

1

2

3

4



5

6

7

## 8 **Liberty Identity Assurance Framework**

9 **Version:** 1.0

10 **Editor:**

11 Russ Cutler, Confinance 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	<b>Contents</b>	
70		
71	<b>1 Introduction .....</b>	<b>5</b>
72	<b>2 Assurance Levels .....</b>	<b>6</b>
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	<b>3 Service Assessment Criteria .....</b>	<b>10</b>
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 .....	74
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	<b>4 Accreditation and Certification Rules .....</b>	<b>97</b>
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.....	101
114	4.3	Process for Handling Non-Compliance .....	102
115	4.3.1	Compliance Determination .....	102
116	4.3.2	Period to Cure .....	102
117	4.3.3	Administrative Recourse.....	102
118	4.4	Acceptable Public Statements Regarding IAEG Accreditation and Certification ....	
119		.....	103
120	<b>5</b>	<b>Business Rules.....</b>	<b>104</b>
121	5.1	Scope.....	104
122	5.2	Participation .....	104
123	5.3	Roles and Obligations .....	105
124	5.3.1	IAEG .....	105
125	5.3.2	CSP Obligations.....	105
126	5.3.3	Relying Party Obligations.....	106
127	5.3.4	Assessor Obligations.....	107
128	5.3.5	General Obligations .....	108
129	5.4	Enforcement and Recourse .....	109
130	5.4.1	Breach of Accreditation or Certification Requirements .....	109
131	5.4.2	Monetary Recourse .....	109
132	5.4.3	Administrative Recourse.....	110
133	5.5	General Terms .....	111
134	5.5.1	Governing Law .....	111
135	5.5.2	Disclaimer .....	111
136	5.5.3	Assignment and Succession.....	111
137	5.5.4	Hold Harmless .....	112
138	5.5.5	Severability .....	112
139	5.6	Interpretation.....	112
140	<b>6</b>	<b>IAEG Glossary.....</b>	<b>113</b>
141	<b>7</b>	<b>Publication Acknowledgements .....</b>	<b>119</b>
142	<b>8</b>	<b>References .....</b>	<b>123</b>
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

<b>Table 2-1. Four Assurance Levels</b>	
<b>Level</b>	<b>Description</b>
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

<b>Table 2-2 Potential Impact at Each Assurance Level</b>				
<b>Potential Impact of Authentication Errors</b>	<b>Assurance Level*</b>			
	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>
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 Assurance Framework. These  
305 criteria set out the requirements for services and their providers at all assurance levels  
306 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

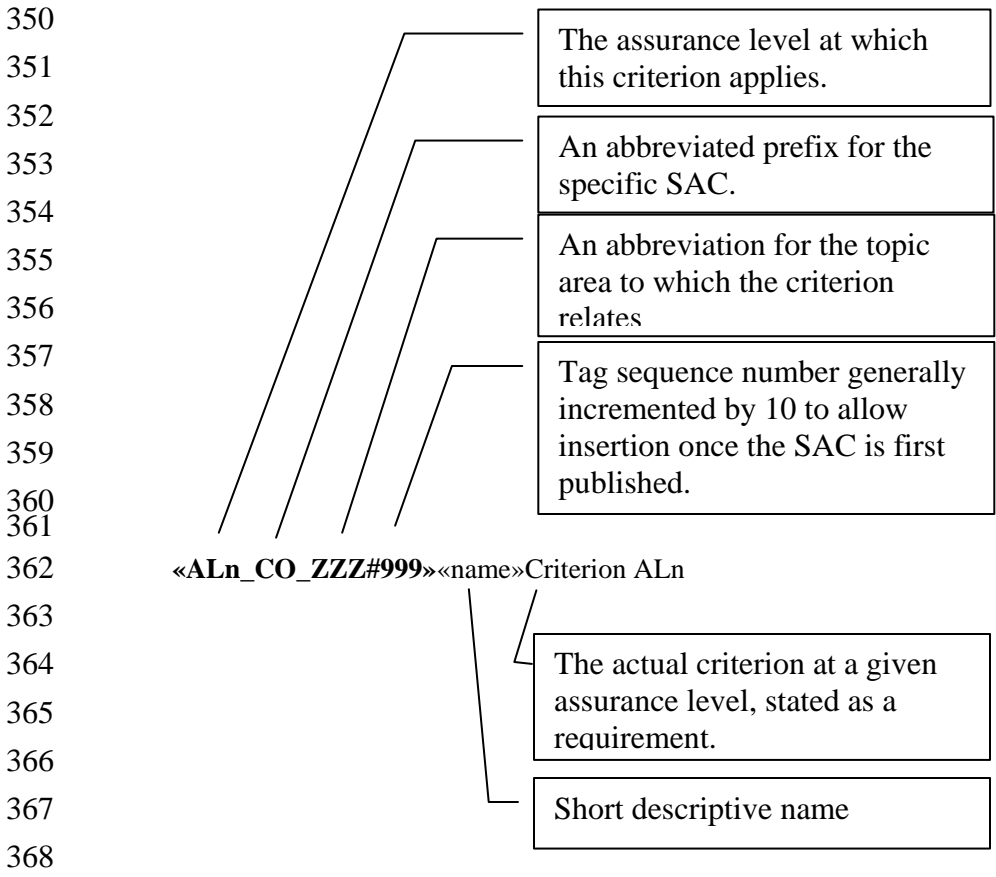
339 All special terms used in this description are defined in the IAEG Glossary.

