensure that:

- 419 a) access to shared secrets shall be subject to discretionary controls which permit
- 420 access to those roles/applications which need such access.
- 421 b) stored shared secrets are not held in their plaintext form.
- 422 c) any plaintext passwords or secrets are not transmitted across any public or
- 423 unsecured network.
- 424

425 **3.5.2** **Assurance Level 2**

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

429 **3.5.2.1 Enterprise and Service Maturity**

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

432 An enterprise and its specified service must:

433 **AL2_CO_ESM#010 Established enterprise**

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

436 **AL2_CO_ESM#020 Established service**

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

439 **AL2_CO_ESM#030 Legal compliance**

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

443 **AL2_CO_ESM#040 Financial Provisions**

444 Demonstrate that it has adequate financial resources for the continued operation of the
445 service and has in place appropriate provision for the degree of liability exposure being
446 carried.

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

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

453

454 **3.5.2.2 Notices and User Information/Agreements**

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

458 An enterprise and its specified service must:

459 **AL2_CO_NUI#010** **General Service Definition**

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

465 **AL2_CO_NUI#020** **Service Definition sections**

466 Publish a service definition for the specified service containing clauses that provide the
467 following information:

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

485 **AL2_CO_NUI#030** **Due notification**

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

491 **AL2_CO_NUI#050** **Subscriber Information**

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

494 **AL2_CO_NUI#060** **Subscriber Agreement**

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

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

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

502 **AL2_CO_NUI#080** **Helpdesk facility**

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

506

507 **3.5.2.3** **Information Security Management**

508 These criteria apply to the way in which the enterprise manages security for its business,
509 the specified service, and information relating to its user community. These criteria focus
510 on the key components of an effective Information Security Management System (ISMS).

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) [AL4
569 provided by a trusted time-source], and such records must be retained with appropriate
570 protection, accounting for service definition, risk management requirements, and
571 applicable legislation.

572

573 **3.5.2.5 Operational infrastructure**

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

577 An enterprise and its specified service must:

578 **AL2_CO_OPN#010 Technical security**

579 Demonstrate that the technical controls employed will provide the level of security
580 required by the risk assessment plan and the ISMS and that these controls are effectively
581 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) and
585 other job descriptions. Where the role is security-critical or where special privileges or
586 shared duties exist, these must be specifically highlighted, including access privileges
587 relating to logical and physical parts of the service's operations.

588 **AL2_CO_OPN#030 Personnel recruitment**

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

592 **AL2_CO_OPN#040 Personnel skills**

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

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

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

601 **AL2_CO_OPN#060 Physical access control**

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

604 **AL2_CO_OPN#070 Logical access control**

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

607

608 **3.5.2.6 External Services and Components**

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

612 An enterprise and its specified service must:

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

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

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

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

625

626 **3.5.2.7** **Secure Communications**

627 An enterprise and its specified service must:

628 **AL2_CO_SCO#010** **Secure remote communications**

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

635 **AL2_CO_SCO#020** **Protection of secrets**

636 Ensure that:

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

643 **3.5.3** **Assurance Level 3**

644 Achieving AL3 requires meeting all criteria required to achieve AL2. This section
645 includes only requirements additional to those described in Section 3.5.2.

646 **3.5.3.1** **Enterprise and Service Maturity**

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

649 An enterprise and its specified service must:

650 **AL3_CO_ESM#010** **Established enterprise**

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

653 **AL3_CO_ESM#020** **Established service**

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

656 **AL3_CO_ESM#030** **Legal compliance**

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

660 **AL3_CO_ESM#040** **Financial Provisions**

661 Demonstrate that it has adequate financial resources for the continued operation of the
662 service and has in place appropriate provision for the degree of liability exposure being
663 carried.

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

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

670 **AL3_CO_ESM#060** **Ownership**

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

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

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

678

679 **3.5.3.2 Notices and User Information**

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

683 An enterprise and its specified service must:

684 **AL3_CO_NUI#010 General Service Definition**

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

690 **AL3_CO_NUI#020 Service Definition Sections**

691 Publish a service definition for the specified service containing clauses that provide the
692 following information:

- 693 a) the legal jurisdiction under, or country in, which the service is operated;
694 b) if different to the above, the legal jurisdiction under which subscriber and any
695 relying party agreements are entered into;
696 c) applicable legislation with which the service complies;
697 d) obligations incumbent upon the ETSP;
698 e) obligations incumbent upon the subscriber;
699 f) notifications and guidance for relying parties, especially in respect of actions they
700 are expected to take should they choose to rely upon the service's product;
701 g) statement of warranties;
702 h) statement of liabilities;
703 i) procedures for notification of changes to terms and conditions;
704 j) steps the ETSP will take in the event that it chooses or is obliged to terminate the
705 service;
706 k) full contact details for the ETSP (i.e., conventional post, telephone, Internet)
707 including a help desk;
708 l) availability of the specified service *per se* and of its help desk facility;
709 m) termination of aspects or all of service.

710 **AL3_CO_NUI#030 Due notification**

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

716 **AL3_CO_NUI#050** **Subscriber Information**

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

719 **AL3_CO_NUI#060** **Subscriber Agreement**

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

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

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

727 **AL3_CO_NUI#080** **Helpdesk facility**

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

731

732 **3.5.3.3** **Information Security Management**

733 Criteria in this section address the way in which the enterprise manages the security of its
734 business, the specified service, and information it holds relating to its user community.
735 This focuses on the key components that make up a well-established Information Security
736 Management System (ISMS).

737 An enterprise and its specified service must:

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

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

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

744 Have a clearly defined managerial role, at a senior level, where full responsibility for the
745 business' security policies is vested and from which promulgation of policy and related

746 procedures is controlled and managed. The policies in place must be properly maintained
747 so as to be effective at all times.

748 **AL3_CO_ISM#030 Risk Management**

749 Demonstrate a risk management methodology that adequately identifies and mitigates
750 risks related to the specified service and its user community and must show that a risk
751 assessment review is performed at least once every six months.

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

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

756 **AL3_CO_ISM#050 Configuration Management**

757 Demonstrate a configuration management system that at least includes:

- 758 a) version control for software system components;
- 759 b) timely identification and installation of all applicable patches for any software
760 used in the provisioning of the specified service;
- 761 c) version control and managed distribution for all documentation associated with
762 the specification, management, and operation of the system, covering both
763 internal and publicly available materials.

764 **AL3_CO_ISM#060 Quality Management**

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

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

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

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

779 **AL3_CO_ISM#080 Internal Service Audit**

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

784 **AL3_CO_ISM#090 Independent Audit**

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

789 **AL3_CO_ISM#100 Audit Records**

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

795 **AL3_CO_ISM#110 Termination provisions**

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

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

802 Have in place an Information Security Management System (ISMS) that follows best
803 practices as accepted by the information security industry and that applies and is
804 appropriate to the CSP in question. All requirements defined by preceding criteria in this
805 section must fall wholly within the scope of this ISMS.

806

807 **3.5.3.4 Security-Relevant Event (Audit) Records**

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

810 An enterprise and its specified service must:

811 **AL3_CO_SER#010 Security Event Logging**

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

814

815 **3.5.3.5 Operational Infrastructure**

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

819 An enterprise and its specified service must:

820 **AL3_CO_OPN#010 Technical security**

821 Demonstrate that the technical controls employed will provide the level of security
822 required by the risk assessment plan and the ISMS, and that these controls are effectively
823 integrated with the appropriate procedural and physical security measures.

824 **AL3_CO_OPN#020 Defined security roles**

825 Define, by means of a job description, the roles and responsibilities for every security-
826 relevant task, relating it to specific procedures (which shall be set out in the ISMS) and
827 other job descriptions. Where the role is security-critical or where special privileges or
828 shared duties exist, these must be specifically highlighted, including access privileges
829 relating to logical and physical parts of the service's operations.

830 **AL3_CO_OPN#030 Personnel recruitment**

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

836 **AL3_CO_OPN#040 Personnel skills**

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

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

843 Have sufficient staff to operate the specified service according to its policies and
844 procedures.

845 **AL3_CO_OPN#060 Physical access control**

846 Apply physical access control mechanisms to ensure access to sensitive areas is restricted
847 to authorized personnel.

848 **AL3_CO_OPN#070 Logical access control**

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

851

852 **3.5.3.6 External Services and Components**

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

856 An enterprise and its specified service must:

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

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

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

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

869

870 **3.5.3.7 Secure Communications**

871 An enterprise and its specified service must:

872 **AL3_CO_SCO#010 Secure remote communications**

873 If the specific service components are located remotely from and communicate over a
874 public or unsecured network with other service components or other CSPs it services, the
875 communications must be cryptographically authenticated by an authentication protocol
876 that meets, at a minimum, the requirements of AL3 and encrypted using an Approved
877 Encryption method.

878 **AL3_CO_SCO#020 Protection of secrets**

879 Ensure that:

- 880 a) access to shared secrets shall be subject to discretionary controls that permit
881 access to those roles/applications requiring such access.
- 882 b) stored shared secrets are encrypted such that:
 - 883 i the encryption key for the shared secret file is encrypted under a key held
884 in a FIPS 140-2 [FIPS140-2] Level 2 (or higher) validated hardware
885 cryptographic module or encryption method of equivalent rigor, or any
886 FIPS 140-2 Level 3 or 4 cryptographic module and decrypted only as
887 immediately required for an authentication operation.
 - 888 ii they are protected as a key within the boundary of a FIPS 140-2 Level 2
889 (or higher) validated hardware cryptographic module, or encryption
890 method of equivalent rigor, or any FIPS 140-2 Level 3 or 4 cryptographic
891 module and are not exported in plaintext from the module.
 - 892 iii they are split by an "*n from m*" cryptographic secret-sharing method.
- 893 c) any long-term (i.e., not session) shared secrets are revealed only to the subscriber
894 and CSP direct agents (bearing in mind "a," above).
895

896 **3.5.4 Assurance Level 4**

897 Achieving AL4 requires meeting all criteria required to achieve AL3. This section
898 includes only requirements additional to those described in Section 3.5.3.

899 **3.5.4.1 Enterprise and Service Maturity**

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

902 An enterprise and its specified service must:

903 **AL4_CO_ESM#010 Established enterprise**

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

906 **AL4_CO_ESM#020** **Established service**

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

909 **AL4_CO_ESM#030** **Legal compliance**

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

913 **AL4_CO_ESM#040** **Financial Provisions**

914 Demonstrate that it has adequate financial resources for the continued operation of the
915 service and has in place appropriate provision for the degree of liability exposure being
916 carried.

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

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

923 **AL4_CO_ESM#060** **Ownership**

924 If the enterprise named as the ETSP is a part of a larger entity, the nature of the
925 relationship with its parent organization, shall be disclosed to the assessors and, on their
926 request, to customers.

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

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

931

932 **3.5.4.2 Notices and User Information/Agreements**

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

936 An enterprise and its specified service must:

937 **AL4_CO_NUI#010** **General Service Definition**

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

943 **AL4_CO_NUI#020** **Service Definition Sections**

944 Publish a service definition for the specified service containing clauses that provide the
945 following information:

- 946 a) the country in or legal jurisdiction under which the service is operated;
- 947 b) if different to the above, the legal jurisdiction under which subscriber and any
948 relying party agreements are entered into;
- 949 c) applicable legislation with which the service complies;
- 950 d) obligations incumbent upon the ETSP;
- 951 e) obligations incumbent upon the subscriber;
- 952 f) notifications and guidance for relying parties, especially in respect of actions they
953 are expected to take should they choose to rely upon the service's product;
- 954 g) statement of warranties;
- 955 h) statement of liabilities;
- 956 i) procedures for notification of changes to terms and conditions;
- 957 j) steps the ETSP will take in the event that it chooses or is obliged to terminate the
958 service;
- 959 k) full contact details for the ETSP (i.e., conventional post, telephone, Internet)
960 including a help desk;
- 961 l) availability of the specified service *per se* and of its help desk facility;
- 962 m) termination of aspects or all of service.

963 **AL4_CO_NUI#030** **Due Notification**

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

969 **AL4_CO_NUI#050** **Subscriber Information**

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

972 **AL4_CO_NUI#060** **Subscriber Agreement**

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

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

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

980 **AL4_CO_NUI#080** **Helpdesk facility**

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

984

985 **3.5.4.3** **Information Security Management**

986 Criteria in this section address the way in which the enterprise manages the security of its
987 business, the specified service, and information it holds relating to its user community.
988 This focuses on the key components that make up a well-established Information Security
989 Management System (ISMS).

990 An enterprise and its specified service must:

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

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

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

997 Have a clearly defined managerial role, at a senior level, where full responsibility for the
998 business' security policies is vested and from which promulgation of policy and related
999 procedures is controlled and managed. The policies in place must be properly maintained
1000 so as to be effective at all times.

1001 **AL4_CO_ISM#030 Risk Management**

1002 Demonstrate a risk management methodology that adequately identifies and mitigates
1003 risks related to the specified service and its user community and must show that on-going
1004 risk assessment review is conducted as a part of the business' procedures.

1005 **AL4_CO_ISM#040 Continuity of Operations Plan**

1006 Have and shall keep updated a continuity of operations plan that covers disaster recovery
1007 and the resilience of the specified service and must show that on-going review of this
1008 plan is conducted as a part of the business' procedures.

1009 **AL4_CO_ISM#050 Configuration Management**

1010 Demonstrate a configuration management system that at least includes:

- 1011 a) version control for software system components;
- 1012 b) timely identification and installation of all applicable patches for any software
1013 used in the provisioning of the specified service;
- 1014 c) version control and managed distribution for all documentation associated with
1015 the specification, management, and operation of the system, covering both
1016 internal and publicly available materials.

1017 **AL4_CO_ISM#060 Quality Management**

1018 Demonstrate a quality management system that is appropriate for the specified service.

1019 **AL4_CO_ISM#070 System Installation and Operation Controls**

1020 Apply controls during system development, procurement, installation, and operation that
1021 protect the security and integrity of the system environment, hardware, software, and
1022 communications having particular regard to:

- 1023 a) the software and hardware development environments, for customized
1024 components;
- 1025 b) the procurement process for COTS components;
- 1026 c) contracted consultancy/support services;
- 1027 d) shipment of system components;
- 1028 e) storage of system components;
- 1029 f) installation environment security;
- 1030 g) system configuration;
- 1031 h) transfer to operational status.

1032 **AL4_CO_ISM#080 Internal Service Audit**

1033 Unless it can show that by reason of its size or for other arguable operational reason it is
1034 unreasonable so to perform, be regularly audited for effective provision of the specified
1035 service by internal audit functions independent of the parts of the enterprise responsible
1036 for the specified service.

1037 **AL4_CO_ISM#090 Independent Audit**

1038 Be audited by an independent auditor at least every 24 months to ensure the
1039 organization's security-related practices are consistent with the policies and procedures
1040 for the specified service and the appointed auditor must have appropriate accreditation or
1041 other acceptable experience and qualification.

1042 **AL4_CO_ISM#100 Audit Records**

1043 Retain full records of all audits, both internal and independent, for a period which, as a
1044 minimum, fulfils its legal obligations and otherwise for greater periods either as it may
1045 have committed to in its service definition or required by any other obligations it has
1046 with/to a subscriber. Such records must be held securely and protected against loss,
1047 alteration, or destruction.

1048 **AL4_CO_ISM#110 Termination provisions**

1049 Have in place a clear plan for the protection of subscribers' private and secret information
1050 related to their use of the service which must ensure the ongoing secure preservation and
1051 protection of legally-required records and for the secure destruction and disposal of any
1052 such information whose retention is not legally required. Essential details of this plan
1053 must be published.

1054 **AL4_CO_ISM#120 Best Practice Security Management**

1055 Have in place a certified Information Security Management System (ISMS) that has been
1056 assessed and found to be in compliance with the code of practice ISO/IEC 17799
1057 [\[ISO/IEC17799\]](#) through application of practices defined in BS 7799 Part 2 [\[BSI7799-2\]](#)
1058 and which applies and is appropriate to the ETPS in question. All requirements expressed
1059 in preceding criteria in this "ISM" section must *inter alia* fall wholly within the scope of
1060 this ISMS.

1061

1062 **3.5.4.4 Security-Related (Audit) Records**

1063 The criteria in this section are concerned with the need to provide an auditable log of all
1064 events that are pertinent to the correct and secure operation of the service.

1065 An enterprise and its specified service must:

1066 **AL4_CO_SER#010 Security Event Logging**

1067 Maintain a log of all security-relevant events concerning the operation of the service,
1068 together with a precise record of the time at which the event occurred (time-stamp)
1069 provided by a trusted time-source and such records must be retained with appropriate
1070 protection, accounting for service definition, risk management requirements, and
1071 applicable legislation.

1072

1073 **3.5.4.5 Operational Infrastructure**

1074 The criteria in this section address the infrastructure within which the delivery of the
1075 specified service takes place. It puts particular emphasis upon the personnel involved,
1076 and their selection, training, and duties.

1077 An enterprise and its specified service must:

1078 **AL4_CO_OPN#010 Technical Security**

1079 Demonstrate that the technical controls employed will provide the level of security
1080 required by the risk assessment plan and the ISMS, and that these controls are effectively
1081 integrated with the appropriate procedural and physical security measures.

1082 **AL4_CO_OPN#020 Defined Security Roles**

1083 Define, by means of a job description, the roles and responsibilities for every security-
1084 relevant task, relating it to specific procedures (which shall be set out in the ISMS) and
1085 other job descriptions. Where the role is security-critical or where special privileges or
1086 shared duties exist, these must be specifically highlighted, including access privileges
1087 relating to logical and physical parts of the service's operations.

1088 **AL4_CO_OPN#030 Personnel Recruitment**

1089 Demonstrate that it has defined practices for the selection, vetting, and contracting of all
1090 personnel, both direct employees and those whose services are provided by third parties.
1091 Full records of all searches and supporting evidence of qualifications and past
1092 employment must be kept for the duration of the individual's employment plus the longest
1093 lifespan of any credential issued under the service policy.

1094 **AL4_CO_OPN#040 Personnel skills**

1095 Ensure that employees are sufficiently trained, qualified, experienced, and current for the
1096 roles they fulfill. Such measures must be accomplished either by recruitment practices or

1097 through a specific training program. Where employees are undergoing on-the-job
1098 training, they must only do so under the guidance of a mentor with established leadership
1099 skills.

1100 **AL4_CO_OPN#050 Adequacy of Personnel resources**

1101 Have sufficient staff to operate the specified service according to its policies and
1102 procedures.

1103 **AL4_CO_OPN#060 Physical access control**

1104 Apply physical access control mechanisms to ensure access to sensitive areas is restricted
1105 to authorized personnel.

1106 **AL4_CO_OPN#070 Logical access control**

1107 Employ logical access control mechanisms to ensure access to sensitive system functions
1108 and controls is restricted to authorized personnel.

1109

1110 **3.5.4.6 External Services and Components**

1111 This section addresses the relationships and obligations upon contracted parties both to
1112 apply the policies and procedures of the enterprise and also to be available for assessment
1113 as critical parts of the overall service provision.

1114 An enterprise and its specified service must:

1115 **AL4_CO_ESC#010 Contracted Policies and Procedures**

1116 Where the enterprise uses the services of external suppliers for specific packaged
1117 components of the service or for resources which are integrated with its own operations
1118 and under its controls, ensure that those parties are engaged through reliable and
1119 appropriate contractual arrangements which stipulate critical policies, procedures, and
1120 practices that the sub-contractor is required to fulfill.

1121 **AL4_CO_ESC#020 Visibility of Contracted Parties**

1122 Where the enterprise uses the services of external suppliers for specific packaged
1123 components of the service or for resources which are integrated with its own operations
1124 and under its controls, ensure that contractors' compliance with contractually stipulated
1125 policies and procedures, and thus with the IAEG's assessment criteria, can be proven and
1126 subsequently monitored.

1127

1128 **3.5.4.7 Secure Communications**

1129 An enterprise and its specified service must:

1130 **AL4_CO_SCO#010 Secure remote communications**

1131 If the specific service components are located remotely from and communicate over a
1132 public or unsecured network with other service components or other ETSP(s) it services,
1133 the communications must be cryptographically authenticated by an authentication
1134 protocol that meets, as a minimum, the requirements of AL4 and encrypted using an
1135 approved encryption method.