### 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.

382 An enterprise and its specified service must:

##### 383 **AL1\_CO\_ESM#010          Established enterprise**

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

##### 386 **AL1\_CO\_ESM#020          Established service**

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

##### 389 **AL1\_CO\_ESM#030          Legal compliance**

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

393

#### 394 **3.5.1.2 Notices and User information**

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

397 An enterprise and its specified service must:

398 **AL1\_CO\_NUI#010**                    **General Service Definition**

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

402 **AL1\_CO\_NUI#030**                    **Due notification**

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

406 **AL1\_CO\_NUI#040**                    **User Agreement**

407 Through a user agreement:

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

413 **3.5.1.3**    **Information Security Management**

414 No stipulation.

415 **3.5.1.4**    **Secure Communications**

416 **AL1\_CO\_SCO#020**                    **Protection of secrets**

417 Ensure that:

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

424 **3.5.2**    **Assurance Level 2**

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

427 **3.5.2.1**    **Enterprise and Service Maturity**

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

430 An enterprise and its specified service must:

431 **AL2\_CO\_ESM#010**      **Established enterprise**

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

434 **AL2\_CO\_ESM#020**      **Established service**

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

437 **AL2\_CO\_ESM#030**      **Legal compliance**

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

441 **AL2\_CO\_ESM#040**      **Financial Provisions**

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

445 **AL2\_CO\_ESM#050**      **Data Retention and Protection**

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

451

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

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

456 An enterprise and its specified service must:

457 **AL2\_CO\_NUI#010**      **General Service Definition**

458 Make available to the intended user community a service definition for its specified  
459 service that includes any specific uses or limitations on its use, all applicable Terms,

460 Conditions, Fees, and Privacy Policy for the service, including any limitations of its usage  
461 and definitions of any terms having specific intention or interpretation. Specific  
462 provisions are stated in further criteria in this section.

463 **AL2\_CO\_NUI#020 Service Definition sections**

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

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

483 **AL2\_CO\_NUI#030 Due notification**

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

489 **AL2\_CO\_NUI#050 Subscriber Information**

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

492 **AL2\_CO\_NUI#060 Subscriber Agreement**

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

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

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

500 **AL2\_CO\_NUI#080** **Helpdesk facility**

501 Ensure that its help desk is available for any queries related to the specified service  
502 during the regular business hours of its primary operational location, minimally from 9  
503 AM to 5 PM, Monday through Friday, excepting Federal holidays.

504

505 **3.5.2.3 Information Security Management**

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

509 An enterprise and its specified service must:

510 **AL2\_CO\_ISM#010** **Documented policies and procedures**

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

515 **AL2\_CO\_ISM#020** **Policy Management and Responsibility**

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

520 **AL2\_CO\_ISM#030** **Risk Management**

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

523 **AL2\_CO\_ISM#040** **Continuity of Operations Plan**

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



526 **AL2\_CO\_ISM#050 Configuration Management**

527 Demonstrate a configuration management system that at least includes:

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

531 **AL2\_CO\_ISM#060 Quality Management**

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

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

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

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

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

542 **AL2\_CO\_ISM#090 Independent Audit**

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

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

548 Retain full records of all audits, both internal and independent, for a period that, at a  
549 minimum, fulfills its legal obligations and otherwise for greater periods either as it may  
550 have committed to in its service definition or required by any other obligations it has  
551 with/to a subscriber. Such records must be held securely and protected against loss,  
552 alteration, or destruction.