1136 **AL4_CO_SCO#020 Protection of secrets**

1137 Ensure that:

- 1138 a) access to shared secrets shall be subject to discretionary controls which permit
1139 access to those roles/applications which need such access;
- 1140 b) stored shared secrets are encrypted such that:
- 1141 i the encryption key for the shared secret file is encrypted under a key held
1142 in a FIPS 140-2 [FIPS140-2] Level 2 (or higher) validated hardware
1143 cryptographic module, or encryption method of equivalent rigor, or any
1144 FIPS 140-2 Level 3 or 4 cryptographic module and decrypted only as
1145 immediately required for an authentication operation.
- 1146 ii they are protected as a key within the boundary of a FIPS 140-2 Level 2
1147 (or higher) validated hardware cryptographic module, or encryption
1148 method of equivalent rigor, or any FIPS 140-2 Level 3 or 4 cryptographic
1149 module and are not exported in plaintext from the module.
- 1150 iii they are split by an "*n from m*" cryptographic secret-sharing method.
- 1151 c) any long-term (i.e., not session) shared secrets are revealed only to the subscriber
1152 and the ETSP's direct agents (bearing in mind (a) above).
1153

1154 **3.6 Identity Proofing Service Assessment Criteria**

1155 The Service Assessment Criteria in this section establish the requirements for the
1156 technical conformity of identity proofing services at all ALs defined in Section 2. These
1157 criteria apply to a particular kind of electronic trust service (ETS) recognized by the
1158 IAEG and to the related electronic trust service provider (ETSP)—an identity proofing
1159 service. (For definitions of terms used in this section, see Section 6). These criteria are
1160 generally referred to elsewhere within IAEG documentation as ID-SAC [ID-SAC].

1161 These criteria do not address the delivery of a credential to the applicant/subscriber,
1162 which is dealt with by the Credential Management SAC (CM-SAC), described in Section
1163 3.7.

1164 These criteria may only be used in an assessment in one of the following circumstances:

- 1165 • In conjunction with the Common Organizational SAC (CO-SAC), described in
1166 Section 3.5, for a standalone identity proofing service.
- 1167 • In combination with one or more other SACs that must include the CO-SAC and
1168 where the identity proofing functions that these criteria address form part of a
1169 larger service offering.
- 1170 Note: Some of the SAC-identifying numbers are not used in all of the ALs. In such cases,
1171 the particular SAC number has been reserved where not used and skipped.

1172 **3.6.1 Assurance Level 1**

1173 **3.6.1.1 Policy**

1174 An enterprise or specified service must:

1175 **AL1_ID_POL#010 Unique service identity**

1176 Ensure that a unique identity is attributed to the specific service, such that credentials
1177 issued by it can be distinguishable from those issued by other services, including services
1178 operated by the same enterprise.

1179 **AL1_ID_POL#020 Unique subject identity**

1180 Ensure that each applicant's identity is unique within the service's community of subjects
1181 and uniquely associable with tokens and/or credentials issued to that identity.

1182

1183 **3.6.1.2 Identity Verification**

1184 **3.6.1.2.1 In-Person Public Verification**

1185 An enterprise or specified service must:

1186 **AL1_ID_IPV#010 Required evidence**

1187 Ensure that the applicant possesses any one of the following forms of evidence:

- 1188 a) one form of Federal, national or state-issued identity;
1189 b) one signed bank or credit card;
1190 c) two utility statements;
1191 d) any other equivalent form of proof.

1192 **AL1_ID_IPV#020 Evidence checks**

1193 Ensure that the name on the evidence offered bears the name the applicant claims and, in
1194 addition, establish, according to the form of evidence provided, any one of the following:

- 1195 a) the applicant appears to be the person named;
1196 b) the applicant can reproduce any signatures shown on bank cards;
1197 c) addresses provided are consistent;
1198 d) any other checks that establish an equivalent degree of certitude.
1199

1200 **3.6.1.2.2 Remote Public Verification**

1201 If the specific service offers remote identity proofing to applicants with whom it has no
1202 previous relationship, then it must comply with the criteria in this section.

1203 An enterprise or specified service must:

1204 **AL1_ID_RPV#010 Required evidence**

1205 Require the applicant to provide a contact telephone number or email address.

1206 **AL1_ID_RPV#020 Evidence checks**

1207 Verify the provided information by either:

- 1208 a) confirming the request by calling the number.
1209 b) successfully sending a confirmatory email and receiving a positive
1210 acknowledgement.
1211

1212 **3.6.1.2.3 Secondary Verification**

1213 In each of the above cases, an enterprise or specified service must:

1214 **AL1_ID_SCV#010 Secondary checks**

1215 Have in place additional measures (e.g., require additional documentary evidence, delay
1216 completion while out-of-band checks are undertaken) to deal with any anomalous
1217 circumstances that can be reasonably anticipated (e.g., a legitimate and recent change of
1218 address that has yet to be established as the address of record).

1219

1220 **3.6.1.3 Verification Records**

1221 No criteria.

1222 **3.6.2 Assurance Level 2**

1223 **3.6.2.1 Policy**

1224 The specific service must show that it applies identity proofing policies and procedures
1225 and that it retains appropriate records of identity proofing activities and evidence.

1226 The enterprise or specified service must:

1227 **AL2_ID_POL#010 Unique service identity**

1228 Ensure that a unique identity is attributed to the specific service, such that credentials
1229 issued by it can be distinguishable from those issued by other services, including services
1230 operated by the same enterprise.

1231 **AL2_ID_POL#020 Unique subject identity**

1232 Ensure that each applicant's identity is unique within the service's community of subjects
1233 and uniquely associable with tokens and/or credentials issued to that identity.

1234 **AL2_ID_POL#030 Published Proofing Policy**

1235 Publish the Identity Proofing Policy under which it verifies the identity of applicants¹ in
1236 form, language, and media accessible to the declared community of users.

1237 **AL2_ID_POL#040 Adherence to Proofing Policy**

1238 Perform all identity proofing strictly in accordance with its published Identity Proofing
1239 Policy, through application of the procedures and processes set out in its Identity Proofing
1240 Practice Statement.

1241

1242 **3.6.2.2 Identity Verification**

1243 The specific service must offer at least one of the following classes of identity proofing
1244 service and may offer any additional sets it chooses, subject to the nature and the
1245 entitlement of the CSP concerned.

1246 **3.6.2.2.1 In-Person Public Verification**

1247 If the specific service offers in-person identity proofing to applicants with whom it has no
1248 previous relationship, then it must comply with the criteria in this section.

1249 The enterprise or specified service must:

¹ 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.

1250 **AL2_ID_IPV#010** **Required evidence**

1251 Ensure that the applicant is in possession of a primary Government Picture ID document
1252 that bears a photographic image of the holder.

1253 **AL2_ID_IPV#020** **Evidence checks**

1254 Ensure that the presented document:

- 1255 a) appears to be a genuine document properly issued by the claimed issuing
1256 authority and valid at the time of application;
1257 b) bears a photographic image of the holder that matches that of the applicant;
1258 c) states an address at which the applicant can be contacted.
1259

1260 **3.6.2.2.2 Remote Public Verification**

1261 If the specific service offers remote identity proofing to applicants with whom it has no
1262 previous relationship, then it must comply with the criteria in this section.

1263 An enterprise or specified service must:

1264 **AL2_ID_RPV#010** **Required evidence**

1265 Ensure that the applicant submits the references of and attests to current possession of a
1266 primary Government Picture ID document, and provides additional verifiable personal
1267 information that at a minimum must include:

- 1268 a) a name that matches the referenced photo-ID;
1269 b) date of birth;
1270 c) current address or personal telephone number;
1271 d) the issuer, account number, and expiration date of a current credit card.
1272 Additional information may be requested so as to ensure a unique identity, and alternative
1273 information may be sought where the enterprise can show that it leads to at least the same
1274 degree of certitude when verified.

1275 **AL2_ID_RPV#020** **Evidence checks**

1276 Electronically verify by a record check against the provided identity references with the
1277 specified issuing authorities/institutions or through similar databases:

- 1278 a) the existence of such records with matching name and reference numbers;
1279 b) corroboration of date of birth, current address of record, and other personal
1280 information sufficient to ensure a unique identity.
1281 Additional checks may be performed so as to establish the uniqueness of the claimed
1282 identity, and alternative checks may be performed where the enterprise can show that they
1283 lead to at least the same degree of certitude.

1284

1285 **3.6.2.2.3 Current Relationship Verification**

1286 If the specific service offers identity proofing to applicants with whom it has a current
1287 relationship, then it must comply with the criteria in this section.

1288 The enterprise or specified service must:

1289 **AL2_ID_CRV#010 Required evidence**

1290 Ensure that it has previously exchanged a shared secret (e.g., a PIN or password) that
1291 meets entropy requirements for the AL with the applicant.

1292 **AL2_ID_CRV#020 Evidence checks**

1293 Ensure that it has:

- 1294 a) only issued the shared secret after originally establishing the applicant's identity
1295 with a degree of rigor equivalent to that required under either the AL2 (or higher)
1296 requirements for in-person or remote public verification
1297 b) an ongoing business relationship sufficient to satisfy the enterprise of the
1298 applicant's continued personal possession of the shared secret.
1299

1300 **3.6.2.2.4 Affiliation Verification**

1301 If the specific service offers identity proofing to applicants on the basis of some form of
1302 affiliation, then it must comply with the criteria in this section for the purposes of
1303 establishing that affiliation, in addition to the previously stated requirements for the
1304 verification of the individual's identity.

1305 The enterprise or specified service must:

1306 **AL2_ID_AFV#010 Required evidence**

1307 Ensure that the applicant possesses:

- 1308 a) identification from the organization with which it is claiming affiliation;
1309 b) agreement from the organization that the applicant may be issued a credential
1310 indicating that an affiliation exists.

1311 **AL2_ID_AFV#020 Evidence checks**

1312 Ensure that the presented documents:

- 1313 a) each appear to be a genuine document properly issued by the claimed issuing
1314 authorities and valid at the time of application;
1315 b) refer to an existing organization with a contact address;

- 1316 c) indicate that the applicant has some form of recognizable affiliation with the
1317 organization;
1318 d) appear to grant the applicant an entitlement to obtain a credential indicating its
1319 affiliation with the organization.
1320

1321 **3.6.2.2.5 Secondary Verification**

1322 In each of the above cases, the enterprise or specified service must:

1323 **AL2_ID_SCV#010 Secondary checks**

1324 Have in place additional measures (e.g., require additional documentary evidence, delay
1325 completion while out-of-band checks are undertaken) to deal with any anomalous
1326 circumstances that can be reasonably anticipated (e.g., a legitimate and recent change of
1327 address that has yet to be established as the address of record).
1328

1329 **3.6.2.3 Verification Records**

1330 The specific service must retain records of the identity proofing (verification) that it
1331 undertakes.

1332 An enterprise or specified service must:

1333 **AL2_ID_VRC#010 Verification Records for Personal Applicants**

1334 Log, taking account of all applicable legislative and policy obligations, a record of the
1335 facts of the verification process. At a minimum, records of identity information must
1336 include:

- 1337 a) the applicant's full name as shown on the government-issued ID;
1338 b) the applicant's date of birth;
1339 c) the applicant's current address of record;
1340 d) the subscriber's current telephone or email address of record;
1341 e) type, issuing authority, and reference number(s) of all documents checked in the
1342 identity proofing process;
1343 f) where required, a telephone or email address for related contact and/or delivery of
1344 credentials/notifications;
1345 g) any pseudonym used by the applicant in lieu of the verified identity;
1346 h) date and time of verification.

1347 **AL2_ID_VRC#020 Verification Records for Affiliated Applicants**

1348 In addition to the foregoing, log, taking account of all applicable legislative and policy
1349 obligations, a record of the additional facts of the verification process. At a minimum,
1350 records of identity information must include:

- 1351 a) the subscriber's full name;
1352 b) the subscriber's current address of record;
1353 c) the subscriber's current telephone or email address of record;
1354 d) the subscriber's acknowledgement for issuing the subject with a credential;
1355 e) type, issuing authority, and reference number(s) of all documents checked in the
1356 identity proofing process.

1357 **AL2_ID_VRC#030 Record Retention**

1358 Either retain, securely, the record of the verification process for the duration of the
1359 subscriber account plus 7.5 years, or submit same record to a client CSP that has
1360 undertaken to retain the record for the requisite period or longer.

1361 **3.6.3 Assurance Level 3**

1362 **3.6.3.1 Policy**

1363 The specific service must show that it applies identity proofing policies and procedures
1364 and that it retains appropriate records of identity proofing activities and evidence.

1365 The enterprise or specified service must:

1366 **AL3_ID_POL#010 Unique service identity**

1367 Ensure that a unique identity is attributed to the specific service, such that credentials
1368 issued by it can be distinguishable from those issued by other services, including services
1369 operated by the same enterprise.

1370 **AL3_ID_POL#020 Unique subject identity**

1371 Ensure that each applicant's identity is unique within the service's community of subjects
1372 and uniquely associable with tokens and/or credentials issued to that identity.

1373 **AL3_ID_POL#030 Published Proofing Policy**

1374 Publish the Identity Proofing Policy under which it verifies the identity of applicants² in
1375 form, language, and media accessible to the declared community of Users.

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.

1376 **AL3_ID_POL#040 Adherence to Proofing Policy**

1377 Perform all identity proofing strictly in accordance with its published Identity Proofing
1378 Policy, applying the procedures and processes set out in its Identity Proofing Practice
1379 Statement.

1380

1381 **3.6.3.2 Identity Verification**

1382 The specific service must offer at least one of the following classes of identity proofing
1383 services and may offer any additional services it chooses, subject to the nature and the
1384 entitlement of the CSP concerned.

1385 **3.6.3.2.1 In-Person Public Verification**

1386 A specific service that offers identity proofing to applicants with whom it has no previous
1387 relationship must comply with the criteria in this section.

1388 The enterprise or specified service must:

1389 **AL3_ID_IPV#010 Required evidence**

1390 Ensure that the applicant is in possession of a primary Government Picture ID document
1391 that bears a photographic image of the holder.

1392 **AL3_ID_IPV#020 Evidence checks**

1393 Ensure that the presented document:

- 1394 a) appears to be a genuine document properly issued by the claimed issuing
1395 authority and valid at the time of application;
1396 b) bears a photographic image of the holder that matches that of the applicant;
1397 c) states an address at which the applicant can be contacted;
1398 d) is electronically verified by a record check with the specified issuing authority or
1399 through similar databases that:
1400 i) establishes the existence of such records with matching name and
1401 reference numbers;
1402 ii) corroborates date of birth, current address of record, and other personal
1403 information sufficient to ensure a unique identity.
1404

1405 **3.6.3.2.2 Remote Public Verification**

1406 A specific service that offers remote identity proofing to applicants with whom it has no
1407 previous relationship must comply with the criteria in this section.

1408 The enterprise or specified service must:

1409 **AL3_ID_RPV#010 Required evidence**

1410 Ensure that the applicant submits details of and attests to current possession of:

- 1411 a) a primary Government Picture ID document, and either
- 1412 i) an account number issued by a regulated financial institution, or
- 1413 ii) a source of personal information relating to the applicant.

1414 **AL3_ID_RPV#020 Evidence checks**

1415 Electronically verify by a record check against the provided identity references with the
1416 specified issuing authorities/institutions or through similar databases:

- 1417 a) the existence of such records with matching name and reference numbers;
- 1418 b) corroboration of date of birth, current address of record or personal telephone
1419 number, and other personal information sufficient to ensure a unique identity;
- 1420 c) dynamic verification of personal information previously provided by or likely to
1421 be known only by the applicant.
1422

1423 **3.6.3.2.3 Affiliation Verification**

1424 A specific service that offers identity proofing to applicants on the basis of some form of
1425 affiliation must comply with the criteria in this section to establish that affiliation and
1426 with the previously stated requirements to verify the individual's identity.

1427 The enterprise or specified service must:

1428 **AL3_ID_AFV#010 Required evidence**

1429 Ensure that the applicant possesses:

- 1430 a) identification from the organization with which it is claiming affiliation;
- 1431 b) agreement from the organization that the applicant may be issued a credential
1432 indicating that an affiliation exists.

1433 **AL3_ID_AFV#020 Evidence checks**

1434 Ensure that the presented documents:

- 1435 a) each appear to be a genuine document properly issued by the claimed issuing
1436 authorities and valid at the time of application;
- 1437 b) refer to an existing organization with a contact address;
- 1438 c) indicate that the applicant has some form of recognizable affiliation with the
1439 organization;
- 1440 d) appear to grant the applicant an entitlement to obtain a credential indicating an
1441 affiliation with the organization.
1442

1443 **3.6.3.2.4 Secondary Verification**

1444 In each of the above cases, the enterprise or specified service must also meet the
1445 following criteria:

1446 **AL3_ID_SCV#010 Secondary checks**

1447 Have in place additional measures (e.g., require additional documentary evidence, delay
1448 completion while out-of-band checks are undertaken) to deal with any anomalous
1449 circumstance that can reasonably be anticipated (e.g., a legitimate and recent change of
1450 address that has yet to be established as the address of record).

1451 **3.6.3.3 Verification Records**

1452 The specific service must retain records of the identity proofing (verification) that it
1453 undertakes.

1454 The enterprise or specified service must:

1455 **AL3_ID_VRC#010 Verification Records**

1456 Log, taking account of all applicable legislative and policy obligations, a record of the
1457 facts of the verification process. At a minimum, records of identity information must
1458 include:

- 1459 a) the applicant's full name as stated on the primary documents;
- 1460 b) the applicant's date and place of birth (as declared, but not necessarily verified);
- 1461 c) the applicant's current address of record;
- 1462 d) the subscriber's current telephone or email address of record;
- 1463 e) type, issuing authority, and reference number(s) of all documents checked in the
1464 identity proofing process;
- 1465 f) any pseudonym used by the applicant in lieu of the verified identity;
- 1466 g) date and time of verification;
- 1467 h) identity of the registrar;
- 1468 i) identity of the CSP providing the verification service or the location at which the
1469 (in-house) verification was performed.

1470 **AL3_ID_VRC#020 Verification Records for Affiliated Applicants**

1471 In addition to the foregoing, log, taking account of all applicable legislative and policy
1472 obligations, a record of the additional facts of the verification process. At a minimum,
1473 records of identity information must include:

- 1474 a) the subscriber's full name;
- 1475 b) the subscriber's current address of record;
- 1476 c) the subscriber's current telephone or email address of record;
- 1477 d) the subscriber's acknowledgement of issuing the subject with a credential;

- 1478 e) type, issuing authority, and reference number(s) of all documents checked in the
1479 identity proofing process;
1480 f) where required, a telephone or email address for related contact and/or delivery of
1481 credentials/notifications.

1482 **AL3_ID_VRC#030 Record Retention**

1483 Either retain, securely, the record of the verification/revocation process for the duration of
1484 the subscriber account plus 7.5 years, or submit the same record to a client CSP that has
1485 undertaken to retain the record for the requisite period or longer.

1486 **3.6.4 Assurance Level 4**

1487 Identity proofing at Assurance Level 4 requires the physical presence of the applicant in
1488 front of the registration officer with photo ID or other readily verifiable biometric identity
1489 information, as well as the requirements set out by the following criteria.

1490 **3.6.4.1 Policy**

1491 The specific service must show that it applies identity proofing policies and procedures
1492 and that it retains appropriate records of identity proofing activities and evidence.

1493 The enterprise or specified service must:

1494 **AL4_ID_POL#010 Unique service identity**

1495 Ensure that a unique identity is attributed to the specific service, such that credentials
1496 issued by it can be distinguishable from those issued by other services, including services
1497 operated by the same enterprise.

1498 **AL4_ID_POL#020 Unique subject identity**

1499 Ensure that each applicant's identity is unique within the service's community of subjects
1500 and uniquely associable with tokens and/or credentials issued to that identity.

1501 **AL4_ID_POL#030 Published Proofing Policy**

1502 Publish the Identity Proofing Policy under which it verifies the identity of applicants³ in
1503 form, language, and media accessible to the declared community of users.

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 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.

1504 **AL4_ID_POL#040 Adherence to Proofing Policy**

1505 Perform all identity proofing strictly in accordance with its published Identity Proofing
1506 Policy, applying the procedures and processes set out in its Identity Proofing Practice
1507 Statement.

1508

1509 **3.6.4.2 Identity Verification**

1510 The specific service may offer only face-to-face identity proofing service. Remote
1511 verification is not allowed at this level.

1512 The enterprise or specified service must:

1513 **3.6.4.2.1 In-Person Public Verification**

1514 **AL4_ID_IPV#010 Required evidence**

1515 Ensure that the applicant is in possession of:

- 1516 a) a primary Government Picture ID document that bears a photographic image of
1517 the holder and either
1518 i) secondary Government Picture ID or an account number issued by a
1519 regulated financial institution, or
1520 ii) two items confirming name, and address or telephone number, such as:
1521 utility bill, professional license or membership, or other evidence of
1522 equivalent standing.

1523 **AL4_ID_IPV#030 Evidence checks – primary ID**

1524 Ensure that the presented document:

- 1525 a) appears to be a genuine document properly issued by the claimed issuing
1526 authority and valid at the time of application;
1527 b) bears a photographic image of the holder which matches that of the applicant;
1528 c) states an address at which the applicant can be contacted;
1529 d) is electronically verified by a record check with the specified issuing authority or
1530 through similar databases that:
1531 i) establishes the existence of such records with matching name and
1532 reference numbers;
1533 ii) corroborates date of birth, current address of record, and other personal
1534 information sufficient to ensure a unique identity.

1535 **AL4_ID_IPV#040 Evidence checks – secondary ID**

1536 Ensure that the presented document meets the following conditions:

- 1537 1) If it is secondary Government Picture ID,

- 1538 a) appears to be a genuine document properly issued by the claimed issuing
1539 authority and valid at the time of application,
1540 b) bears a photographic image of the holder which matches that of the
1541 applicant,
1542 c) states an address at which the applicant can be contacted.
1543 2) If it is a financial institution account number,
1544 a) is verified by a record check with the specified issuing authority or
1545 through similar databases that:
1546 i) establishes the existence of such records with matching name and
1547 reference numbers,
1548 ii) corroborates date of birth, current address of record, and other
1549 personal information sufficient to ensure a unique identity.
1550 3) If it is two utility bills or equivalent documents,
1551 a) each appears to be a genuine document properly issued by the claimed
1552 issuing authority,
1553 b) corroborates current address of record or telephone number sufficient to
1554 ensure a unique identity.

1555 **AL4_ID_IPV#050 Applicant knowledge checks**

1556 Where the applicant is unable to satisfy any of the above requirements, that the applicant
1557 can provide a unique identifier, such as a Social Security Number (SSN), that matches the
1558 claimed identity.

1559

1560 **3.6.4.2.2 Affiliation Verification**

1561 A specific service that offers identity proofing to applicants on the basis of some form of
1562 affiliation must comply with the criteria in this section to establish that affiliation, in
1563 addition to complying with the previously stated requirements for verifying the
1564 individual's identity.

1565 The enterprise or specified service must:

1566 **AL4_ID_AFV#010 Required evidence**

1567 Ensure that the applicant possesses:

- 1568 a) identification from the organization with which the applicant is claiming
1569 affiliation;
1570 b) agreement from the organization that the applicant may be issued a credential
1571 indicating that an affiliation exists.

1572 **AL4_ID_AFV#020 Evidence checks**

1573 Ensure that the presented documents:

- 1574 a) each appear to be a genuine document properly issued by the claimed issuing
1575 authorities and valid at the time of application;
1576 b) refer to an existing organization with a contact address;
1577 c) indicate that the applicant has some form of recognizable affiliation with the
1578 organization;
1579 d) appear to grant the applicant an entitlement to obtain a credential indicating an
1580 affiliation with the organization.
1581

1582 **3.6.4.2.3 Secondary Verification**

1583 In each of the above cases, the enterprise or specified service must also meet the
1584 following criteria:

1585 **AL4_ID_SCV#010 Secondary checks**

1586 Have in place additional measures (e.g., require additional documentary evidence, delay
1587 completion while out-of-band checks are undertaken) to deal with any anomalous
1588 circumstances that can reasonably be anticipated (e.g., a legitimate and recent change of
1589 address that has yet to be established as the address of record).

1590

1591 **3.6.4.3 Verification Records**

1592 The specific service must retain records of the identity proofing (verification) that it
1593 undertakes.

1594 The enterprise or specified service must:

1595 **AL4_ID_VRC#010 Verification Records for Personal Applicants**

1596 Log, taking account of all applicable legislative and policy obligations, a record of the
1597 facts of the verification process. At a minimum, records of identity information must
1598 include:

- 1599 a) the applicant's full name,
1600 b) the applicant's date and place of birth (as declared, but not necessarily verified),
1601 c) the applicant's current address of record,
1602 d) the type, issuing authority, and reference number(s) of all documents checked in
1603 the identity proofing process,
1604 e) a telephone or email address for related contact and/or delivery of
1605 credentials/notifications,
1606 f) any pseudonym used by the applicant in lieu of the verified identity,
1607 g) a biometric record of the applicant (e.g., a photograph, fingerprint, voice
1608 recording),
1609 h) date and time of verification issued by a trusted time-source,

- 1610 i) the signature of the applicant,
1611 j) identity of the registrar,
1612 k) identity of the CSP providing the verification service or the location at which the
1613 (in-house) verification was performed.

1614 **AL4_ID_VRC#020 Verification Records for Affiliated Applicants**

1615 In addition to the foregoing, log, taking account of all applicable legislative and policy
1616 obligations, a record of the additional facts of the verification process. At a minimum,
1617 records of identity information must include:

- 1618 a) the subscriber's full name,
1619 b) the subscriber's current address of record,
1620 c) the subscriber's current telephone or email address of record,
1621 d) the subscriber's authorization for issuing the subject a credential,
1622 e) type, issuing authority, and reference number(s) of all documents checked in the
1623 identity proofing process,
1624 f) a biometric record of each required representative of the affiliating organization
1625 (e.g., a photograph, fingerprint, voice recording), as determined by that
1626 organization's governance rules/charter.

1627 **AL4_ID_VRC#030 Record Retention**

1628 Either retain, securely, the record of the verification/revocation process for the duration of
1629 the subscriber account plus 10.5 years, or submit the record to a client CSP that has
1630 undertaken to retain the record for the requisite period or longer.

1631 **3.6.5 Compliance Tables**

1632 Use the following tables to correlate criteria for a particular AL and the evidence offered
1633 to support compliance.

1634 CSPs preparing for an assessment can use the table appropriate to the level at which they
1635 are seeking approval to correlate evidence with criteria or to justify non-applicability
1636 (e.g., "specific service types not offered"). Assessors can use the tables to record
1637 assessment steps and their determination of compliance or failure.

1638 **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	

1639

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	

1640

1641

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	

1642

1643

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	

1644

1645 **3.7 Credential Management Service Assessment Criteria**

1646 The Service Assessment Criteria in this section establish requirements for the functional
1647 conformity of credential management services and their providers at all ALs defined in
1648 Section 2. These criteria are generally referred to elsewhere within IAEG documentation
1649 as CM-SAC.

1650 The criteria are divided into five parts. Each part deals with a specific functional aspect
1651 of the overall credential management process.

1652 This SAC must be used in conjunction with the Common Organizational SAC (CO-
1653 SAC), described in Section 3.5, and, in addition, must either:

- 1654 • explicitly include the criteria of the Identity Proofing SAC ([ID-SAC]) described
1655 in Section 3.6, or
- 1656 • rely upon the criteria of the ID-SAC [ID-SAC] being fulfilled by the use of an
1657 IAEG-approved ID-proofing service.

1658 Note: Some of the SAC-identifying numbers are not used in all of the ALs. In such cases,
1659 the particular SAC number has been reserved where not used and skipped.

1660 **3.7.1 Part A--Credential Operating Environment**

1661 The criteria in this part deal with the overall operational environment in which the
1662 credential life-cycle management is conducted. The credential management service
1663 assessment criteria must be used in conjunction with the common organizational criteria
1664 described in Section 3.5. In addition, they must either explicitly include the identity
1665 proofing service assessment criteria described in Section 3.6 or rely upon those criteria
1666 being fulfilled by the use of an IAEG-approved identity proofing service.

1667 These criteria describe requirements for the overall operational environment in which
1668 credential lifecycle management is conducted. The common organizational criteria
1669 describe broad requirements. The criteria in this section describe implementation
1670 specifics. Implementation depends on the AL. The procedures and processes required to
1671 create a secure environment for management of credentials and the particular
1672 technologies that are considered strong enough to meet the assurance requirements differ
1673 considerably from level to level.

1674 **3.7.1.1 Assurance Level 1**

1675 These criteria apply to PINs and passwords.

1676 **3.7.1.1.1 Credential Policy and Practices**

1677 These criteria apply to the policy and practices under which credentials are managed.

1678 An enterprise and its specified service must:

1679 **AL1_CM_CPP#010** **Credential Policy and Practice Statement**

1680 No stipulation.

1681

1682 **3.7.1.1.2 Security Controls**

1683 An enterprise and its specified service must:

1684 **AL1_CM_CTR#010** **Secret revelation**

1685 No stipulation.

1686 **AL1_CM_CTR#020** **Protocol threat risk assessment and controls**

1687 Account for the following protocol threats and apply appropriate controls:

- 1688 a) password guessing,
- 1689 b) message replay.

1690 **AL1_CM_CTR#030** **System threat risk assessment and controls**

1691 Account for the following system threats and apply appropriate controls:

- 1692 a) the introduction of malicious code,
- 1693 b) compromised authentication arising from insider action,
- 1694 c) out-of-band attacks by other users and system operators (e.g., shoulder-surfing),
- 1695 d) spoofing of system elements/applications,
- 1696 e) malfeasance on the part of subscribers and subjects.

1697

1698 **3.7.1.1.3 Storage of Long-term Secrets**

1699 An enterprise and its specified service must:

1700 **AL1_CM_STS#010** **Stored Secrets**

1701 *Not* store secrets (such as passwords) as plain text and apply discretionary access controls
1702 that limit access to administrators and those applications that require access.

1703

1704 **3.7.1.1.4 Security-relevant Event (Audit) Records**

1705 No stipulation.

1706 **3.7.1.1.5 Subject Options**

1707 An enterprise and its specified service must:

1708 **AL1_CM_OPN#010 Changeable PIN/Password**

1709 Permit subjects to change their PINs/passwords.

1710

1711 **3.7.1.2 Assurance Level 2**

1712 These criteria apply to passwords.

1713 **3.7.1.2.1 Credential Policy and Practices**

1714 These criteria apply to the policy and practices under which credentials are managed.

1715 An enterprise and its specified service must:

1716 **AL2_CM_CPP#010 Credential Policy and Practice Statement**

1717 Include in its service definition a description of the policy against which it issues
1718 credentials and the corresponding practices it applies in their management. At a
1719 minimum, the Credential Policy and Practice Statement must specify:

- 1720 a) if applicable, any OIDs related to the Practice and Policy Statement;
- 1721 b) how users may subscribe to the service/apply for credentials and how users'
1722 credentials will be delivered to them;
- 1723 c) how subscribers acknowledge receipt of tokens and credentials and what
1724 obligations they accept in so doing (including whether they consent to publication
1725 of their details in credential status directories);
- 1726 d) how credentials may be renewed, modified, revoked, and suspended, including
1727 how requestors are authenticated or their identity re-proven;
- 1728 e) what actions a subscriber must take to terminate a subscription.

1729 **AL2_CM_CPP#030 Management Authority**

1730 Have a nominated management body with authority and responsibility for approving the
1731 Credential Policy and Practice Statement and for its implementation.

1732

1733 **3.7.1.2.2 Security Controls**

1734 An enterprise and its specified service must:

1735 **AL2_CM_CTR#010 Secret revelation**

1736 Use communication and authentication protocols that minimize the duration of any clear-
1737 text disclosure of long-term secrets, even when disclosed to trusted parties.

1738 **AL2_CM_CTR#020 Protocol threat risk assessment and controls**

1739 Account for the following protocol threats in its risk assessment and apply controls that
1740 reduce them to acceptable risk levels:

- 1741 a) password guessing,
- 1742 b) message replay,
- 1743 c) eavesdropping.

1744 **AL2_CM_CTR#030 System threat risk assessment and controls**

1745 Account for the following system threats in its risk assessment and apply controls that
1746 reduce them to acceptable risk levels:

- 1747 a) the introduction of malicious code;
- 1748 b) compromised authentication arising from insider action;
- 1749 c) out-of-band attacks by both users and system operators (e.g., the ubiquitous
1750 shoulder-surfing);
- 1751 d) spoofing of system elements/applications;
- 1752 e) malfeasance on the part of subscribers and subjects;
- 1753 f) intrusions leading to information theft.

1754 **AL2_CM_CTR#040 Specified Service's Key Management**

1755 Specify and observe procedures and processes for the generation, storage, and destruction
1756 of its own cryptographic keys used for securing the specific service's assertions and other
1757 publicized information. At a minimum, these should address:

- 1758 a) the physical security of the environment;
- 1759 b) access control procedures limiting access to the minimum number of authorized
1760 personnel;
- 1761 c) public-key publication mechanisms;
- 1762 d) application of controls deemed necessary as a result of the service's risk
1763 assessment;
- 1764 e) destruction of expired or compromised private keys in a manner that prohibits
1765 their retrieval, or their archival in a manner that prohibits their reuse.

1766

1767 **3.7.1.2.3 Storage of Long-term Secrets**

1768 An enterprise and its specified service must:

1769 **AL2_CM_STS#010 Stored Secrets**

1770 *Not* store secrets (such as passwords) as plain text and apply discretionary access controls
1771 that limit access to administrators and to those applications requiring access.

1772

1773 **3.7.1.2.4 Security-Relevant Event (Audit) Records**

1774 These criteria describe the need to provide an auditable log of all events that are pertinent
1775 to the correct and secure operation of the service. The common organizational criteria
1776 applying to provision of an auditable log of all events pertinent to the correct and secure
1777 operation of the service must also be considered carefully. These criteria carry
1778 implications for credential management operations.

1779 **3.7.1.2.5 Subject Options**

1780 An enterprise and its specified service must:

1781 **AL2_CM_OPN#010 Changeable PIN/Password**

1782 Permit subjects to change their passwords, but employ reasonable practices with respect
1783 to password resets and repeated password failures.

1784

1785 **3.7.1.3 Assurance Level 3**

1786 These criteria apply to one-time password devices and soft crypto applications protected
1787 by passwords or biometric controls.

1788 **3.7.1.3.1 Credential Policy and Practices**

1789 These criteria apply to the policy and practices under which credentials are managed.

1790 An enterprise and its specified service must:

1791 **AL3_CM_CPP#010 Credential Policy and Practice Statement**

1792 Include in its service definition a full description of the policy against which it issues
1793 credentials and the corresponding practices it applies in their issuance. At a minimum,
1794 the Credential Policy and Practice Statement must specify:

- 1795 a) if applicable, any OIDs related to the Credential Policy and Practice Statement;
1796 b) how users may subscribe to the service/apply for credentials and how the users'
1797 credentials will be delivered to them;
1798 c) how subscribers acknowledge receipt of tokens and credentials and what
1799 obligations they accept in so doing (including whether they consent to publication
1800 of their details in credential status directories);
1801 d) how credentials may be renewed, modified, revoked, and suspended, including
1802 how requestors are authenticated or their identity -proven;
1803 e) what actions a subscriber must take to terminate a subscription.

1804 **AL3_CM_CPP#030 Management Authority**

1805 Have a nominated management body with authority and responsibility for approving the
1806 Credential Policy and Practice Statement, and for its implementation.

1807

1808 **3.7.1.3.2 Security Controls**

1809 **AL3_CM_CTR#020 Protocol threat risk assessment and controls**

1810 Account for the following protocol threats in its risk assessment and apply controls that
1811 reduce them to acceptable risk levels:

- 1812 a) password guessing,
- 1813 b) message replay,
- 1814 c) eavesdropping,
- 1815 d) relying party (verifier) impersonation,
- 1816 e) man-in-the-middle attack.

1817 **AL3_CM_CTR#030 System threat risk assessment and controls**

1818 Account for the following system threats in its risk assessment and apply controls that
1819 reduce them to acceptable risk levels:

- 1820 a) the introduction of malicious code;
- 1821 b) compromised authentication arising from insider action;
- 1822 c) out-of-band attacks by both users and system operators (e.g., the ubiquitous
1823 shoulder-surfing);
- 1824 d) spoofing of system elements/applications;
- 1825 e) malfeasance on the part of subscribers and subjects;
- 1826 f) intrusions leading to information theft.

1827 **AL3_CM_CTR#040 Specified Service's Key Management**

1828 Specify and observe procedures and processes for the generation, storage, and destruction
1829 of its own cryptographic keys used for securing the specific service's assertions and other
1830 publicized information. At a minimum, these should address:

- 1831 a) the physical security of the environment;
- 1832 b) access control procedures limiting access to the minimum number of authorized
1833 personnel;
- 1834 c) public-key publication mechanisms;
- 1835 d) application of controls deemed necessary as a result of the service's risk
1836 assessment;
- 1837 e) destruction of expired or compromised private keys in a manner that prohibits
1838 their retrieval **or** their archival in a manner that prohibits their reuse.

1839

1840 **3.7.1.3.3 Storage of Long-term Secrets**

1841 An enterprise and its specified service must:

1842 **AL3_CM_STS#010 Stored Secrets**

1843 *Not* store secrets (such as passwords) as plain text and apply discretionary access controls
1844 that limit access to administrators and to those applications that require access.

1845 **AL3_CM_STS#020 Stored Secret Encryption**

1846 Encrypt such shared secret files so that:

- 1847 a) the encryption key for the shared secret file is encrypted under a key held in a
- 1848 FIPS 140-2 [FIPS140-2] Level 2 or higher validated hardware cryptographic
- 1849 module or any FIPS 140-2 Level 3 or 4 cryptographic module, or encryption
- 1850 method of equivalent rigor;
- 1851 b) the shared secret file is decrypted only as immediately required for an
- 1852 authentication operation;
- 1853 c) shared secrets are protected as a key within the boundary of a FIPS 140-2 Level 2
- 1854 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or
- 1855 4 cryptographic module and are not exported from the module in plain text, or
- 1856 encryption method of equivalent rigor;
- 1857 d) shared secrets are split by an "*n from m*" cryptographic secret sharing method.
- 1858

1859 **3.7.1.3.4 Security-relevant Event (Audit) Records**

1860 These criteria describe the need to provide an auditable log of all events that are pertinent
1861 to the correct and secure operation of the service. The common organizational criteria
1862 applying to the recording of all security-related events must also be considered carefully.
1863 These criteria carry implications for credential management operations.

1864 In the specific context of a certificate management service, an enterprise and its specified
1865 service must:

1866 **AL3_CM_SER#010 Security event logging**

1867 Ensure that such audit records include:

- 1868 a) the identity of the point of registration (irrespective of whether internal or
- 1869 outsourced);
- 1870 b) generation of the subscriber's keys or the evidence that the subscriber was in
- 1871 possession of both parts of their own key-pair;
- 1872 c) generation of the subscriber's certificate;
- 1873 d) dissemination of the subscriber's certificate;

1874 e) any revocation or suspension associated with the subscriber's certificate.
1875

1876 **3.7.1.3.5 Subject options**

1877 An enterprise and its specified service must:

1878 **AL3_CM_OPN#010 Changeable PIN/Password**

1879 Permit subjects to change the password used to activate their credentials.
1880

1881 **3.7.1.4 Assurance Level 4**

1882 These criteria apply exclusively to cryptographic technology deployed through a Public
1883 Key Infrastructure. This technology requires hardware tokens protected by password or
1884 biometric controls. No other forms of credential are permitted at AL4.