553 **AL2\_CO\_ISM#110 Termination provisions**

554 Have in place a clear plan for the protection of subscribers' private and secret information  
555 related to their use of the service which must ensure the ongoing secure preservation and  
556 protection of legally required records and for the secure destruction and disposal of any

557 such information whose retention is not legally required. Essential details of this plan  
558 must be published.

559

#### 560 **3.5.2.4 Security-relevant Event (Audit) Records**

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

563 An enterprise and its specified service must:

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

565 Maintain a log of all security-relevant events concerning the operation of the service,  
566 together with a precise record of the time at which the event occurred (time-stamp) [AL4  
567 provided by a trusted time-source], and such records must be retained with appropriate  
568 protection, accounting for service definition, risk management requirements, and  
569 applicable legislation.

570

#### 571 **3.5.2.5 Operational infrastructure**

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

575 An enterprise and its specified service must:

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

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

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

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

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

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

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

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

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

597 Have sufficient staff to operate the specified service according to its policies and  
598 procedures.

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

600 Apply physical access control mechanisms to ensure that access to sensitive areas is  
601 restricted to authorized personnel.

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

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

605

606 **3.5.2.6 External Services and Components**

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

610 An enterprise and its specified service must:

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

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

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

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

623

624 **3.5.2.7**    **Secure Communications**

625 An enterprise and its specified service must:

626 **AL2\_CO\_SCO#010**            **Secure remote communications**

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

633 **AL2\_CO\_SCO#020**            **Protection of secrets**

634 Ensure that:

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

640

641 **3.5.3**    **Assurance Level 3**

642 Achieving AL3 requires meeting all criteria required to achieve AL2. This section  
643 includes only requirements additional to those described in Section [3.5.2](#).

644 **3.5.3.1**    **Enterprise and Service Maturity**

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

647 An enterprise and its specified service must:

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

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

651 **AL3\_CO\_ESM#020**            **Established service**

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

654 **AL3\_CO\_ESM#030**            **Legal compliance**

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

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

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

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

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

668 **AL3\_CO\_ESM#060**            **Ownership**

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

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

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

676

677 **3.5.3.2 Notices and User Information**

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

681 An enterprise and its specified service must:

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

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

688 **AL3\_CO\_NUI#020 Service Definition Sections**

689 Publish a service definition for the specified service containing clauses that provide the  
690 following information:

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

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

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

714 **AL3\_CO\_NUI#050**                    **Subscriber Information**

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

717 **AL3\_CO\_NUI#060**                    **Subscriber Agreement**

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

720 **AL3\_CO\_NUI#070**                    **Change of Subscriber Information**

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

725 **AL3\_CO\_NUI#080**                    **Helpdesk facility**

726 Ensure that its help desk is available for any queries related to the specified service  
727 during the regular business hours of its primary operational location, minimally from 9:00  
728 a.m. through 5:00 p.m., Monday to Friday, inclusive, excepting Federal holidays.

729

730 **3.5.3.3 Information Security Management**

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

735 An enterprise and its specified service must:

736 **AL3\_CO\_ISM#010**                    **Documented policies and procedures**

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

741 **AL3\_CO\_ISM#020**                    **Policy Management and Responsibility**

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

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

746 **AL3\_CO\_ISM#030 Risk Management**

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

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

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

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

755 Demonstrate a configuration management system that at least includes:

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

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

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

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

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

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



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

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

782 **AL3\_CO\_ISM#090 Independent Audit**

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

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

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

793 **AL3\_CO\_ISM#110 Termination provisions**

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

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

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

804

805 **3.5.3.4 Security-Relevant Event (Audit) Records**

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

808 An enterprise and its specified service must:

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

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

813 **3.5.3.5 Operational Infrastructure**

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

817 An enterprise and its specified service must:

818 **AL3\_CO\_OPN#010 Technical security**

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

822 **AL3\_CO\_OPN#020 Defined security roles**

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

828 **AL3\_CO\_OPN#030 Personnel recruitment**

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

834 **AL3\_CO\_OPN#040 Personnel skills**

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

840 **AL3\_CO\_OPN#050 Adequacy of Personnel resources**

841 Have sufficient staff to operate the specified service according to its policies and  
842 procedures.

843 **AL3\_CO\_OPN#060 Physical access control**

844 Apply physical access control mechanisms to ensure access to sensitive areas is restricted  
845 to authorized personnel.