1885 **3.7.1.4.1 Certification Policy and Practices**

1886 These criteria apply to the policy and practices under which certificates are managed.

1887 An enterprise and its specified service must:

1888 **AL4_CM_CPP#020 Certificate Policy/Certification Practice Statement**

1889 Include in its service definition its full Certificate Policy and the corresponding
1890 Certification and Practice Statement. The Certificate Policy and Certification Practice
1891 Statement must conform to IETF RFC 3647 (2003-11) [[RFC 3647](#)] in their content and
1892 scope or be demonstrably consistent with the content or scope of that RFC. At a
1893 minimum, the Certificate Policy must specify:

- 1894 a) applicable OIDs for each certificate type issued;
- 1895 b) how users may subscribe to the service/apply for certificates, and how certificates
1896 will be issued to them;
- 1897 c) if users present their own keys, how they will be required to demonstrate
1898 possession of the private key;
- 1899 d) if users' keys are generated for them, how the private keys will be delivered to
1900 them;
- 1901 e) how subscribers acknowledge receipt of tokens and credentials and what
1902 obligations they accept in so doing (including whether they consent to publication
1903 of their details in certificate status directories);
- 1904 f) how certificates may be renewed, re-keyed, modified, revoked, and suspended,
1905 including how requestors are authenticated or their identity proven;
- 1906 g) what actions a subscriber must take to terminate their subscription.

1907 **AL4_CM_CPP#030 Management Authority**

1908 Have a nominated or appointed high-level management body with authority and
1909 responsibility for approving the Certificate Policy and Certification Practice Statement,
1910 including ultimate responsibility for its proper implementation.

1911

1912 **3.7.1.4.2 Security Controls**

1913 An enterprise and its specified service must:

1914 **AL4_CM_CTR#020 Protocol threat risk assessment and controls**

1915 Account for the following protocol threats in its risk assessment and apply controls that
1916 reduce them to acceptable risk levels:

- 1917 a) man-in-the-middle attack,
1918 b) session hijacking.

1919 **AL4_CM_CTR#030 System threat risk assessment and controls**

1920 Account for the following system threats in its risk assessment and apply controls that
1921 reduce them to acceptable risk levels:

- 1922 a) the introduction of malicious code;
1923 b) compromised authentication arising from insider action;
1924 c) out-of-band attacks by both users and system operators (e.g., the ubiquitous
1925 shoulder-surfing);
1926 d) spoofing of system elements/applications;
1927 e) malfeasance on the part of subscribers and subjects;
1928 f) intrusions leading to information theft.

1929 **AL4_CM_CTR#040 Specified Service's Key Management**

1930 Specify and observe procedures and processes for the generation, storage, and destruction
1931 of its own cryptographic keys used for securing the specific service's assertions and other
1932 publicized information. At a minimum, these should address:

- 1933 a) the physical security of the environment;
1934 b) access control procedures limiting access to the minimum number of authorized
1935 personnel;
1936 c) public-key publication mechanisms;
1937 d) application of controls deemed necessary as a result of the service's risk
1938 assessment;
1939 e) destruction of expired or compromised private keys in a manner that prohibits
1940 their retrieval, or their archival in a manner which prohibits their reuse;

1941

1942 **3.7.1.4.3 Storage of Long-term Secrets**

1943 The enterprise and its specified service must meet the following criteria:

1944 **AL4_CM_STS#010 Stored Secrets**

1945 *Not* store secrets (such as private keys) as plain text and must apply discretionary access
1946 controls that limit access to trusted administrators.

1947 **AL4_CM_STS#020 Stored Secret Encryption**

1948 Encrypt such secret files so that:

- 1949 a) the encryption key for the secret file is encrypted under a key held in a FIPS 140-
1950 2 [FIPS140-2] Level 2 or higher validated hardware cryptographic module or any
1951 FIPS 140-2 Level 3 or 4 cryptographic module, or encryption method of
1952 equivalent rigor;
- 1953 b) the secret file is decrypted only as immediately required for a key recovery
1954 operation;
- 1955 c) secrets are protected as a key within the boundary of a FIPS 140-2 Level 2 or
1956 higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4
1957 cryptographic module and are not exported from the module in plaintext, or
1958 encryption method of equivalent rigor;
- 1959 d) escrowed secrets are split by an "*n from m*" cryptographic secret storing method.
1960

1961 **3.7.1.4.4 Security-relevant Event (Audit) Records**

1962 These criteria describe the need to provide an auditable log of all events that are pertinent
1963 to the correct and secure operation of the service. The common organizational criteria
1964 relating to the recording of all security-related events must also be considered carefully.
1965 These criteria carry implications for credential management operations.

1966 An enterprise and its specified service must:

1967 **AL4_CM_SER#010 Security event logging**

1968 Ensure that such audit records include:

- 1969 a) the identity of the point of registration (whether internal or outsourced);
1970 b) generation of the subscriber's keys or evidence that the subscriber was in
1971 possession of both parts of the key-pair;
- 1972 c) generation of the subscriber's certificate;
- 1973 d) dissemination of the subscriber's certificate;
- 1974 e) any revocation or suspension associated with the subscriber's certificate.
1975

1976 **3.7.1.4.5 Subject Options**

1977 An enterprise and its specified service must:

1978 **AL4_CM_OPN#010 Changeable PIN/Password**

1979 Permit subjects to change the passwords used to activate their credentials.

1980 **3.7.2 Part B--Credential Issuing**

1981 These criteria apply to the verification of the identity of the subject of a credential and
1982 with token strength and credential delivery mechanisms. They address requirements
1983 levied by the use of various technologies to achieve the appropriate AL⁴. These criteria
1984 include by reference all applicable criteria in Section 3.6.

1985 **3.7.2.1 Assurance Level 1**

1986 **3.7.2.1.1 Identity Proofing**

1987 These criteria determine how the enterprise shows compliance with the criteria for
1988 fulfilling identity proofing functions.

1989 The enterprise and its specified service must:

1990 **AL1_CM_IDP#010 Self-managed Identity Proofing**

1991 If the enterprise assumes direct responsibility for identity proofing functions, show, by
1992 direct inclusion, compliance with all applicable identity proofing service assessment
1993 criteria⁵ ([ID-SAC]) for AL1 or higher.

1994 **AL1_CM_IDP#020 IAEG-approved outsourced service**

1995 If the enterprise outsources responsibility for identity proofing functions and uses a
1996 service already operating under an IAEG Identity Proofing Approval, show that the
1997 service in question has been approved at AL1 or higher.

1998 **AL1_CM_IDP#030 Non IAEG-approved outsourced service**

1999 If the enterprise outsources responsibility for identity proofing functions, ensure that each
2000 provider of such a service demonstrates compliance with all applicable identity proofing
2001 service assessment criteria for AL1 or higher, and that the enterprise, itself, has in place

⁴ Largely driven by the guidance in NIST SP 800-63 [NIST800-63].

⁵ 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.

- 2002 controls to ensure the continued fulfillment of those criteria by the provider to which the
2003 functions have been outsourced.
- 2004 **AL1_CM_IDP#040 Revision to subscriber information**
- 2005 Provide a means for subscribers to amend their stored information after registration.
- 2006
- 2007 **3.7.2.1.2 Credential Creation**
- 2008 These criteria address the requirements for creation of credentials that can only be used at
2009 AL1. Any credentials/tokens that comply with the criteria stipulated for AL2 and higher
2010 are acceptable at AL1.
- 2011 An enterprise and its specified service must:
- 2012 **AL1_CM_CRN_#010 Authenticated Request**
- 2013 Only accept a request to generate a credential and bind it to an identity if the source of the
2014 request can be authenticated as being authorized to perform identity proofing at AL1 or
2015 higher.
- 2016 **AL1_CM_CRN_#020 Unique identity**
- 2017 Ensure that the identity (e.g., UserID) to which a credential is to be bound is unique
2018 within the specified service's intended community.
- 2019 **AL1_CM_CRN_#030 Token uniqueness**
- 2020 Allow the subscriber to select a unique token (e.g., UserID combined with PIN/password)
2021 that must be validated to be unique within the specified service's intended community and
2022 assigned uniquely to a single identity subject.
- 2023
- 2024 **3.7.2.2 Assurance Level 2**
- 2025 **3.7.2.2.1 Identity Proofing**
- 2026 These criteria determine how the enterprise shows compliance with the criteria for
2027 fulfilling identity proofing functions.
- 2028 The enterprise and its specified service must:

2029 **AL2_CM_IDP#010 Self-managed Identity Proofing**

2030 If the enterprise assumes direct responsibility for identity proofing functions, show, by
2031 direct inclusion, compliance with all applicable identity proofing service assessment
2032 criteria for AL2 or higher.

2033 **AL2_CM_IDP#020 IAEG-approved outsourced service**

2034 If the enterprise outsources responsibility for identity proofing functions and uses a
2035 service already operating under an IAEG Identity Proofing Approval, show that the
2036 service in question has been approved at AL2 or higher and that its approval has at least 6
2037 months of remaining validity.

2038 **AL2_CM_IDP#030 Non IAEG-approved outsourced service**

2039 If the enterprise outsources responsibility for identity proofing functions, ensure that each
2040 provider of such a service demonstrates compliance with all applicable identity proofing
2041 service assessment criteria for AL2 or higher, and that the enterprise, itself, has in place
2042 controls to ensure the continued fulfillment of those criteria by the provider to which the
2043 functions have been outsourced.

2044 **AL2_CM_IDP#040 Revision to subscriber information**

2045 Provide a means for subscribers to securely amend their stored information after
2046 registration, either by re-proving their identity, as in the initial registration process, or by
2047 using their credentials to authenticate their revision.

2048

2049 **3.7.2.2.2 Credential Creation**

2050 These criteria define the requirements for creation of credentials whose highest use is at
2051 AL2. Credentials/tokens that comply with the criteria stipulated at AL3 and higher are
2052 also acceptable at AL2 and below.

2053 Note, however, authentication can only be provided at the assurance level at which the
2054 identity is proven.

2055 An enterprise and its specified service must:

2056 **AL2_CM_CRN_#010 Authenticated Request**

2057 Only accept a request to generate a credential and bind it to an identity if the source of the
2058 request can be authenticated as being authorized to perform identity proofing at AL2 or
2059 higher.

- 2060 **AL2_CM_CRN_#020 Unique identity**
- 2061 Ensure that the identity (e.g., UserID) to which a credential is to be bound is unique
2062 within the specified service's intended community.
- 2063 **AL2_CM_CRN_#030 Token uniqueness**
- 2064 Allow the subscriber to select a unique token (e.g., UserID combined with PIN/password)
2065 that must be validated to be unique within the specified service's intended community and
2066 assigned uniquely to a single identity.
- 2067 **AL2_CM_CRN_#040 Password strength**
- 2068 Only allow passwords that, over the life of the password, have resistance to an on-line
2069 guessing attack against a selected user/password of at least 1 in 2^{14} (16,384), accounting
2070 for state-of-the-art attack strategies.
- 2071 **AL2_CM_CRN_#050 One-time password strength**
- 2072 Only allow password tokens that, over the life of the password, have a resistance to
2073 guessing of 1 in 2^{14} (16,384), accounting for state-of-the-art attack strategies.
- 2074 **AL2_CM_CRN_#060 Software cryptographic token strength**
- 2075 Refer to Section [3.7.2.3](#).
- 2076 **AL2_CM_CRN_#070 Hardware token strength**
- 2077 Refer to Section [3.7.2.3](#).
- 2078 **AL2_CM_CRN_#080 Binding of key**
- 2079 No stipulation.
- 2080 **AL2_CM_CRN_#090 Nature of subject**
- 2081 Record the nature of the subject of the credential (which must correspond to the manner
2082 of identity proofing performed), i.e., physical person, a named person acting on behalf of
2083 a corporation or other legal entity, corporation or legal entity, or corporate machine entity,
2084 in a manner that can be unequivocally associated with the credential and the identity that
2085 it asserts.
- 2086 **3.7.2.2.3 Credential Delivery**
- 2087 An enterprise and its specified service must:

2088 **AL2_CM_CRD_#010 Confirm subject's details**

2089 Confirm the subject's contact details and notify the subject of the credential's issuance by:

- 2090 a) sending notice to the address of record confirmed during identity proofing or
2091 b) issuing the credential(s) in a manner that confirms the address of record supplied
2092 by the applicant during identity proofing or
2093 c) issuing the credential(s) in a manner that confirms the ability of the applicant to
2094 receive telephone communications at a telephone number or email at an email
2095 address supplied by the applicant during identity proofing.
2096

2097 **3.7.2.3 Assurance Level 3**

2098 **3.7.2.3.1 Identity Proofing**

2099 These criteria in this section determine how the enterprise shows compliance with the
2100 criteria for fulfilling identity proofing functions.

2101 The enterprise and its specified service must:

2102 **AL3_CM_IDP#010 Self-managed Identity Proofing**

2103 If the enterprise assumes direct responsibility for identity proofing functions, show, by
2104 direct inclusion, compliance with all applicable identity proofing service assessment
2105 criteria for AL3 or AL4.

2106 **AL3_CM_IDP#020 IAEG-approved outsourced service**

2107 If the enterprise outsources responsibility for identity proofing functions and uses a
2108 service already operating under an IAEG Identity Proofing Approval, show that the
2109 service in question has been approved at AL3 or AL4 and that its approval has at least 6
2110 months of remaining validity.

2111 **AL3_CM_IDP#030 Non IAEG-approved outsourced service**

2112 *Not* use any non-IAEG-approved outsourced services for identity proofing.

2113 **AL3_CM_IDP#040 Revision to subscriber information**

2114 Provide a means for subscribers to securely amend their stored information after
2115 registration, either by re-proving their identity as in the initial registration process or by
2116 using their credentials to authenticate their revision. Successful revision must, where
2117 necessary, instigate the re-issuance of the credential.

2118

2119 **3.7.2.3.2 Credential Creation**

2120 These criteria define the requirements for creation of credentials whose highest use is
2121 AL3. Any credentials/tokens that comply with the criteria stipulated at AL4 are also
2122 acceptable at AL3 and below.

2123 Note, however, that a token and credential created according to these criteria may not
2124 necessarily provide that level of assurance for the claimed identity of the subscriber.
2125 Authentication can only be provided at the assurance level at which the identity is proven.

2126 An enterprise and its specified service must:

2127 **AL3_CM_CRN_#010 Authenticated Request**

2128 Only accept a request to generate a credential and bind it to an identity if the source of the
2129 request can be authenticated as being authorized to perform identity proofing at AL3 or
2130 higher.

2131 **AL3_CM_CRN_#020 Unique identity**

2132 Ensure that the identity (e.g., UserID) to which a credential is to be bound is unique
2133 within the specified service's intended community, accounting fully for identities
2134 previously used and that are now cancelled.

2135 **AL3_CM_CRN_#030 Token uniqueness**

2136 Allow the subscriber to select a unique token (e.g., UserID combined with PIN/password)
2137 that must be validated to be unique within the specified service's intended community and
2138 assigned uniquely to a single identity.

2139 **AL3_CM_CRN_#040 PIN/Password strength**

2140 Must not use PIN/password tokens.

2141 **AL3_CM_CRN_#050 One-time password strength**

2142 Only allow one-time password tokens that:

- 2143 a) depend on a symmetric key stored on a personal hardware device evaluated
2144 against FIPS 140-2 [[FIPS140-2](#)] Level 1 or higher, or encryption method of
2145 equivalent rigor,;
- 2146 b) permit at least 10^6 possible password values;
- 2147 c) require password or biometric activation by the subscriber.

2148 **AL3_CM_CRN_#060 Software cryptographic token strength**

2149 Ensure that software cryptographic keys stored on general-purpose devices:

- 2150 a) are protected by a key and cryptographic protocol that are evaluated against FIPS
2151 140-2 Level 2, or encryption method of equivalent rigor,;
2152 b) require password or biometric activation by the subscriber or employ a password
2153 protocol when being used for authentication.

2154 **AL3_CM_CRN_#070 Hardware token strength**

2155 Ensure that hardware tokens used to store cryptographic keys:

- 2156 a) employ a cryptographic module that is evaluated against FIPS 140-2 Level 1 or
2157 higher, or encryption method of equivalent rigor,;
2158 b) require password or biometric activation by the subscriber or also employ a
2159 password when being used for authentication.

2160 **AL3_CM_CRN_#080 Binding of key**

2161 If the specified service generates the subject's key pair, that the key generation process
2162 securely and uniquely binds that process to the certificate generation and maintains at all
2163 times the secrecy of the private key, until it is accepted by the subject.

2164 **AL3_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., private person, a named person acting on behalf of a
2167 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

2171 **3.7.2.3.3 Subject Key Pair Generation**

2172 An enterprise and its specified service must:

2173 **AL3_CM_SKP_#010 Key generation by Specified Service**

2174 If the specified service generates the subject's keys:

- 2175 a) use a FIPS-approved [FIPS] algorithm, or encryption method of equivalent rigor,
2176 that is recognized as being fit for the purposes of the service;
2177 b) only create keys of a key length and for use with a FIPS-approved public key
2178 algorithm, or encryption method of equivalent rigor, recognized as being fit for
2179 the purposes of the service;
2180 c) generate and store the keys securely until delivery to and acceptance by the
2181 subject;
2182 d) deliver the subject's private key in a manner that ensures that the privacy of the
2183 key is not compromised and only the subject has access to the private key.

2184 **AL3_CM_SKP_#020 Key generation by Subject**

2185 If the subject generates and presents its own keys, obtain the subject's written
2186 confirmation that it has:

- 2187 a) used a FIPS-approved algorithm, or encryption method of equivalent rigor, that is
2188 recognized as being fit for the purposes of the service;
2189 b) created keys of a key length and for use with a FIPS-approved public key
2190 algorithm, or encryption method of equivalent rigor, recognized as being fit for
2191 the purposes of the service.
2192

2193 **3.7.2.3.4 Credential Delivery**

2194 An enterprise and its specified service must:

2195 **AL3_CM_CRD_#010 Confirm subject's details**

2196 Confirm the subject's contact details and notify the subject of the credential's issuance by:

- 2197 a) sending notice to the address of record confirmed during identity proofing, and
2198 either
2199 i) issuing the credential(s) in a manner that confirms the address of record
2200 supplied by the applicant during identity proofing; or
2201 ii) issuing the credential(s) in a manner that confirms the ability of the
2202 applicant to receive telephone communications at a phone number
2203 supplied by the applicant during identity proofing while recording the
2204 applicant's voice.

2205 **AL3_CM_CRD_#020 Subject's acknowledgement**

2206 Receive acknowledgement of receipt of the credential before it is activated and its
2207 directory status record is published (and thereby the subscription becomes active or re-
2208 activated, depending upon the circumstances of issue).

2209

2210 **3.7.2.4 Assurance Level 4**

2211 **3.7.2.4.1 Identity Proofing**

2212 These criteria determine how the enterprise shows compliance with the criteria for
2213 fulfilling identity proofing functions.

2214 An enterprise and its specified service must:

- 2215 **AL4_CM_IDP#010 Self-managed Identity Proofing**
- 2216 If the enterprise assumes direct responsibility for identity proofing functions, show, by
2217 direct inclusion, compliance with all applicable identity proofing service assessment
2218 criteria for AL4.
- 2219 **AL4_CM_IDP#020 IAEG-approved outsourced service**
- 2220 If the enterprise outsources responsibility for identity proofing functions and uses a
2221 service already operating under an IAEG Identity Proofing Approval, show that the
2222 service in question has been approved at AL4 and that its approval has at least 12 months
2223 of remaining validity.
- 2224 **AL4_CM_IDP#030 Non IAEG-approved outsourced service**
- 2225 Not use any non-IAEG-approved outsourced services for identity proofing unless they
2226 can be demonstrated to have satisfied equivalently rigorous requirements established by
2227 another scheme recognized by IAEG.
- 2228 **AL4_CM_IDP#040 Revision to subscriber information**
- 2229 Provide a means for subscribers to securely amend their stored information after
2230 registration, either by re-proving their identity as in the initial registration process or by
2231 using their credentials to authenticate their revision. Successful revision must, where
2232 necessary, instigate the re-issuance of the credential.
- 2233 **3.7.2.4.2 Credential Creation**
- 2234 These criteria define the requirements for creation of credentials whose highest use is
2235 AL4.
- 2236 Note, however, that a token and credential created according to these criteria may not
2237 necessarily provide that level of assurance for the claimed identity of the subscriber.
2238 Authentication can only be provided at the assurance level at which the identity is proven.
2239 An enterprise and its specified service must:
- 2240 **AL4_CM_CRN_#010 Authenticated Request**
- 2241 Only accept a request to generate a credential and bind it to an identity if the source of the
2242 request can be authenticated as being authorized to perform identity proofing at AL4.
- 2243 **AL4_CM_CRN_#020 Unique identity**
- 2244 Ensure that the identity (e.g., UserID) to which a credential is to be bound is unique
2245 within the specified service's intended community.