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

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

849

850 **3.5.3.6 External Services and Components**

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

854 An enterprise and its specified service must:

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

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

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

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

867

868 **3.5.3.7 Secure Communications**

869 An enterprise and its specified service must:

870 **AL3\_CO\_SCO#010 Secure remote communications**

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

876 **AL3\_CO\_SCO#020 Protection of secrets**

877 Ensure that:

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

894 **3.5.4 Assurance Level 4**

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

897 **3.5.4.1 Enterprise and Service Maturity**

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

900 An enterprise and its specified service must:

901 **AL4\_CO\_ESM#010 Established enterprise**

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

904 **AL4\_CO\_ESM#020**            **Established service**

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

907 **AL4\_CO\_ESM#030**            **Legal compliance**

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

911 **AL4\_CO\_ESM#040**            **Financial Provisions**

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

915 **AL4\_CO\_ESM#050**            **Data Retention and Protection**

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

921 **AL4\_CO\_ESM#060**            **Ownership**

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

925 **AL4\_CO\_ESM#070**            **Independent Management and Operations**

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

929

930 **3.5.4.2 Notices and User Information/Agreements**

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

934 An enterprise and its specified service must:

935 **AL4\_CO\_NUI#010** **General Service Definition**

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

941 **AL4\_CO\_NUI#020** **Service Definition Sections**

942 Publish a service definition for the specified service containing clauses that provide the  
943 following information:

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

961 **AL4\_CO\_NUI#030** **Due Notification**

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

967 **AL4\_CO\_NUI#050** **Subscriber Information**

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

970 **AL4\_CO\_NUI#060**                    **Subscriber Agreement**

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

973 **AL4\_CO\_NUI#070**                    **Change of Subscriber Information**

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

978 **AL4\_CO\_NUI#080**                    **Helpdesk facility**

979 Ensure that its help desk is available for any queries related to the specified service  
980 during the regular business hours of its primary operational location, minimally from 9:00  
981 a.m. to 5:00 p.m., Monday to Friday, inclusive, excepting Federal holidays.

982

983 **3.5.4.3**    **Information Security Management**

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

988 An enterprise and its specified service must:

989 **AL4\_CO\_ISM#010**                    **Documented policies and procedures**

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

994 **AL4\_CO\_ISM#020**                    **Policy Management and Responsibility**

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

999 **AL4\_CO\_ISM#030 Risk Management**

1000 Demonstrate a risk management methodology that adequately identifies and mitigates  
1001 risks related to the specified service and its user community and must show that on-going  
1002 risk assessment review is conducted as a part of the business' procedures.

1003 **AL4\_CO\_ISM#040 Continuity of Operations Plan**

1004 Have and shall keep updated a continuity of operations plan that covers disaster recovery  
1005 and the resilience of the specified service and must show that on-going review of this  
1006 plan is conducted as a part of the business' procedures.

1007 **AL4\_CO\_ISM#050 Configuration Management**

1008 Demonstrate a configuration management system that at least includes:

- 1009 a) version control for software system components;
- 1010 b) timely identification and installation of all applicable patches for any software  
1011 used in the provisioning of the specified service;
- 1012 c) version control and managed distribution for all documentation associated with  
1013 the specification, management, and operation of the system, covering both  
1014 internal and publicly available materials.

1015 **AL4\_CO\_ISM#060 Quality Management**

1016 Demonstrate a quality management system that is appropriate for the specified service.

1017 **AL4\_CO\_ISM#070 System Installation and Operation Controls**

1018 Apply controls during system development, procurement, installation, and operation that  
1019 protect the security and integrity of the system environment, hardware, software, and  
1020 communications having particular regard to:

- 1021 a) the software and hardware development environments, for customized  
1022 components;
- 1023 b) the procurement process for COTS components;
- 1024 c) contracted consultancy/support services;
- 1025 d) shipment of system components;
- 1026 e) storage of system components;
- 1027 f) installation environment security;
- 1028 g) system configuration;
- 1029 h) transfer to operational status.