- 2246 **AL4_CM_CRN_#030** **Token uniqueness**
- 2247 Allow the subscriber to select a unique token (e.g., UserID combined with PIN/password)
2248 that must be validated to be unique within the specified service's intended community and
2249 assigned uniquely to a single identity.
- 2250 **AL4_CM_CRN_#040** **PIN/Password strength**
- 2251 *Not* use PIN/password tokens.
- 2252 **AL4_CM_CRN_#050** **One-time password strength**
- 2253 *Not* use one-time password tokens.
- 2254 **AL4_CM_CRN_#060** **Software cryptographic token strength**
- 2255 *Not* use software cryptographic tokens.
- 2256 **AL4_CM_CRN_#070** **Hardware token strength**
- 2257 Ensure that hardware tokens used to store cryptographic keys:
- 2258 a) employ a cryptographic module that is evaluated against FIPS 140-2 [\[FIPS140-2\]](#) Level
2259 2 or higher, or encryption method of equivalent rigor;
2260 b) are evaluated against FIPS 140-2 Level 3 or higher, or encryption method of equivalent
2261 rigor, for their physical security;
2262 c) require password or biometric activation by the subscriber.
- 2263 **AL4_CM_CRN_#080** **Binding of key**
- 2264 If the specified service generates the subject's key pair, that the key generation process
2265 securely and uniquely binds that process to the certificate generation and maintains at all
2266 times the secrecy of the private key, until it is accepted by the subject.
- 2267 **AL3_CM_CRN_#090** **Nature of subject**
- 2268 Record the nature of the subject of the credential, i.e., private person, a named person
2269 acting on behalf of a corporation or other legal entity, corporation or legal entity, or
2270 corporate machine entity, in a manner that can be unequivocally associated with the
2271 credential and the identity that it asserts.
2272
- 2273 **3.7.2.4.3 Subject Key Pair Generation**
- 2274 An enterprise and its specified service must:

2275 **AL4_CM_SKP_#010 Key generation by Specified Service**

2276 If the specified service generates the subject's keys:

- 2277 a) use a FIPS-approved [FIPS] algorithm, or encryption method of equivalent rigor,
2278 that is recognized as being fit for the purposes of the service;
- 2279 b) only create keys of a key length and for use with a FIPS-approved public key
2280 algorithm, or encryption method of equivalent rigor, recognized as being fit for
2281 the purposes of the service;
- 2282 c) generate and store the keys securely until delivery to and acceptance by the
2283 subject;
- 2284 d) deliver the subject's private key in a manner that ensures that the privacy of the
2285 key is not compromised and only the subject has access to the private key.

2286 **AL4_CM_SKP_#020 Key generation by Subject**

2287 If the subject generates and presents its own keys, obtain the subject's written
2288 confirmation that it has:

- 2289 a) used a FIPS-approved algorithm, or encryption method of equivalent rigor, that is
2290 recognized as being fit for the purposes of the service;
- 2291 b) created keys of a key length and for use with a FIPS-approved public key
2292 algorithm, or encryption method of equivalent rigor, recognized as being fit for
2293 the purposes of the service.
2294

2295 **3.7.2.4.4 Credential Delivery**

2296 An enterprise and its specified service must:

2297 **AL4_CM_CRD_#010 Confirm subject's details**

2298 Confirm the subject's contact details and notify the subject of the credential's issuance by:

- 2299 a) sending notice to the address of record confirmed during identity proofing;
- 2300 b) unless the subject presented with a private key, issuing the hardware token to the
2301 subject in a manner that confirms the address of record supplied by the applicant
2302 during identity proofing;
- 2303 c) issuing the certificate to the subject over a separate channel in a manner that
2304 confirms either the address of record or the email address supplied by the
2305 applicant during identity proofing.

2306 **AL4_CM_CRD_#020 Subject's acknowledgement**

2307 Receive acknowledgement of receipt of the hardware token before it is activated and the
2308 corresponding certificate and its directory status record are published (and thereby the
2309 subscription becomes active or re-activated, depending upon the circumstances of issue).

2310 **3.7.3 Part C--Credential Revocation**

2311 These criteria deal with credential revocation and the determination of the legitimacy of a
2312 revocation request.

2313 **3.7.3.1 Assurance Level 1**

2314 An enterprise and its specified service must:

2315 **3.7.3.1.1 Not used**

2316 **3.7.3.1.2 Not used**

2317 **3.7.3.1.3 Secure Revocation Request**

2318 This criterion applies when revocation requests between remote components of a service
2319 are made over a secured communication.

2320 An enterprise and its specified service must:

2321 **AL1_ID_SRR#010 Submit Request**

2322 Submit a request for revocation to the Credential Issuer service (function), using a
2323 secured network communication, if necessary.

2324

2325 **3.7.3.2 Assurance Level 2**

2326 **3.7.3.2.1 Revocation Procedures**

2327 These criteria address general revocation functions, such as the processes involved and
2328 the basic requirements for publication.

2329 An enterprise and its specified service must:

2330 **AL2_CM_RVP#010 Revocation procedures**

2331 State the conditions under which revocation of an issued credential may occur, the
2332 processes by which a revocation request may be submitted, the persons and organizations
2333 from which a revocation request will be accepted, the validation steps that will be applied
2334 to ensure the validity (identity) of the Revocant, and the response time between a
2335 revocation request being accepted and the publication of revised certificate status.

2336 **AL2_CM_RVP#020 Secure status notification**

2337 Ensure that published credential status notification information can be relied upon in
2338 terms of the enterprise being its origin (i.e., its authenticity) and its correctness (i.e., its
2339 integrity).

2340 **AL2_CM_RVP#030 Revocation publication**

2341 Ensure that published credential status notification is revised within 72 hours of the
2342 receipt of a valid revocation request, such that any subsequent attempts to use that
2343 credential in an authentication shall be unsuccessful.

2344 **AL2_ID_RVP#040 Verify revocation identity**

2345 Establish that the identity for which a revocation request is received is one that was
2346 issued by the specified service.

2347 **AL2_ID_RVP#050 Revocation Records**

2348 Retain a record of any revocation of a credential that is related to a specific identity
2349 previously verified, solely in connection to the stated credential. At a minimum, records
2350 of revocation must include:

- 2351 a) the Revocant's full name;
- 2352 b) the Revocant's current address;
- 2353 c) type, issuing authority, and reference number(s) of all documents checked in the
2354 identity proofing process for the Revocant;
- 2355 d) the Revocant's authority to revoke (e.g., subscriber themselves, someone acting
2356 with the subscriber's power of attorney, the credential issuer, law enforcement, or
2357 other legal due process);
- 2358 e) the subscriber's full name and, where applicable, unique service reference (e.g.,
2359 certificate serial number, IP address);
- 2360 f) the subscriber's date of birth;
- 2361 g) the subscriber's current address of record;
- 2362 h) the Credential Issuer's identity (if not directly responsible for the identity proofing
2363 service);
- 2364 i) the identity associated with the credential (whether the subscriber's name or a
2365 pseudonym);
- 2366 j) the reason for revocation.

2367 **AL2_ID_RVP#060 Record Retention**

2368 Retain, securely, the record of the revocation process for the duration of the subscriber's
2369 account plus 7.5 years.

2370

2371 **3.7.3.2.2 Verify Revocant's Identity**

2372 The enterprise should not act on a request for revocation without first establishing the
2373 validity of the request (if it does not, itself, determine the need for revocation).

2374 In order to do so, the enterprise and its specified service must:

2375 **AL2_ID_RVR#010** **Verify revocation identity**

2376 Establish that the credential for which a revocation request is received was one that was
2377 issued by the specified service.

2378 **AL2_ID_RVR#020** **Revocation reason**

2379 Establish the reason for the revocation request as being sound and well founded, in
2380 combination with verification of the Revocant, according to AL2_ID_RVR#030,
2381 AL2_ID_RVR#040, or AL2_ID_RVR#050.

2382 **AL2_ID_RVR#030** **Verify Subscriber as Revocant**

2383 When the subscriber seeks revocation of the subscriber's own credential, the enterprise
2384 must:

- 2385 a) if in person, require presentation of a primary Government Picture ID document
2386 that must be electronically verified by a record check against the provided identity
2387 with the specified issuing authority's records, or
- 2388 b) if remote:
 - 2389 i. electronically verify a signature against records (if available), confirmed
2390 with a call to a telephone number of record, or
 - 2391 ii. authenticate an electronic request as being from the same subscriber,
2392 supported by a credential at Assurance Level 2 or higher.

2393 **AL2_ID_RVR#040** **ETSP as Revocant**

2394 Where a CSP seeks revocation of a subscriber's credential, the enterprise must establish
2395 that the request is either:

- 2396 a) from the specified service itself, with authorization as determined by established
2397 procedures, or
- 2398 b) from the client Credential Issuer, by authentication of a formalized request over
2399 the established secure communications network.

2400 **AL2_ID_RVR#050** **Verify Legal Representative as Revocant**

2401 Where the request for revocation is made by a law enforcement officer or presentation of
2402 a legal document, the enterprise must:

- 2403 a) if in person, verify the identity of the person presenting the request, or
- 2404 b) if remote:
 - 2405 i. in paper/facsimile form, verify the origin of the legal document by a
2406 database check or by telephone with the issuing authority, or
 - 2407 ii. authenticate an electronic request as being from a recognized legal office,
2408 supported by a credential at Assurance Level 3 or higher.
2409

2410 **3.7.3.2.3 Secure Revocation Request**

2411 This criterion requires that revocation requests between remote components of the service
2412 be made with secured communications.

2413 An enterprise and its specified service must:

2414 **AL2_ID_SRR#010 Submit Request**

2415 Submit a request for the revocation to the Credential Issuer service (function), using a
2416 secured network communication if necessary.

2417

2418 **3.7.3.3 Assurance Level 3**

2419 **3.7.3.3.1 Revocation Procedures**

2420 These criteria address general revocation functions, such as the processes involved and
2421 the basic requirements for publication.

2422 An enterprise and its specified service must:

2423 **AL3_CM_RVP#010 Revocation procedures**

2424 State the conditions under which revocation of an issued credential may occur, the
2425 processes by which a revocation request may be submitted, the persons and organizations
2426 from which a revocation request will be accepted, the validation steps that will be applied
2427 to ensure the validity (identity) of the Revocant, and the response time between a
2428 revocation request being accepted and the publication of revised certificate status.

2429 **AL3_CM_RVP#020 Secure status notification**

2430 Ensure that published credential status notification information can be relied upon in
2431 terms of the enterprise being its origin (i.e., its authenticity) and its correctness (i.e., its
2432 integrity).

2433 **AL3_CM_RVP#030 Revocation publication**

2434 Ensure that published credential status notification is revised within 24 hours of the
2435 receipt of a valid revocation request, such that any subsequent attempts to use that
2436 credential in an authentication shall be unsuccessful. The nature of the revocation
2437 mechanism shall be in accord with the technologies supported by the service.

2438 **AL3_ID_RVP#050** **Revocation Records**

2439 Retain a record of any revocation of a credential that is related to a specific identity
2440 previously verified, solely in connection to the stated credential. At a minimum, records
2441 of revocation must include:

- 2442 a) the Revocant's full name;
- 2443 b) the Revocant's current address;
- 2444 c) type, issuing authority, and reference number(s) of all documents checked in the
2445 identity proofing process for the Revocant;
- 2446 d) the Revocant's authority to revoke (e.g., subscriber themselves, someone acting
2447 with the subscriber's power of attorney, the credential issuer, law enforcement, or
2448 other legal due process);
- 2449 e) the subscriber's full name and, where applicable, unique service reference (e.g.,
2450 certificate serial number, IP address);
- 2451 f) the subscriber's date of birth;
- 2452 g) the subscriber's current address of record;
- 2453 h) the Credential Issuer's identity (if not directly responsible for the identity proofing
2454 service);
- 2455 i) the identity associated with the credential (whether the subscriber's name or a
2456 pseudonym);
- 2457 j) the reason for revocation.

2458 **AL3_ID_RVP#060** **Record Retention**

2459 Retain, securely, the record of the revocation process for the duration of the subscriber's
2460 account plus 7.5 years.

2461

2462 **3.7.3.3.2 Verify Revocant's Identity**

2463 Revocation of a credential requires that the requestor and the nature of the request be
2464 verified as rigorously as the original identity proofing. The enterprise should not act on a
2465 request for revocation without first establishing the validity of the request (if it does not,
2466 itself, determine the need for revocation).

2467 In order to do so, the enterprise and its specified service must:

2468 **AL3_ID_RVR#010** **Verify revocation identity**

2469 Establish that the credential for which a revocation request is received is one that was
2470 initially issued by the specified service, applying the same process and criteria as would
2471 be applied to an original identity proofing.

2472 **AL3_ID_RVR#020 Revocation reason**

2473 Establish the reason for the revocation request as being sound and well founded, in
2474 combination with verification of the Revocant, according to AL3_ID_RVR#030,
2475 AL3_ID_RVR#040, or AL3_ID_RVR#050.

2476 **AL3_ID_RVR#030 Verify Subscriber as Revocant**

2477 When the subscriber seeks revocation of the subscriber's own credential:

- 2478 a) if in-person, require presentation of a primary Government Picture ID document
- 2479 that must be electronically verified by a record check against the provided identity
- 2480 with the specified issuing authority's records, or
- 2481 b) if remote:
 - 2482 i. electronically verify a signature against records (if available), confirmed
 - 2483 with a call to a telephone number of record, or
 - 2484 ii. authenticate an electronic request as being from the same subscriber,
 - 2485 supported by a credential at Assurance Level 3 or higher.

2486 **AL3_ID_RVR#040 Verify ETSP as Revocant**

2487 Where a CSP seeks revocation of a subscriber's credential, establish that the request is
2488 either:

- 2489 a) from the specified service itself, with authorization as determined by established
- 2490 procedures, or
- 2491 b) from the client Credential Issuer, by authentication of a formalized request over
- 2492 the established secure communications network.

2493 **AL3_ID_RVR#050 Legal Representative as Revocant**

2494 Where the request for revocation is made by a law enforcement officer or presentation of
2495 a legal document:

- 2496 a) if in person, verify the identity of the person presenting the request, or
- 2497 b) if remote:
 - 2498 i. in paper/facsimile form, verify the origin of the legal document by a
 - 2499 database check or by telephone with the issuing authority, or
 - 2500 ii. authenticate an electronic request as being from a recognized legal office,
 - 2501 supported by a credential at Assurance Level 3 or higher.
 - 2502

2503 **3.7.3.3.3 Secure Revocation Request**

2504 This criterion requires that revocation requests between remote components of the service
2505 be made with secured communications.

2506 An enterprise and its specified service must:

2507 **AL3_ID_SRR#010 Submit Request**

2508 Submit a request for the revocation to the Credential Issuer service (function), using a
2509 secured network communication if necessary.

2510

2511 **3.7.3.4 Assurance Level 4**

2512 **3.7.3.4.1 Revocation Procedures**

2513 These criteria address general revocation functions, such as the processes involved and
2514 the basic requirements for publication.

2515 An enterprise and its specified service must:

2516 **AL4_CM_RVP#010 Revocation procedures**

2517 State the conditions under which revocation of an issued certificate may occur, the
2518 processes by which a revocation request may be submitted, the persons and organizations
2519 from which a revocation request will be accepted, the validation steps that will be applied
2520 to ensure the validity (identity) of the Revocant, and the response time between a
2521 revocation request being accepted and the publication of revised certificate status.

2522 **AL4_CM_RVP#020 Secure status notification**

2523 Ensure that published credential status notification information can be relied upon in
2524 terms of the enterprise being its origin (i.e., its authenticity) and its correctness (i.e., its
2525 integrity).

2526 **AL4_CM_RVP#030 Revocation publication**

2527 Ensure that published credential status notification is revised within 24 hours of the
2528 receipt of a valid revocation request, such that any subsequent attempts to use that
2529 credential in an authentication shall be unsuccessful. The nature of the revocation
2530 mechanism shall be in accordance with the technologies supported by the service.

2531 **AL4_ID_RVP#050 Revocation Records**

2532 Retain a record of any revocation of a credential that is related to a specific identity
2533 previously verified, solely in connection to the stated credential. At a minimum, records
2534 of revocation must include:

- 2535 a) the Revocant's full name;
2536 b) the Revocant's current address;
2537 c) type, issuing authority, and reference number(s) of all documents checked in the
2538 identity proofing process for the Revocant;

- 2539 d) the Revocant's authority to revoke (e.g., subscriber themselves, someone acting
2540 with the subscriber's power of attorney, the credential issuer, law enforcement, or
2541 other legal due process);
2542 e) the subscriber's full name and, where applicable, unique service reference (e.g.,
2543 certificate serial number, IP address);
2544 f) the subscriber's date of birth;
2545 g) the subscriber's current address of record;
2546 h) the Credential Issuer's identity (if not directly responsible for the identity proofing
2547 service);
2548 i) the identity associated with the credential (whether the subscriber's name or a
2549 pseudonym);
2550 j) the reason for revocation.

2551 **AL4_ID_RVP#060 Record Retention**

2552 Retain, securely, the record of the revocation process for the duration of the subscriber's
2553 account plus 7.5 years.

2554

2555 **3.7.3.4.2 Revocation and Re-key**

2556 Revocation of a credential requires that the requestor and the nature of the request be
2557 verified as rigorously as the original identity proofing. The enterprise should not act on a
2558 request for revocation without first establishing the validity of the request (if it does not,
2559 itself, determine the need for revocation).

2560 In order to do so, the enterprise and its specified service must:

2561 **AL4_ID_RVR#010 Verify revocation identity**

2562 Establish that the credential for which a revocation request is received is one that was
2563 initially issued by the specified service, applying the same process and criteria as would
2564 apply to an original identity proofing.

2565 **AL4_ID_RVR#020 Revocation reason**

2566 Establish the reason for the revocation request as being sound and well founded, in
2567 combination with verification of the Revocant, according to AL4_CM_RVR#030,
2568 AL4_CM_RVR#040, or AL4_CM_RVR#050.

2569 **AL4_CM_RVR#030 Verify Subscriber as Revocant**

2570 Where the subscriber seeks revocation of the subscriber's own credential:

- 2571 a) if in person, require presentation of a primary Government Picture ID document
2572 that shall be verified by a record check against the provided identity with the
2573 specified issuing authority's records, or
2574 b) if remote:
2575 i. verify a signature against records (if available), confirmed with a call to a
2576 telephone number of record, or
2577 ii. authenticate an electronic request as being from the same subscriber,
2578 supported by a different credential at Assurance Level 4.

2579 **AL4_CM_RVR#040 Verify ETSP as Revocant**

2580 Where a CSP seeks revocation of a subscriber's credential, establish that the request is
2581 either:

- 2582 a) from the specified service itself, with authorization as determined by established
2583 procedures, or
2584 b) from the client Credential Issuer, by authentication of a formalized request over
2585 the established secure communications network.

2586 **AL4_CM_RVR#050 Legal Representative as Revocant**

2587 Where the request for revocation is made by a law enforcement officer or presentation of
2588 a legal document:

- 2589 a) if in person, verify the identity of the person presenting the request, or
2590 b) if remote:
2591 i. in paper/facsimile form, verify the origin of the legal document by a
2592 database check or by telephone with the issuing authority, or
2593 ii. authenticate an electronic request as being from a recognized legal office,
2594 supported by a different credential at Assurance Level 4.

2595 Re-key of a credential requires that the requestor be verified as the subject with as much
2596 rigor as was applied to the original identity proofing. The enterprise should not act on a
2597 request for re-key without first establishing that the requestor is identical to the subject.

2598 In order to do so, the enterprise and its specified service must:

2599 **AL4_CM_RKY#010 Verify Requestor as Subscriber**

2600 Where the subscriber seeks a re-key for the subscriber's own credential:

- 2601 a) if in-person, require presentation of a primary Government Picture ID document
2602 that shall be verified by a record check against the provided identity with the
2603 specified issuing authority's records, or
2604 b) if remote:
2605 i. verify a signature against records (if available), confirmed with a call to a
2606 telephone number of record, or

- 2607 ii. authenticate an electronic request as being from the same subscriber,
2608 supported by a different credential at Assurance Level 4.
2609

2610 **3.7.3.4.3 Re-key requests from any other parties must not be accepted**

2611 **3.7.3.4.4 Secure Revocation/Re-key Request**

2612 This criterion requires that revocation requests between remote components of the service
2613 be made with secured communications.

2614 The enterprise and its specified service must:

2615 **AL4_ID_SRR#010 Submit Request**

2616 Submit a request for the revocation to the Credential Issuer service (function), using a
2617 secured network communication if necessary.

2618 **3.7.4 Part D--Credential Status Management**

2619 These criteria deal with credential status management, such as the receipt of requests for
2620 new status information arising from a new credential being issued or a revocation or other
2621 change to the credential that requires notification. They also deal with the provision of
2622 status information to requesting parties having the right to access such information.

2623 **3.7.4.1 Assurance Level 1**

2624 **3.7.4.1.1 Status Maintenance**

2625 An enterprise and its specified service must:

2626 **AL1_CM_CSM#010 Maintain Status Record**

2627 Maintain a record of the status of all credentials issued.

2628 **AL1_CM_CSM#040 Status Information Availability**

2629 Provide, with 95% availability, a secure automated mechanism to allow relying parties to
2630 determine credential status and authenticate the subject's identity.

2631

2632 **3.7.4.2 Assurance Level 2**

2633 **3.7.4.2.1 Status Maintenance**

2634 An enterprise and its specified service must:

2635 **AL2_CM_CSM#010 Maintain Status Record**

2636 Maintain a record of the status of all credentials issued.

2637 **AL2_CM_CSM#020 Validation of Status Change Requests**

2638 Authenticate all requestors seeking to have a change of status recorded and published and
2639 validate the requested change before considering processing the request. Such validation
2640 should include:

- 2641 a) the requesting source as one from which the specified service expects to receive
- 2642 such requests;
- 2643 b) if the request is not for a new status, the credential or identity as being one for
- 2644 which a status is already held.

2645 **AL2_CM_CSM#030 Revision to Published Status**

2646 Process authenticated requests for revised status information and have the revised
2647 information available for access within a period of 72 hours.

2648 **AL2_CM_CSM#040 Status Information Availability**

2649 Provide, with 95% availability, a secure automated mechanism to allow relying parties to
2650 determine credential status and authenticate the subject's identity.

2651 **AL2_CM_CSM#050 Inactive Credentials**

2652 Disable any credential that has not been successfully authenticated during a period of 12
2653 months.

2654

2655 **3.7.4.3 Assurance Level 3**

2656 **3.7.4.3.1 Status Maintenance**

2657 An enterprise and its specified service must:

2658 **AL3_CM_CSM#010 Maintain Status Record**

2659 Maintain a record of the status of all credentials issued.

2660 **AL3_CM_CSM#020 Validation of Status Change Requests**

2661 Authenticate all requestors seeking to have a change of status recorded and published and
2662 validate the requested change before considering processing the request. Such validation
2663 should include:

- 2664 a) the requesting source as one from which the specified service expects to receive
2665 such requests;
2666 b) if the request is not for a new status, the credential or identity as being one for
2667 which a status is already held.

2668 **AL3_CM_CSM#030 Revision to Published Status**

2669 Process authenticated requests for revised status information and have the revised
2670 information available for access within a period of 72 hours.

2671 **AL3_CM_CSM#040 Status Information Availability**

2672 Provide, with 95% availability, a secure automated mechanism to allow relying parties to
2673 determine credential status and authenticate the subject's identity.

2674 **AL3_CM_CSM#050 Inactive Credentials**

2675 Disable any credential that has not been successfully authenticated during a period of 12
2676 months.

2677

2678 **3.7.4.4 Assurance Level 4**

2679 **3.7.4.4.1 Status Maintenance**

2680 An enterprise and its specified service must:

2681 **AL4_CM_CSM#010 Maintain Status Record**

2682 Maintain a record of the status of all credentials issued.

2683 **AL4_CM_CSM#020 Validation of Status Change Requests**

2684 Authenticate all requestors seeking to have a change of status recorded and published and
2685 validate the requested change before considering processing the request. Such validation
2686 should include:

- 2687 a) the requesting source as one from which the specified service expects to receive
2688 such requests;
2689 b) if the request is not for a new status, the credential or identity as being one for
2690 which a status is already held.

2691 **AL4_CM_CSM#030 Revision to Published Status**

2692 Process authenticated requests for revised status information and have the revised
2693 information available for access within a period of 72 hours.

- 2694 **AL4_CM_CSM#040** **Status Information Availability**
- 2695 Provide, with 95% availability, a secure automated mechanism to allow relying parties to
2696 determine credential status and authenticate the subject's identity.
- 2697 **AL4_CM_CSM#050** **Inactive Credentials**
- 2698 Disable any credential that has not been successfully authenticated during a period of 12
2699 months.
- 2700 **3.7.5 Part E--Credential Validation/Authentication**
- 2701 These criteria apply to credential validation and identity authentication.
- 2702 **3.7.5.1 Assurance Level 1**
- 2703 **3.7.5.1.1 Assertion Security**
- 2704 An enterprise and its specified service must:
- 2705 **AL1_CM_ASS#010** **Validation and Assertion Security**
- 2706 Provide validation of credentials to a relying party using a protocol that:
- 2707 a) requires authentication of the specified service or of the validation source;
- 2708 b) ensures the integrity of the authentication assertion.
- 2709 **AL1_CM_ASS#020** **No Post Authentication**
- 2710 *Not* authenticate credentials that have been revoked.
- 2711 **AL1_CM_ASS#030** **Proof of Possession**
- 2712 Use an authentication protocol that requires the claimant to prove possession and control
2713 of the authentication token.
- 2714 **AL1_CM_ASS#040** **Assertion Lifetime**
- 2715 No stipulation.
- 2716
- 2717 **3.7.5.2 Assurance Level 2**
- 2718 **3.7.5.2.1 Assertion Security**
- 2719 An enterprise and its specified service must:

2720 **AL2_CM_ASS#010 Validation and Assertion Security**

2721 Provide validation of credentials to a relying party using a protocol that:

- 2722 a) requires authentication of the specified service, itself, or of the validation source;
2723 b) ensures the integrity of the authentication assertion.

2724 **AL2_CM_ASS#020 No Post Authentication**

2725 *Not* authenticate credentials that have been revoked.

2726 **AL2_CM_ASS#030 Proof of Possession**

2727 Use an authentication protocol that requires the claimant to prove possession and control
2728 of the authentication token.

2729 **AL2_CM_ASS#040 Assertion Lifetime**

2730 Generate assertions so as to indicate and effect their expiration 12 hours after their
2731 creation.

2732

2733 **3.7.5.3 Assurance Level 3**

2734 **3.7.5.3.1 Assertion Security**

2735 An enterprise and its specified service must:

2736 **AL3_CM_ASS#010 Validation and Assertion Security**

2737 Provide validation of credentials to a relying party using a protocol that:

- 2738 a) requires authentication of the specified service, itself, or of the validation source;
2739 b) ensures the integrity of the authentication assertion.

2740 **AL3_CM_ASS#020 No Post Authentication**

2741 *Not* authenticate credentials that have been revoked.

2742 **AL3_CM_ASS#030 Proof of Possession**

2743 Use an authentication protocol that requires the claimant to prove possession and control
2744 of the authentication token.

2745 **AL3_CM_ASS#040 Assertion Lifetime**

2746 For non-cryptographic credentials, generate assertions that indicate and effect their
2747 expiration 12 hours after their creation; otherwise, notify the relying party of how often
2748 the revocation status sources are updated.

2749

2750 **3.7.5.4 Assurance Level 4**

2751 **3.7.5.4.1 Assertion Security**

2752 An enterprise and its specified service must:

2753 **AL4_CM_ASS#010 Validation and Assertion Security**

2754 Provide validation of credentials to a relying party using a protocol that:

- 2755 a) requires authentication of the specified service, itself, or of the validation source;
2756 b) ensures the integrity of the authentication assertion.

2757 **AL4_CM_ASS#020 No Post Authentication**

2758 *Not* authenticate credentials that have been revoked.

2759 **AL4_CM_ASS#030 Proof of Possession**

2760 Use an authentication protocol that requires the claimant to prove possession and control
2761 of the authentication token.

2762 **AL4_CM_ASS#040 Assertion Lifetime**

2763 Notify the relying party of how often the revocation status sources are updated.

2764

2765 **3.7.6 Compliance Tables**

2766 Use the following tables to correlate criteria and evidence offered/compliance achieved.
2767 A table is provided for each assurance level. The tables are linked to their respective
2768 criteria and vice-versa, to aid referencing between them. Service providers preparing for
2769 an assessment can use the table appropriate to the level at which they are seeking
2770 approval to correlate evidence with criteria or to justify non-applicability of criteria (e.g.,
2771 specific service types not offered): Assessors can use the tables to record the steps they
2772 take in their assessment and their determination of compliance or failure.

2773

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	Token uniqueness	
Part C – Credential Revocation		
AL1_ID_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	

2774

2775

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	Token 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	Confirm subject's details	
Part C – Credential Revocation		
AL2_CM_RVP#010	Revocation procedures	
AL2_CM_RVP#020	Secure status notification	

AL2_CM_RVP#030	Revocation publication	
AL2_ID_RVP#040	Verify revocation identity	
AL2_ID_RVP#050	Revocation Records	
AL2_ID_RVP#060	Record Retention	
AL2_ID_RVR#010	Verify revocation identity	
AL2_ID_RVR#020	Revocation reason	
AL2_ID_RVR#030	Verify Subscriber as Revocant	
AL2_ID_RVR#040	ETSP as Revocant	
AL2_ID_RVR#050	Verify Legal Representative as Revocant	
AL2_ID_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	

2776

2777

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	Token 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	Confirm subject's details	
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_ID_RVP#040	Verify revocation identity	
AL3_ID_RVP#050	Revocation Records	
AL3_ID_RVP#060	Record Retention	
AL3_ID_RVR#010	Verify revocation identity	
AL3_ID_RVR#020	Revocation reason	
AL3_ID_RVR#030	Verify Subscriber as Revocant	
AL3_ID_RVR#040	ETSP as Revocant	
AL3_ID_RVR#050	Verify Legal Representative as Revocant	
AL3_ID_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	

2778

2779

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	Token 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	Confirm subject's details	
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_ID_RVP#050	Revocation Records	
AL4_ID_RVP#060	Record Retention	
AL4_ID_RVR#010	Verify revocation identity	
AL4_ID_RVR#020	Revocation reason	
AL4_ID_RVR#030	Verify Subscriber as Revocant	
AL4_ID_RVR#040	Verify ETSP as Revocant	
AL4_ID_RVR#050	Verify Legal Representative as Revocant	
AL4_CM_RKY#010	Verify Requestor as Subscriber	
AL4_ID_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	

2780

2781 **4 Accreditation and Certification Rules**

2782 **4.1 Assessor Accreditation**

2783 IAEG certified services can be offered only by a CSP who is IAEG-certified. IAEG
2784 certification will be granted by a Federation Operator based on an assessment provided
2785 by an IAEG-accredited assessor. Assessor accreditation requires the following steps.

- 2786 1. An assessor submits an application for accreditation.
- 2787 2. The IAEG evaluates the application according to the criteria set for accreditation.
- 2788 3. The applicant is notified of the IAEG decision.
- 2789 4. In the event of a negative decision, the applicant is offered an appeal.

2790 **4.1.1 Criteria for Assessor Accreditation**

2791 The Board of Directors or any committee or other entity the Board may empower by
2792 delegation (the Board) may choose to recognize the accreditation of another body in lieu
2793 of its own accreditation or as a supplement to its own accreditation. The Board shall
2794 apply the following criteria when determining whether to approve the application of an
2795 assessor for accreditation.

2796 **4.1.1.1 Expertise With Relevant Standards**

2797 Prior to accreditation, the assessor must demonstrate expertise in the application of at
2798 least one of the following evaluation standards. In addition, the assessor must
2799 demonstrate competence in the application of any supplemental evaluation criteria
2800 formally identified by the IAEG and against which CSPs are to be assessed for
2801 certification by Federation Operators and other trust providers.

2802 **4.1.1.2 Business Expertise**

2803 The assessor must:

- 2804 • have been in existence for more than 1 month;
- 2805 • be financially solvent and stable and reasonably certain to remain so for the
2806 foreseeable future;
- 2807 • have sufficient financial resources, either through direct reserves, insurance, or
2808 otherwise, to absorb the cost resulting from wrongful certification of a CSP upon
2809 its recommendation for the period of such certification and for 1 year thereafter;
- 2810 • demonstrate excellence, breadth, and depth in the relevant fields of endeavor,
2811 including electronic authentication, federated identity management, information
2812 security, and the processes and methods of assessment of such fields;

- 2813 • *not* have any key personnel or personnel directly involved in assessments or
2814 development and delivery of assessment reports and recommendations to the
2815 IAEG who have been convicted of a crime.

2816 **4.1.2 Assessment**

2817 Prior to accreditation, assessors may be subject to an on-site evaluation by the IAEG or a
2818 designee. This assessment is to determine compliance with the current IAEG criteria for
2819 accreditation and to evaluate expertise, processes and equipment necessary to conduct the
2820 assessment of CSPs according to IAEG certification criteria and rules. Whether an on-
2821 site inspection is scheduled or not, the assessor shall provide information as provided for
2822 in Section 4.1.1.1 and Section 4.1.1.2.

2823 **4.1.3 Accreditation Decision and Appeal**

2824 Within a reasonable time and at the discretion of the IAEG, the IAEG shall make a
2825 determination of accreditation and communicate that determination to the applicant.

2826 In the event of a negative decision, the assessor may request an appeal of the
2827 accreditation decision by the IAEG. Such request shall be considered by a three-member
2828 panel of the IAEG Board of Directors or any committee or other entity the Board may
2829 empower by delegation, composed of people who have been uninvolved with the decision
2830 and are impartial.

2831 **4.1.4 Maintaining Accreditation**

2832 After the initial year of accreditation, assessors may be subject to an on-site or remote
2833 surveillance evaluation. The surveillance assessment shall include review of at least the
2834 following:

- 2835 • Internal audit reports.
- 2836 • Minutes of management review meetings.
- 2837 • Results of certification assessments, if any.
- 2838 • Any changes in key personnel, facilities and/or major test equipment.
- 2839 • Information on any other significant changes in the quality system of the assessor.

2840 The IAEG, or a designee, may conduct an on-site reassessment or surveillance assessment
2841 of accredited assessors at a minimum of once every 2 years, for verification of continued
2842 compliance with IAEG accreditation criteria and rules.

2843 **4.2 Certification of Credential Service Provider Offerings**

2844 Only a CSP whose product or line of business is currently IAEG certified can issue or
2845 otherwise purvey certified credentials or validation of IAEG certified credentials under an
2846 IAEG brand or IAEG business rules or for use within the IAEG system.

2847 **4.2.1 Process of Certification**

2848 The process of certification for each product or line of business for which certification is
2849 sought by a CSP includes the following steps.

- 2850 1. A CSP seeking certification for a product or line of business begins the formal
2851 process by reviewing the list of IAEG accredited and approved assessors. The
2852 CSP selects an assessor for commencing formal assessment, for which there shall
2853 be a separate contractual arrangement between the applicant and the chosen
2854 assessor.
- 2855 2. The IAEG accredited assessor selected by the applicant conducts an assessment of
2856 the CSP product or line of business. At the conclusion of the assessment process,
2857 the assessor and the CSP separately submit their respective materials upon request
2858 by Federation Operators.
- 2859 3. The assessor submits the assessment report and its recommendation regarding
2860 certification upon request to Federation Operators.
- 2861 4. The CSP submits an application for certification to the Federation Operator,
2862 including agreement to the IAEG business rules, as well as specification of each
2863 line of offerings for which certification is sought, and the assurance level (AL) at
2864 which each certification is sought.
- 2865 5. After receiving the assessment and application materials from the assessor and
2866 CSP, respectively, the Federation Operator evaluates the relevant information and
2867 makes a decision on certification.
- 2868 6. The requestor communicates its decision on certification to the CSP, the assessor
2869 and the IAEG.
- 2870 7. In the event of a negative decision, the CSP is afforded an appeal.
- 2871 8. In the event of a positive decision, the CSP's certified product or line of business
2872 is added to the IAEG Certified CSP offering list.

2873 **4.2.1.1 Application**

2874 The IAEG shall provide a standard application form for certification by Federation
2875 Operators as an IAEG-certified CSP both on the IAEG web site and in paper form. The
2876 application, to be completed by the CSP and submitted to the Federation Operator, shall
2877 include contact information; an agreement to abide by the IAEG rules and any other
2878 applicable IAEG requirements identified in the application, such as a license agreement

2879 or other terms and conditions; and an IAEG appeal request form to request review of the
2880 final certification determination. In addition, the application shall require the applicant to
2881 specify the precise scope of each line of business for which certification is sought, the AL
2882 at which each certification is sought, and any existing applicable accreditation,
2883 certification or similar approvals granted to each specified line of business.

2884 **4.2.1.2 Initial Evaluation**

2885 Upon receipt of an application for certification, the Federation Operator shall review the
2886 contents and the assessment report.

2887 **4.2.1.3 Assessment**

2888 Prior to submitting an application for certification, CSPs must obtain an assessment by an
2889 IAEG accredited assessor. The assessment shall determine compliance with the current
2890 IAEG Service Assessment Criteria.

2891 An IAEG accredited assessor will conduct an on-site reassessment or surveillance
2892 assessment of a CSP at least 1 year after certification and, at a minimum, once every 2
2893 years thereafter, for verification of continued compliance with IAEG certification
2894 requirements.

2895 **4.2.2 Criteria for Certification of CSP Line of Business**

2896 **4.2.2.1 Standard Evaluation Criteria Used by Assessor**

2897 For each line of business for which certification is sought, the practices, operations,
2898 organization, personnel and other relevant aspects of a CSP must be assessed against one
2899 of the following evaluation standards:

2900

2901 **Table 4-1. Evaluation Standards for Different Assurance Levels**

Assurance Level	Evaluation Standard
1	Password CAP AL1
2	Password and Certificate CAP AL2
3	Certificate CAP AL3
4	Certificate CAP AL4

2902

2903 When multiple offerings share one or more assessment criteria, the criteria need only be
2904 considered once per assessment. Such criteria may include management organization,
2905 physical security, or personnel who are common to each line of business for which
2906 certification is sought. In addition, criteria that have been previously assessed positively
2907 by an adequate assessor and assessment process and that are equivalent to IAEG criteria
2908 may be relied upon for purposes of an IAEG assessment. Whether such criteria are
2909 deemed adequate and equivalent must be decided by the IAEG Board. Such

2910 determination by the Board may be triggered by a request by a previously assessed
2911 applicant CSP, an accredited assessor or on the initiative of the Board itself. Such
2912 determinations may be published from time to time as assessment guidance by the IAEG.

2913 **4.2.2.2 Supplemental Criteria Used by Assessor**

2914 The criteria applied by assessors are identified in the IAEG Service Assessment Criteria
2915 (Section 3).

2916 **4.2.3 Certification Decision**

2917 **4.2.3.1 Assessor Delivers Report and Recommendation**

2918 Upon conclusion of the assessment, for each line of business for which certification has
2919 been sought, the assessor shall deliver to the Federation Operator a final assessment
2920 report, including a recommendation on whether to certify the assessed CSP.

2921 **4.2.3.2 Federation Operator Makes Certification Decision**

2922 Upon receipt of each assessment report and recommendation on certification from the
2923 accredited assessor, the Federation Operator shall determine within a reasonable time
2924 whether to deny certification to the CSP, certify the CSP, or take such other action as may
2925 be appropriate, including requesting further information, contractual agreements, or
2926 provable action from the CSP by a certain date.

2927 The decision of the Federation Operator shall be communicated to both the CSP and the
2928 assessor within a reasonable time, to be set by the IAEG Board. The assessor will then
2929 communicate the decision to the IAEG.

2930 **4.2.4 Appeals Process**

2931 Upon receipt of the decision on certification by a participating Federation Operator, a
2932 CSP may request an appeal of that decision. Upon receiving the Appeal Request from a
2933 CSP and within a reasonable period of time, to be set by the IAEG Board, the IAEG shall
2934 appoint a three-member review panel from among IAEG Board of Directors or any
2935 committee or other entity the Board may empower by delegation, comprised of people
2936 who have been uninvolved with the decision at issue and are impartial. Said panel shall
2937 consider the request and make a final determination. The panel may make its
2938 determination based solely upon the information presented in the appeal request,
2939 including any attachments, or it may request additional information from one or more
2940 parties or schedule a hearing to permit the affected parties to further clarify and present
2941 their positions.