1030 **AL4\_CO\_ISM#080 Internal Service Audit**

1031 Unless it can show that by reason of its size or for other arguable operational reason it is  
1032 unreasonable so to perform, be regularly audited for effective provision of the specified  
1033 service by internal audit functions independent of the parts of the enterprise responsible  
1034 for the specified service.

1035 **AL4\_CO\_ISM#090 Independent Audit**

1036 Be audited by an independent auditor at least every 24 months to ensure the  
1037 organization's security-related practices are consistent with the policies and procedures  
1038 for the specified service and the appointed auditor must have appropriate accreditation or  
1039 other acceptable experience and qualification.

1040 **AL4\_CO\_ISM#100 Audit Records**

1041 Retain full records of all audits, both internal and independent, for a period which, as a  
1042 minimum, fulfils its legal obligations and otherwise for greater periods either as it may  
1043 have committed to in its service definition or required by any other obligations it has  
1044 with/to a subscriber. Such records must be held securely and protected against loss,  
1045 alteration, or destruction.

1046 **AL4\_CO\_ISM#110 Termination provisions**

1047 Have in place a clear plan for the protection of subscribers' private and secret information  
1048 related to their use of the service which must ensure the ongoing secure preservation and  
1049 protection of legally-required records and for the secure destruction and disposal of any  
1050 such information whose retention is not legally required. Essential details of this plan  
1051 must be published.

1052 **AL4\_CO\_ISM#120 Best Practice Security Management**

1053 Have in place a certified Information Security Management System (ISMS) that has been  
1054 assessed and found to be in compliance with the code of practice ISO/IEC 17799  
1055 [ISO/IEC17799] through application of practices defined in BS 7799 Part 2 [BSI7799-2]  
1056 and which applies and is appropriate to the ETPS in question. All requirements expressed  
1057 in preceding criteria in this "ISM" section must *inter alia* fall wholly within the scope of  
1058 this ISMS.

1059

1060 **3.5.4.4 Security-Related (Audit) Records**

1061 The criteria in this section are concerned with the need to provide an auditable log of all  
1062 events that are pertinent to the correct and secure operation of the service.

1063 An enterprise and its specified service must:

1064 **AL4\_CO\_SER#010 Security Event Logging**

1065 Maintain a log of all security-relevant events concerning the operation of the service,  
1066 together with a precise record of the time at which the event occurred (time-stamp)  
1067 provided by a trusted time-source and such records must be retained with appropriate  
1068 protection, accounting for service definition, risk management requirements, and  
1069 applicable legislation.

1070

1071 **3.5.4.5 Operational Infrastructure**

1072 The criteria in this section address the infrastructure within which the delivery of the  
1073 specified service takes place. It puts particular emphasis upon the personnel involved,  
1074 and their selection, training, and duties.

1075 An enterprise and its specified service must:

1076 **AL4\_CO\_OPN#010 Technical Security**

1077 Demonstrate that the technical controls employed will provide the level of security  
1078 required by the risk assessment plan and the ISMS, and that these controls are effectively  
1079 integrated with the appropriate procedural and physical security measures.

1080 **AL4\_CO\_OPN#020 Defined Security Roles**

1081 Define, by means of a job description, the roles and responsibilities for every security-  
1082 relevant task, relating it to specific procedures (which shall be set out in the ISMS) and  
1083 other job descriptions. Where the role is security-critical or where special privileges or  
1084 shared duties exist, these must be specifically highlighted, including access privileges  
1085 relating to logical and physical parts of the service's operations.

1086 **AL4\_CO\_OPN#030 Personnel Recruitment**

1087 Demonstrate that it has defined practices for the selection, vetting, and contracting of all  
1088 personnel, both direct employees and those whose services are provided by third parties.  
1089 Full records of all searches and supporting evidence of qualifications and past  
1090 employment must be kept for the duration of the individual's employment plus the longest  
1091 lifespan of any credential issued under the service policy.

1092 **AL4\_CO\_OPN#040 Personnel skills**

1093 Ensure that employees are sufficiently trained, qualified, experienced, and current for the  
1094 roles they fulfill. Such measures must be accomplished either by recruitment practices or

1095 through a specific training program. Where employees are undergoing on-the-job  
1096 training, they must only do so under the guidance of a mentor with established leadership  
1097 skills.