2942 **4.2.5 Maintaining Certification**

2943 The CSP must notify the assessor, the Federation Operator and the IAEG of any material
2944 change that may lower the assurance level of the certified product or line of business 60
2945 days before the change is performed or immediately upon the incidence of any unplanned
2946 change. The IAEG, in consultation with the assessor, will determine whether the changes
2947 are sufficient to require re-assessment. The re-assessment, if required, need only cover
2948 those elements that have changed.

2949

2950 **4.3 Process for Handling Non-Compliance**

2951 The process for handling non-compliance applies both to accredited assessors and to
2952 certified CSPs, unless otherwise noted, and is outlined in Sec. 5 – Business Rules.

2953

2954 **4.4 Acceptable Public Statements Regarding IAEG**
2955 **Accreditation and Certification**

2956 It is acceptable for a party to indicate that it is an "IAEG Accredited Assessor" or an
2957 "IAEG Certified Credential Service Provider" for any period during which such statement
2958 is true. However, no party may make any public claim, whether to media outlets, in bids
2959 and other proposals, in marketing materials or otherwise, regarding its status as an
2960 applicant for accreditation or certification, nor can it claim that it is in the process of
2961 achieving such status.

2962 **5 Business Rules**

2963 **5.1 Scope**

2964 Signatories to these business rules agree that these rules govern the use and validation of
2965 Liberty Alliance IAEG certified credentials, the certification of such credentials and the
2966 accreditation of those who assess issuers of such credentials. These business rules are
2967 intended to cover use of credentials for purposes of authentication and not specifically for
2968 the application of a legal signature, which may be subject to other rules depending upon
2969 the parties and transactions involved. The IAEG will employ a phased approach to
2970 establishing business rules and assessment criteria for identity trust service providers,
2971 starting with credential service providers, then rolling out to include federations.

2972 The IAEG will provide a framework of assessment criteria as a guideline for the
2973 certification of credentials issued by a CSP. The IAEG is responsible for the accreditation
2974 of assessors who evaluate CSPs for purposes of IAEG certification of credentials.

2975 Federations and/or Federation Operators will utilize the assessors' evaluations to provide
2976 certification statements with respect to the individual CSPs. A certification statement
2977 made by a federation or federation operator regarding a CSP's compliance with IAEG
2978 certification criteria may be accepted by other federations in consideration of that CSP.

2979 The foregoing does not prohibit use of an IAEG credential under a different brand,
2980 certification, or set of rules, provided that the credential is clearly being used as a non-
2981 IAEG credential.

2982 Claimants are not direct signatories to these business rules. Claimants may have
2983 contracts with each CSP issuing an IAEG credential to the claimant. The claimant can be
2984 a person, the electronic agent of a person, or any legal entity, including a corporation.
2985 Any issues or conflicts arising from use of IAEG-certified credentials will be directed to
2986 the Federation Operator for resolution.

2987 **5.2 Participation**

2988 Before becoming eligible to become a participant in these rules, a CSP must successfully
2989 complete an assessment by an IAEG-accredited assessor and be awarded IAEG
2990 certification for one or more lines of credentials issued by that CSP. A relying party may
2991 become bound by these business rules by agreeing to accept and rely on credentials
2992 issued by one or more IAEG-certified CSPs. A CSP need not be a member of the IAEG
2993 non-profit corporation in order to become certified to these business rules.

2994 **5.3 Roles and Obligations**

2995 **5.3.1 IAEG**

2996 **5.3.1.1 Promulgation and Amendment of Business Rules and Other Documents**

2997 The IAEG shall formalize and may periodically amend these business rules. The IAEG
2998 shall also formalize and may periodically amend a set of documents governing the
2999 accreditation of assessors of IAEG CSPs and the certification criteria of IAEG
3000 credentials. The IAEG reserves the right, at its discretion, to formalize and periodically
3001 amend such other materials, including policies or guidelines, participation agreements,
3002 handbooks or other documents relevant to the IAEG. Notice of all amendments shall be
3003 given by IAEG by electronic mail to the contact person(s) identified by each signatory for
3004 such purpose and by posting to the IAEG web site. All amendments shall be effective as
3005 of the date specified in such notice. If a signatory objects in writing to an amendment
3006 within 30 days after notice of the amendment is given by IAEG, such objection shall be
3007 deemed to be a notice of termination of such signatory's participation in IAEG under
3008 Section 5.2.

3009 **5.3.1.2 Assessor Accreditation and CSP Certification Requirements**

3010 The IAEG is responsible for accreditation of assessors in the IAEG System. The IAEG
3011 shall formalize and may periodically amend requirements for certification of credentials
3012 issued by a CSP and the accreditation of assessors of CSPs.

3013 **5.3.1.3 IAEG Providers List**

3014 The IAEG will maintain and update as needed a list of current accredited assessors and
3015 IAEG-certified CSPs. To the extent allowable, the IAEG will publish this list as a service
3016 to the industry.

3017 **5.3.1.4 Contact Information**

3018 Current contact information for the IAEG can be found at <http://www.projectliberty.org>.

3019 **5.3.2 CSP Obligations**

3020 **5.3.2.1 CSP Certification**

3021 A CSP is obliged to obtain certification of one or more lines of credentials as a
3022 prerequisite for participation in the IAEG System. Certification of CSPs will be
3023 determined by federations and/or Federation Operators based on their review of an
3024 assessment report provided by an IAEG-accredited assessor upon request.

3025 **5.3.2.2 CSP Participation**

3026 A CSP is obliged to abide by the criteria set forth in this document in order to achieve and
3027 maintain IAEG certification status.

3028 **5.3.2.3 Continued Compliance with Certification Requirements**

3029 Each approved and certified CSP must comply with all certification requirements during
3030 the period of time for which credentials issued by the CSP are certified.

3031 **5.3.2.4 Use of IAEG Trademark**

3032 A CSP may not use or display the IAEG or Liberty Alliance trademark in association with
3033 the issuance, validation or other servicing of an IAEG credential or otherwise use or
3034 display the IAEG or Liberty trademark on or associated with any service, product,
3035 literature or other information unless such use has been approved by the IAEG and/or
3036 Liberty Alliance and the trademark is used in accordance with the applicable agreement
3037 with the IAEG.

3038 **5.3.2.5 Records of IAEG Related Disputes**

3039 A CSP is required to investigate any complaint raised to the CSP from a relying party
3040 regarding an IAEG credential. The CSP is also required to keep auditable records of its
3041 investigation and decisions regarding any complaint.

3042 **5.3.2.6 Validation**

3043 Each CSP must make available a method of validation for each IAEG credential it issues
3044 or is otherwise responsible for validating. Such method must be accessible and reliable.

3045 **5.3.2.7 Privacy Practices**

3046 Each CSP must be able to verify that it is complying with applicable privacy practices, as
3047 stated in Section [5.3.5.4](#) of these business rules.

3048 **5.3.2.8 Relying Party Agreements**

3049 It is advised that each approved CSP shall have in place an agreement governing the
3050 rights and obligations between it and any relying party using, validating or otherwise
3051 relying upon IAEG-certified credentials issued by that CSP. As an example, such
3052 agreement may include a clause for conflict resolution upon which the Federation
3053 Operator can rely in the event a conflict arises. Such agreement may contain such
3054 additional terms as the parties may agree to.

3055 **5.3.3 Relying Party Obligations**

3056 **5.3.3.1 Relying Party Agreements**

3057 It is advised that a relying party have in place an agreement with a CSP governing the
3058 practices as well as the rights and obligations between it and the CSP providing the
3059 IAEG-certified credential. A relying party may also have in place an agreement that
3060 governs these practices directly with a federation and/or Federation Operator.

3061 **5.3.3.2 Reasonable Reliance and Level of Assurance**

3062 A relying party is expected through its normal course of business to determine for, itself,
3063 the appropriate level of assurance of the IAEG credential needed for a particular
3064 application, transaction or other session. A relying party is expected to establish that a
3065 credential is in fact issued by an IAEG-certified CSP in order for the relying party's
3066 reliance upon the asserted identity of the claimant to be deemed reasonable under these
3067 business rules. A relying party is expected to successfully validate an IAEG credential in
3068 order for its reliance upon the asserted identity of the claimant to be deemed reasonable
3069 under these business rules. Any use by or validation of an IAEG credential by a party
3070 that has not entered into an agreement with the CSP that issued the credential shall be at
3071 the sole risk of that party, for which the CSP shall have no liability whatsoever.

Comment [ERC1]: Are these more appropriately guidelines for relying parties?

3072 **5.3.3.3 Use of IAEG Trademark**

3073 A relying party may not use or display the IAEG or Liberty Alliance trademark in
3074 association with the acceptance, validation or other use of an IAEG credential or
3075 otherwise use or display the IAEG or Liberty trademark on or associated with any
3076 service, product, literature or other information unless such use has been approved by the
3077 IAEG and/or Liberty Alliance.

3078 **5.3.4 Assessor Obligations**

3079 **5.3.4.1 Assessor Accreditation**

3080 An assessor is not eligible for approval by the IAEG to conduct an assessment for
3081 purposes of IAEG certification of a CSP or otherwise participate as an assessor in the
3082 IAEG System unless that assessor has been and remains accredited by the IAEG.

3083 **5.3.4.2 Assessor Agreement**

3084 An assessor is obliged to execute an IAEG assessor agreement as a prerequisite to being
3085 approved by the IAEG.

3086 **5.3.4.3 Continued Compliance with Accreditation Requirements**

3087 In accordance with the requirements of the IAEG accreditation and certification rules and
3088 any applicable service assessment criteria, approved and accredited assessors must
3089 remain in compliance with all accreditation requirements for the period of time for which
3090 they are accredited.

3091 **5.3.4.4 Use of IAEG Trademark**

3092 An assessor may not use or display the IAEG or Liberty Alliance trademark in association
3093 with an assessment or otherwise use or display the IAEG or Liberty trademark on or
3094 associated with any service, product, literature or other information unless such use has
3095 been approved by the IAEG and/or Liberty Alliance and the trademark is used in
3096 accordance with the applicable agreement with the IAEG.

3097 **5.3.5 General Obligations**

3098 **5.3.5.1 Record Keeping**

3099 Every signatory wishing to avail itself of IAEG resolution of disputes under the terms of
3100 these business rules is obliged to keep records sufficient to preserve evidence of the facts
3101 related to a particular dispute.

3102 **5.3.5.2 System Security and Reliability**

3103 Every signatory agrees to safeguard the security and reliability of the IAEG System.
3104 Specifically, every signatory agrees that the IAEG reserves the right to suspend use of the
3105 IAEG System, in whole or in part, and the participation of any party or parties to the
3106 system without notice and at the sole discretion of the IAEG to protect the integrity and
3107 efficacy of the IAEG System or the rights or property of any party. Agreement to access,
3108 use or rely upon the IAEG System is subject to such terms and conditions as the IAEG
3109 may provide in these business rules, related participation agreements or otherwise.

3110 **5.3.5.3 Third Party Processors**

3111 Any IAEG-certified or -accredited party that is participating in these rules and uses a
3112 third-party processor to perform any processing, transactions or other obligations related
3113 to participation in the IAEG System either must take full responsibility for assuring that
3114 actions of the third-party processor are in compliance with all applicable terms of these
3115 business rules or assure that the third party, itself, becomes a direct signatory of these
3116 business rules.

3117 **5.3.5.4 Claimant Privacy**

3118 Every participant in these business rules must assure that each claimant for which the
3119 participating organization collects or otherwise uses personally identifiable information
3120 has granted informed consent with regard to the sharing of any personally identifiable
3121 information about the claimant by the participant with any other party, whether such
3122 information is contained in a credential, other identity assertion or otherwise. The
3123 informed consent of the individual must be obtained before personally identifiable
3124 information is used for enrollment, authentication or any subsequent uses. Claimants
3125 must be provided with a clear statement about the collection and use of personally
3126 identifiable information upon which to make informed decisions. Participants must
3127 collect only the information necessary to complete the intended authentication function.

3128 Informed consent, for the purposes of this section, is an agreement made by a claimant
3129 with the legal capacity to do so who is so situated as to be able to exercise free power of
3130 choice without the intervention of any element of force, fraud, deceit, duress, over-
3131 reaching, or other form of constraint or coercion and who is given sufficient information
3132 about the subject matter and elements of the transaction involved as to enable him or her
3133 to make an informed and enlightened decision.

3134 Nothing in these business rules shall be construed to authorize or permit the sharing of
3135 any personally identifiable information about an end user other than the information
3136 contained in a certificate or other identity assertion. Such information can be shared only
3137 with an approved relying party to whom the end user has presented credentials or
3138 attempted to access services with an identity assertion operating under the IAEG. If any
3139 other personally identifiable information about a claimant is shared with any party
3140 operating within the IAEG System or any other party, the required consent terms listed in
3141 this section of these business rules must be affirmatively assented to by the claimant.

3142 **5.4 Enforcement and Recourse**

3143 **5.4.1 Breach of Accreditation or Certification Requirements**

3144 **5.4.1.1 Compliance Determination**

3145 Upon receipt by the IAEG of credible information that any IAEG-certified or -accredited
3146 party is not in compliance with the requirements for accreditation or certification, the
3147 IAEG Board or staff or a committee at Board discretion shall make a determination on
3148 whether the party is in fact in material non-compliance with IAEG requirements and shall
3149 communicate the determination to the affected parties. The Board of Directors shall
3150 establish further criteria, as needed, detailing conduct or circumstances constituting
3151 material non-compliance with IAEG rules or standards.

3152 Upon receipt of credible information that a CSP is not in compliance with the
3153 requirements for certification, a Federation Operator may make the determination on
3154 whether the CSP is in fact in material non-compliance with IAEG requirements and shall
3155 communicate the determination to affected parties.

3156 **5.4.1.2 Period to Cure**

3157 An IAEG-certified or -accredited party found to be in material non-compliance shall be
3158 afforded an opportunity and period of time to remedy that material non-compliance,
3159 provided such period does not unduly jeopardize the integrity of the IAEG System or the
3160 rights or property of another party.

3161 **5.4.2 Monetary Recourse**

3162 A CSP may be liable solely under the terms of an existing agreement with a relying party
3163 for losses suffered by the relying party where the cause is attributable to conduct by the
3164 CSP that was carried out in material non-compliance with these business rules or with
3165 certification requirements. Conflict resolution will be directed to the appropriate
3166 Federation Operator.

3167 A CSP may offer credentials at a band of monetary recourse set independently from levels
3168 of assurance. A CSP shall disclose the monetary recourse it will or will not make

3169 available with respect to IAEG credentials and any applicable terms or limitations
3170 governing the recourse according to Table 5-1.

3171

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

3172

3173 **5.4.2.1 Safe Harbors**

3174 **5.4.2.1.1 Losses Arising From Authorization or Unreasonable Reliance**

3175 In no event shall liability or other recourse specified herein be triggered by unreasonable
3176 reliance on a credential by a relying party or by losses resulting from authorization errors
3177 that have not been caused by errors in authentication of identity of a claimant by means
3178 of an IAEG credential.

3179 **5.4.2.1.2 Conduct in Accordance with Business Rules**

3180 Under these business rules, an approved CSP is not liable for losses suffered by a relying
3181 party where the cause is attributable to conduct by the CSP that was carried out in
3182 accordance with these business rules.

3183 **5.4.2.2 Request for Monetary Recourse**

3184 All requests for monetary recourse and the dispositions of all requests must be directed to
3185 the appropriate Federation Operator or trust provider by each relying party and CSP
3186 involved.

3187 **5.4.2.3 Reporting to the IAEG**

3188 All disputes and monetary requests involving IAEG-certified CSPs will be reported to the
3189 IAEG by the Federation Operator or identity trust provider involved.

3190 **5.4.3 Administrative Recourse**

3191 Based on review of all available data and in light of all relevant circumstances, the IAEG
3192 Board of Directors may take administrative recourse against any participant determined
3193 to be in material non-compliance with these business rules, to include, as needed, any of
3194 the following remedies.

3195 **5.4.3.1 Warning**

3196 The non-complying party may be given a warning. The warning may be confidential or
3197 may be publicized within the IAEG or publicized more broadly, at the discretion of the
3198 IAEG Board of Directors.

3199 **5.4.3.2 Credential Revocation**

3200 The non-complying party may be required to revoke one or more IAEG credentials.

3201 **5.4.3.3 Non-compliance Fees**

3202 The non-complying party may be subject to a schedule of fees, to be specified by the
3203 IAEG Board of Directors. The fees may increase according to the length of time before
3204 the party comes back into compliance.

3205 **5.4.3.4 Suspension**

3206 The non-complying party may have its participation in the IAEG System suspended,
3207 including the suspension of accreditation or certification, pending coming back into
3208 compliance.

3209 **5.4.3.5 Termination**

3210 The non-complying party may have its participation in the IAEG System terminated,
3211 including the termination of accreditation or certification.

3212 **5.5 General Terms**

3213 **5.5.1 Governing Law**

3214 These business rules and any related materials governing the IAEG shall be construed
3215 and adjudicated according to the laws of the state of Delaware, U.S.A.

3216 **5.5.2 Disclaimer**

3217 No signatory may disclaim the warranty of merchantability and fitness for a particular
3218 purpose with respect to the provision of any service or product to any other signatory
3219 under these business rules.

3220 **5.5.3 Assignment and Succession**

3221 No signatory may sell, rent, lease, sublicense, assign, grant a security interest in or
3222 otherwise transfer any right and/or obligation contained in these business rules or the
3223 participation agreement executed by that signatory without the express written consent of
3224 the IAEG.

3225 **5.5.4 Hold Harmless**

3226 All signatories to these business rules agree to hold the IAEG harmless for any losses or
3227 other liability arising out of or in relation to the issuance, use, acceptance, validation, or
3228 other reliance upon an IAEG credential or otherwise arising out of or in relation to
3229 participation in the IAEG System or other conduct subject to these business rules.

3230 **5.5.5 Severability**

3231 If any provision, set of provisions or part of a provision of these business rules is held to
3232 be unenforceable or otherwise invalid in whole or in part, the remaining provisions shall
3233 remain in full force and effect and shall be construed to the maximum extent practicable
3234 as a consistent and reasonable entire agreement.

3235 **5.6 Interpretation**

3236 The terms of these business rules shall be interpreted by the IAEG so as to avoid conflict
3237 or inconsistencies between the various provisions and between these business rules,
3238 applicable participation agreements and other relevant IAEG materials.

3239 6 IAEG Glossary

- 3240 *Accreditation.* The process used to achieve formal recognition that an organization has
3241 agreed to the IAEG operating rules and is competent to perform assessments using
3242 the Service Assessment Criteria.
- 3243 *AL.* See *assurance level*
- 3244 *Applicant.* An individual or person acting as a proxy for a machine or corporate entity
3245 who is the subject of an identity proofing process.
- 3246 *Approval.* The process by which the IAEG Board accepts the compliance of a certified
3247 service and the ETSP responsible for that service commits to upholding the IAEG
3248 Rules.
- 3249 *Approved encryption.* Any cryptographic algorithm or method specified in a FIPS or a
3250 NIST recommendation, or encryption method of equivalent rigor. Refer to
3251 <http://csrc.nist.gov/cryptval/>
- 3252 *Approved service.* A certified service which has been granted an approval by the IAEG
3253 Board.
- 3254 *Assertion.* A statement from a verifier to a relying party that contains identity or other
3255 information about a subscriber.
- 3256 *Assessment.* A process used to evaluate an electronic trust service and the service
3257 provider using the requirements specified by one or more Service Assessment
3258 Criteria for compliance with all applicable requirements.
- 3259 *Assessor.* A person or corporate entity who performs an assessment.
- 3260 *Assurance level (AL).* A degree of certainty that a claimant has presented a credential
3261 that refers to the claimant's identity. Each assurance level expresses a degree of
3262 confidence in the process used to establish the identity of the individual to whom
3263 the credential was issued and a degree of confidence that the individual who uses
3264 the credential is the individual to whom the credential was issued. The four
3265 assurance levels are:
- 3266 Level 1: Little or no confidence in the asserted identity's validity
3267 Level 2: Some confidence in the asserted identity's validity
3268 Level 3: High confidence in the asserted identity's validity
3269 Level 4: Very high confidence in the asserted identity's validity
- 3270 *Attack.* An attempt to obtain a subscriber's token or to fool a verifier into believing that
3271 an unauthorized individual possesses a claimant's token.
- 3272 *Attribute.* A property associated with an individual.
- 3273 *Authentication.* Authentication simply establishes identity, not what that identity is
3274 authorized to do or what access privileges he or she has.