1098 **AL4\_CO\_OPN#050 Adequacy of Personnel resources**

1099 Have sufficient staff to operate the specified service according to its policies and  
1100 procedures.

1101 **AL4\_CO\_OPN#060 Physical access control**

1102 Apply physical access control mechanisms to ensure access to sensitive areas is restricted  
1103 to authorized personnel.

1104 **AL4\_CO\_OPN#070 Logical access control**

1105 Employ logical access control mechanisms to ensure access to sensitive system functions  
1106 and controls is restricted to authorized personnel.

1107

1108 **3.5.4.6 External Services and Components**

1109 This section addresses the relationships and obligations upon contracted parties both to  
1110 apply the policies and procedures of the enterprise and also to be available for assessment  
1111 as critical parts of the overall service provision.

1112 An enterprise and its specified service must:

1113 **AL4\_CO\_ESC#010 Contracted Policies and Procedures**

1114 Where the enterprise uses the services of external suppliers for specific packaged  
1115 components of the service or for resources which are integrated with its own operations  
1116 and under its controls, ensure that those parties are engaged through reliable and  
1117 appropriate contractual arrangements which stipulate critical policies, procedures, and  
1118 practices that the sub-contractor is required to fulfill.

1119 **AL4\_CO\_ESC#020 Visibility of Contracted Parties**

1120 Where the enterprise uses the services of external suppliers for specific packaged  
1121 components of the service or for resources which are integrated with its own operations  
1122 and under its controls, ensure that contractors' compliance with contractually stipulated  
1123 policies and procedures, and thus with the IAEG's assessment criteria, can be proven and  
1124 subsequently monitored.

1125

1126 **3.5.4.7 Secure Communications**

1127 An enterprise and its specified service must:

1128 **AL4\_CO\_SCO#010 Secure remote communications**

1129 If the specific service components are located remotely from and communicate over a  
1130 public or unsecured network with other service components or other ETSP(s) it services,  
1131 the communications must be cryptographically authenticated by an authentication  
1132 protocol that meets, as a minimum, the requirements of AL4 and encrypted using an  
1133 approved encryption method.

1134 **AL4\_CO\_SCO#020 Protection of secrets**

1135 Ensure that:

- 1136 a) access to shared secrets shall be subject to discretionary controls which permit  
1137 access to those roles/applications which need such access;
- 1138 b) stored shared secrets are encrypted such that:
- 1139 i the encryption key for the shared secret file is encrypted under a key held  
1140 in a FIPS 140-2 [FIPS140-2] Level 2 (or higher) validated hardware  
1141 cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic  
1142 module and decrypted only as immediately required for an authentication  
1143 operation.
- 1144 ii they are protected as a key within the boundary of a FIPS 140-2 Level 2  
1145 (or higher) validated hardware cryptographic module or any FIPS 140-2  
1146 Level 3 or 4 cryptographic module and are not exported in plaintext from  
1147 the module.
- 1148 iii they are split by an "*n from m*" cryptographic secret-sharing method.
- 1149 c) any long-term (i.e., not session) shared secrets are revealed only to the subscriber  
1150 and the ETSP's direct agents (bearing in mind (a) above).
- 1151

1152 **3.6 Identity Proofing Service Assessment Criteria**

1153 The Service Assessment Criteria in this section establish the requirements for the  
1154 technical conformity of identity proofing services at all ALs defined in Section 2. These  
1155 criteria apply to a particular kind of electronic trust service (ETS) recognized by the  
1156 IAEG and to the related electronic trust service provider (ETSP)—an identity proofing  
1157 service. (For definitions of terms used in this section, see Section 6). These criteria are  
1158 generally referred to elsewhere within IAEG documentation as ID-SAC [ID-SAC].

1159 These criteria do not address the delivery of a credential to the applicant/subscriber,  
1160 which is dealt with by the Credential Management SAC (CM-SAC), described in Section  
1161 3.7.

1162 These criteria may only be used in an assessment in one of the following circumstances:

1163 • In conjunction with the Common Organizational SAC (CO-SAC), described in  
1164 Section 3.5, for a standalone identity proofing service.

1165 • In combination with one or more other SACs that must include the CO-SAC and  
1166 where the identity proofing functions that these criteria address form part of a  
1167 larger service offering.