- 3275 *Authentication protocol.* A well-specified message exchange process that verifies
3276 possession of a token to remotely authenticate a claimant. Some authentication
3277 protocols also generate cryptographic keys that are used to protect an entire
3278 session, so that the data transferred in the session is cryptographically protected.
- 3279 *Authorization.* Process of deciding what an individual ought to be allowed to do.
- 3280 *Bit.* A binary digit: 0 or 1
- 3281 *Brand.* See IAEG Branded Credential.
- 3282 *CAP:* Credential Assessment Profile
- 3283 *Certification.* The IAEG's affirmation that a particular credential service provider can
3284 provide a particular credential service at a particular assurance level.
- 3285 *Claimant.* A party whose identity is to be verified.
- 3286 *Certification Body.* An organization which has been deemed competent to perform
3287 assessments of a particular type. Such assessments may be formal evaluations or
3288 testing and be based upon some defined set of standards or other criteria.
- 3289 *Certified service.* An electronic trust service which has been assessed by an IAEG-
3290 recognized certification body and found to be compliant with the applicable
3291 SACs.
- 3292 *Credential.* An object to be verified when presented in an authentication transaction. A
3293 credential can be bound in some way to the individual to whom it was issued, or it
3294 can be a bearer credential. Electronic credentials are digital documents that bind
3295 an identity or an attribute to a subscriber's token.
- 3296 *Credential management.* A service that supports the lifecycle of identity credentials from
3297 issuance to revocation, including renewal, status checks and authentication
3298 services.
- 3299 *Credential service.* A type of electronic trust service that supports the verification of
3300 identities (identity proofing), the issuance of identity related
3301 assertions/credentials/tokens, and the subsequent management of those credentials
3302 (for example, renewal, revocation and the provision of related status and
3303 authentication services).
- 3304 *Credential service provider (CSP)* . An electronic trust service provider that operates one
3305 or more credential services. A CSP can include a Registration Authority.
- 3306 *Credential service.* A reliable, efficient means of disseminating credential information.
- 3307 *CSP.* See *credential service provider*.
- 3308 *Cryptographic token.* A token for which the secret is a cryptographic key.
- 3309 *IAEG.* See *Identity Assurance Expert Group*

- 3310 *IAEG assessor*. An organization that has agreed to the IAEG Rules and that has been
3311 accredited to conduct assessments of credential service providers.
- 3312 *IAEG-branded credential*. Information indicating the individual identity of a natural
3313 person, according to a CSP certified by the IAEG to issue, process, validate or
3314 otherwise purvey such credential.
- 3315 *IAEG credential service provider*. Organization that has agreed to the IAEG Operating
3316 Rules and other applicable Rules, and that has been Certified to issue, process,
3317 validate, etc., an IAEG branded credential.
- 3318 *IAEG-recognized assessor*. A body that has been granted an accreditation to perform
3319 assessments against Service Assessment Criteria, at the specified assurance
3320 level(s).
- 3321 *IAEG-recognized certification body*. A certification body which has been accredited by,
3322 or whose qualifications have been otherwise established by, a scheme which the
3323 IAEG Board has deemed to be appropriate for the purposes of determining an
3324 ETSP's competence to perform assessments against IAEG's criteria.
- 3325 *Identity Assurance Expert Group (IAEG)*. The multi-industry Liberty Alliance
3326 partnership working on enabling interoperability among public and private
3327 electronic identity authentication systems.
- 3328 *Electronic credentials*. Digital documents used in authentication that bind an identity or
3329 an attribute to a subscriber's token.
- 3330 *Electronic Trust service (ETS)*. A service that enhances trust and confidence in electronic
3331 transactions, typically but not necessarily using cryptographic techniques or
3332 involving confidential material such as PINs and passwords.
- 3333 *Electronic Trust service provider (ETSP)*. An entity that provides one or more electronic
3334 trust services.
- 3335 *ETS*. See electronic trust service.
- 3336 *ETSP*. See electronic trust service provider,
- 3337 *Federated identity management*. A system that allows individuals to use the same user
3338 name, password, or other personal identification to sign on to the networks of
3339 more than one enterprise in order to conduct transactions.
- 3340 *Federal Information Processing Standards ([FIPS])*. Standards and guidelines issued by
3341 the National Institute of Standards and Technology (NIST) for use government-
3342 wide in the United States. NIST develops FIPS when the U.S. Federal government
3343 has compelling requirements, such as for security and interoperability, for which
3344 no industry standards or solutions are acceptable.
- 3345 *FIPS*. See Federal Information Processing Standards.
- 3346 *Identification*. Process of using claimed or observed attributes of an individual to infer
3347 who the individual is.

- 3348 *Identifier.* Something that points to an individual, such as a name, a serial number, or
3349 some other pointer to the party being identified.
- 3350 *Identity authentication.* Process of establishing an understood level of confidence that an
3351 identifier refers to an identity. It may or may not be possible to link the
3352 authenticated identity to an individual.
- 3353 *Identity.* A unique name for single person. Because a person's legal name is not
3354 necessarily unique, identity must include enough additional information (for
3355 example, an address or some unique identifier such as an employee or account
3356 number) to make a unique name.
- 3357 *Identity binding.* The extent to which an electronic credential can be trusted to be a proxy
3358 for the entity named in it.
- 3359 *Identity Proofing.* The process by which identity related information is validated so as to
3360 identify a person with a degree of uniqueness and certitude sufficient for the
3361 purposes for which that identity is to be used.
- 3362 *Identity Proofing policy.* A set of rules that defines identity proofing requirements
3363 (required evidence, format, manner of presentation, validation), records actions
3364 required of the registrar, and describes any other salient aspects of the identity
3365 proofing function that are applicable to a particular community or class of
3366 applications with common security requirements. An identity proofing policy is
3367 designed to accomplish a stated assurance level.
- 3368 *Identity Proofing service provider.* An electronic trust service provider which offers, as a
3369 standalone service, the specific electronic trust service of identity proofing. This
3370 service provider is sometimes referred to as a Registration Agent/Authority (RA).
- 3371 *Identity Proofing practice statement.* A statement of the practices that an identity
3372 proofing service provider employs in providing its services in accordance with the
3373 applicable identity proofing policy.
- 3374 *Issuer.* Somebody or something that supplies or distributes something officially.
- 3375 *Level of assurance.* See assurance level.
- 3376 *Network.* An open communications medium, typically, the Internet, that is used to
3377 transport messages between the claimant and other parties.
- 3378 *OID.* Object identifier.
- 3379 *Password.* A shared secret character string used in authentication protocols. In many
3380 cases the claimant is expected to memorize the password.
- 3381 *Practice statement.* A formal statement of the practices followed by an authentication
3382 entity (e.g., RA, CSP, or verifier) that typically defines the specific steps taken to
3383 register and verify identities, issue credentials and authenticate claimants.

- 3384 *Public key.* The public part of the asymmetric key pair that is typically used to verify
3385 signatures or encrypt data.
- 3386 *Public key infrastructure (PKI)* . A set of technical and procedural measures used to
3387 manage public keys embedded in digital certificates. The keys in such certificates
3388 can be used to safeguard communication and data exchange over potentially
3389 unsecure networks.
- 3390 *Registration.* An entry in a register, or somebody or something whose name or
3391 designation is entered in a register.
- 3392 *Relying party.* An entity that relies upon a subscriber's credentials, typically to process a
3393 transaction or grant access to information or a system.
- 3394 *Role.* The usual or expected function of somebody or something, or the part somebody or
3395 something plays in a particular action or event.
- 3396 *SAC.* See Service Assessment Criteria.
- 3397 *Security.* A collection of safeguards that ensures the confidentiality of information,
3398 protects the integrity of information, ensures the availability of information,
3399 accounts for use of the system, and protects the system(s) and/or network(s) used
3400 to process the information.
- 3401 *Service Assessment Criteria (SAC).* A set of requirements levied upon specific
3402 organizational and other functions performed by electronic trust services and
3403 service providers. Services and service providers must comply with all applicable
3404 criteria to qualify for IAEG approval.
- 3405 *Signatory.* A party that opts into and agrees to be bound by the IAEG Rules according to
3406 the specified procedures.
- 3407 *Specified service.* The electronic trust service which, for the purposes of an IAEG
3408 assessment, is the subject of criteria set out in a particular SAC, or in an
3409 application for assessment, in a grant of an approval or other similar usage as may
3410 be found in various IAEG documentation.
- 3411 *Subject.* An entity that is able to use an electronic trust service subject to agreement with
3412 an associated subscriber. A subject and a subscriber can be the same entity.
- 3413 *Subscriber.* A party that has entered into an agreement to use an electronic trust service.
3414 A subscriber and a subject can be the same entity.
- 3415 *Threat.* An adversary that is motivated and capable to violate the security of a target and
3416 has the capability to mount attacks that will exploit the target's vulnerabilities.
- 3417 *Token.* Something that a claimant possesses and controls (typically a key or password)
3418 that is used to authenticate the claimant's identity.
- 3419 *Assurance framework.* The body of work that collectively defines the industry-led self-
3420 regulatory framework for electronic trust services in the United States and around

3421 the globe, as operated by the IAEG. The assurance framework includes
3422 descriptions of criteria, rules, procedures, processes, and other documents.
3423 *Verification.* Establishment of the truth or correctness of something by investigation of
3424 evidence.

3425 **7 Publication Acknowledgements**

3426 The IAEG would like to thank the following working group chairs and vice chairs for
3427 their commitment and dedication to the Liberty Identity Assurance Framework.

3428

3429 IAEG Co-Chair: Jane Hennessey, Wells Fargo

3430 IAEG Co-Chair: Michael Sessa, PESC

3431

3432 Interim Chair: James Lewis, The Center for Strategic and International Studies

3433 Interim Vice Chair: David Temoshok, U.S. General Services Administration

3434

3435 Business Requirements and Processes Work Group

3436 Chair: Linda G. Elliot, PingID Network

3437 Vice Chair: Thomas Greco, beTRUSTed

3438

3439 Credential Services Assessment Criteria and Levels of Assurance Work Group

3440 Chair: Robert J. Schlecht, Mortgage Bankers Association of America

3441 Vice Chair: Von Harrison, U.S. General Services Administration

3442

3443 Credential Services Assessment Criteria Sub Work

3444 Chair: Nancy Black, HollenGroup

3445 Vice Chair: Richard Wilsher, The Zygma Partnership

3446

3447 Levels of Assurance Sub Work Group

3448 Chair: Peter Alterman, National Institutes of Health

3449 Vice Chair: Noel Nazario, KPMG LLP

3450

3451 Interoperability Sub Work Group

3452 Chair: William E. Burr, National Institute of Standards and Technology

3453 Vice Chair: Kurt Van Etten, eBay, Inc.

3454

3455 Evaluation, Accreditation and Compliance Work Group

3456 Chair: Gary Glickman, Giesecke & Devrient Cardtech, Inc.

3457 Vice Chair: Cornelia Chebinou, National Association of State Auditors, Comptrollers
3458 and Treasurers

3459

3460 EAP Governance Work Group

3461 Chair: Paula Arcioni, State of New Jersey, Office of Information Technology

3462 Vice Chair: Roger J. Cochetti, CompTIA

3463

3464 Consultants

3465 Russ Cutler, Confiance Advisors, LLC

3466 Yuriy Dzambasow, A&N Associates, Inc.
3467 Nathan Faut, KPMG
3468 Dan Greenwood, Commonwealth of Massachusetts
3469 Rebecca Nielsen, Booz Allen Hamilton
3470 Richard Wilsher, The Zygma Partnership
3471
3472 Members of the various work groups include:
3473 Khaja Ahmed, Microsoft Corporation
3474 Michael A. Aisenberg, VeriSign, Inc.
3475 Peter Alterman, National Institutes of Health
3476 Paula Arcioni, State of New Jersey, Office of Information Technology
3477 Jonathan Askins, ACXIOM Corporation
3478 Asaf Awan, Parkweb Associates
3479 Stefano Baroni, SETECS
3480 Paul Barrett, Real User Corporation
3481 Nancy Black, Hollen Group
3482 Debb Blanchard, Enspier Technologies/GDT
3483 Warren Blosjo, 3Factor
3484 Daniel Blum, Burton Group
3485 Iana Bohmer, Northrop Grumman Information Technology
3486 Christine Borucke, Electronic Data Systems
3487 Kirk Brafford, SSP-Litronic, Inc.
3488 Mayi Canales, M Squared Strategies, Inc.
3489 Richard Carter, American Association of Motor Vehicles Administration
3490 Kim Cartwright, Experian
3491 James A. Casey, NeuStar, Inc.
3492 Ray Cavanaugh, Entegrity Solutions
3493 Chuck Chamberlain, U.S. Postal Service
3494 Cornelia Chebinou, National Association of State Auditors, Comptrollers and Treasurers
3495 Rebecca Chisolm, Sun Microsystems Federal
3496 Roger J. Cochetti, CompTIA
3497 Dan Combs, Global Identity Solutions
3498 John Cornell, U.S. General Services Administration
3499 Sarah Currier, CheckFree Corporation
3500 Chris Daly, IBM Corporation
3501 Peter Davis, Neustar
3502 Kathy DiMaggio, Sigaba Corporation
3503 Yuriy Dzambasow, A&N Associates, Inc.
3504 Josh Elliott, American Management Systems
3505 Clay Epstein, Indentrus LLC
3506 Irving R. Gilson, Department of Defense
3507 Gary Glickman, Giesecke & Devrient Cardtech, Inc.
3508 James A. Gross, Wells Fargo

3509 Kirk R. Hall, GeoTrust
3510 Von Harrison, U.S. General Services Administration
3511 Christopher Hankin, Sun Microsystems, Inc.
3512 Michael Horkey, Global Identity Solutions
3513 Katherine M. Hollis, Electronic Data Systems
3514 Robert Housel, National City Corporation
3515 Burt Kaliski, RSA Security, Inc.
3516 Shannon Kellog, RSA Security, Inc.
3517 James Kobielus, Burton Group
3518 Patrick Lally, SSP-Litronic, Inc.
3519 Steve Lazerowich, Enspier Technologies/GDT
3520 Phillip S. Lee, SC Solutions, Inc.
3521 Peter Lieberwirth, Authentidate
3522 Rob Lockhart, IEEE-ISTO
3523 Chris Loudon, Enspier Technologies/GDT
3524 J. Scott Lowry, Enspier Technologies/GDT
3525 Lena Kannappan, FuGen Solutions
3526 Paul Madsen, NTT
3527 Adele Marsh, PA Higher Education Assistance Agency
3528 Patty McCarty, Private ID Systems
3529 Doug McCoy, SAFLINK Corporation
3530 Ben Miller, InsideID
3531 Larry Miller, Identrus LLC
3532 Sead Muftic, SETECS
3533 Noel Nazario, KPMG LLP
3534 Michael R. Nelson, IBM Corporation
3535 Simon Nicholson, Sun Microsystems, Inc.
3536 Pete Palmer, HIMSS NHII Task Force Advisor, Guidant Corporation
3537 Stephen Permison, Standards Based Programs
3538 Bob Pinheiro, Independent Security Researcher, Bob Pinheiro Consulting
3539 Alex Popowycz, Fidelity Investments
3540 Hemma Prafullchandra, FuGen Solutions
3541 Stephen L. Ranzini, University Bank
3542 Christiane Reinhold, BearingPoint
3543 Donald E. Rhodes, American Banker Association
3544 Jason Roualt, HP
3545 Randy V. Sabett, Cooley Woodward, LLP
3546 Ravi Sandhu, NSD Security
3547 Dean Sarff, Minerals Management Service
3548 Donald Saxinger, FDIC
3549 Robert J. Schlecht, Mortgage Bankers Association of America
3550 Howard Schmidt, eBay, Inc.
3551 Ari Schwartz, Center for Democracy and Technology

3552 John Shipley, The Shipley Group
3553 Stephen P. Sill, U.S. General Services Administration
3554 Helena G. Sims, NACHA – The Electronic Payments Association
3555 Bill Smith, Sun Microsystems, Inc.
3556 Tadgh Smith, IBM
3557 Judith Spencer, U.S. General Services Administration
3558 William Still, ChoicePoint Public Sector
3559 Michael M. Talley, University Bancorp
3560 David Temoshok, U.S. General Services Administration
3561 Richard Thayer, ComTech, Inc.
3562 John Ticer, NeuStar, Inc.
3563 Kevin Trilli, VeriSign, Inc.
3564 Matthew Tuttle, beTRUSTed
3565 A. Jerald Varner, U.S. General Services Administration
3566 Martin Wargon, Wave Systems Corporation
3567 Richard Wilsher, The Zygma Partnership
3568 | David Weitzel, Mitretek Systems, Inc.
3569 Michael Wolf, Authentidate
3570 Gordon R. Woodrow, ClearTran, Inc.
3571 Steve Worona, EDUCAUSE
3572 David Wasley, Int2

Formatted: German (Germany)

3573 8 References

- 3574 [BSI7799-2] "BS 7799-2:2002 Information security management. Specification with
3575 guidance for use," BSI Group (September 05, 2002). [http://www.bsi-](http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=00000000030049529)
3576 [global.com/en/Shop/Publication-Detail/?pid=00000000030049529](http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=00000000030049529)
- 3577
- 3578 [CAF] Louden, Chris, Spenser, Judy, Burr, Bill, Hawkins, Kevin, Temoshok, David,
3579 Cornell, John, Wilsher, Richard G., Timchak, Steve, Sill, Stephen, Silver, Dave, Harrison,
3580 Von, eds., "E-Authentication Credential Assessment Framework (CAF)," E-
3581 Authentication Initiative, Version 2.0.0 (March 16, 2005).
3582 <http://www.cio.gov/eauthentication/documents/CAF.pdf>
- 3583
- 3584 [EAP CSAC 04011] "EAP working paper: Identity Proofing Service Assessment Criteria
3585 (ID-SAC)," Electronic Authentication Partnership, Draft 0.1.3 (July 20, 2004)
3586 http://eap.projectliberty.org/docs/Jul2004/EAP_CSAC_04011_0-1-3_ID-SAC.doc
- 3587
- 3588 [EAPTrustFramework] "Electronic Authentication Partnership Trust Framework"
3589 Electronic Authentication Partnership, Version 1.0. (January 6, 2005)
3590 http://eap.projectliberty.org/docs/Trust_Framework_010605_final.pdf
- 3591
- 3592 [FIPS] "Federal Information Processing Standards Publications" Federal Information
3593 Processing Standards. <http://www.itl.nist.gov/fipspubs/>
- 3594
- 3595 [FIPS140-2] "Security Requirements for Cryptographic Modules" Federal Information
3596 Processing Standards. (May 25, 2001) [http://csrc.nist.gov/publications/fips/fips140-](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)
3597 [2/fips1402.pdf](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)
- 3598
- 3599 [ISO/IEC17799] "ISO/IEC 17799:2005 Information technology -- Security techniques --
3600 Code of practice for information security management" International Organization for
3601 Standardization.
3602 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39612
- 3603
- 3604 [M-04-04] Bolton, Joshua B., eds., "E-Authentication Guidance for Federal Agencies,"
3605 Office of Management and Budget, (December 16, 2003).
3606 <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>
- 3607

3608 [NIST800-63] Burr, William E., Dodson, Donna F., Polk, W. Timothy, eds., "Electronic
3609 Authentication Guideline: : Recommendations of the National Institute of Standards and
3610 Technology," Version 1.0.2, National Institute of Standards and Technology, (April,
3611 2006). http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
3612
3613 [RFC 3647] Chokhani, S., Ford, W., Sabett, R., Merrill, C., Wu, S., eds., "Internet X.509
3614 Public Key Infrastructure Certificate Policy and Certification Practices Framework," The
3615 Internet Engineering Task Force (November, 2003). <http://www.ietf.org/rfc/rfc3647.txt>
3616