1168 Note: Some of the SAC-identifying numbers are not used in all of the ALs. In such cases,  
1169 the particular SAC number has been reserved where not used and skipped.

### 1170 **3.6.1 Assurance Level 1**

#### 1171 **3.6.1.1 Policy**

1172 An enterprise or specified service must:

##### 1173 **AL1\_ID\_POL#010 Unique service identity**

1174 Ensure that a unique identity is attributed to the specific service, such that credentials  
1175 issued by it can be distinguishable from those issued by other services, including services  
1176 operated by the same enterprise.

##### 1177 **AL1\_ID\_POL#020 Unique subject identity**

1178 Ensure that each applicant's identity is unique within the service's community of subjects  
1179 and uniquely associable with tokens and/or credentials issued to that identity.

1180

#### 1181 **3.6.1.2 Identity Verification**

##### 1182 **3.6.1.2.1 In-Person Public Verification**

1183 An enterprise or specified service must:

##### 1184 **AL1\_ID\_IPV#010 Required evidence**

1185 Ensure that the applicant possesses any one of the following forms of evidence:

- 1186 a) one form of Federal or state-issued identity;  
1187 b) one signed bank or credit card;  
1188 c) two utility statements;  
1189 d) any other equivalent form of proof.

##### 1190 **AL1\_ID\_IPV#020 Evidence checks**

1191 Ensure that the name on the evidence offered bears the name the applicant claims and, in  
1192 addition, establish, according to the form of evidence provided, any one of the following:

- 1193 a) the applicant appears to be the person named;  
1194 b) the applicant can reproduce any signatures shown on bank cards;  
1195 c) addresses provided are consistent;  
1196 d) any other checks that establish an equivalent degree of certitude.  
1197

1198 **3.6.1.2.2 Remote Public Verification**

1199 If the specific service offers remote identity proofing to applicants with whom it has no  
1200 previous relationship, then it must comply with the criteria in this section.

1201 An enterprise or specified service must:

1202 **AL1\_ID\_RPV#010 Required evidence**

1203 Require the applicant to provide a contact telephone number or email address.

1204 **AL1\_ID\_RPV#020 Evidence checks**

1205 Verify the provided information by either:

- 1206 a) confirming the request by calling the number.  
1207 b) successfully sending a confirmatory email and receiving a positive  
1208 acknowledgement.  
1209

1210 **3.6.1.2.3 Secondary Verification**

1211 In each of the above cases, an enterprise or specified service must:

1212 **AL1\_ID\_SCV#010 Secondary checks**

1213 Have in place additional measures (e.g., require additional documentary evidence, delay  
1214 completion while out-of-band checks are undertaken) to deal with any anomalous  
1215 circumstances that can be reasonably anticipated (e.g., a legitimate and recent change of  
1216 address that has yet to be established as the address of record).

1217

1218 **3.6.1.3 Verification Records**

1219 No criteria.

1220 **3.6.2 Assurance Level 2**

1221 **3.6.2.1 Policy**

1222 The specific service must show that it applies identity proofing policies and procedures  
1223 and that it retains appropriate records of identity proofing activities and evidence.

1224 The enterprise or specified service must:

1225 **AL2\_ID\_POL#010 Unique service identity**

1226 Ensure that a unique identity is attributed to the specific service, such that credentials  
1227 issued by it can be distinguishable from those issued by other services, including services  
1228 operated by the same enterprise.

1229 **AL2\_ID\_POL#020 Unique subject identity**

1230 Ensure that each applicant's identity is unique within the service's community of subjects  
1231 and uniquely associable with tokens and/or credentials issued to that identity.

1232 **AL2\_ID\_POL#030 Published Proofing Policy**

1233 Publish the Identity Proofing Policy under which it verifies the identity of applicants<sup>1</sup> in  
1234 form, language, and media accessible to the declared community of users.

1235 **AL2\_ID\_POL#040 Adherence to Proofing Policy**

1236 Perform all identity proofing strictly in accordance with its published Identity Proofing  
1237 Policy, through application of the procedures and processes set out in its Identity Proofing  
1238 Practice Statement.

1239

1240 **3.6.2.2 Identity Verification**

1241 The specific service must offer at least one of the following classes of identity proofing  
1242 service and may offer any additional sets it chooses, subject to the nature and the  
1243 entitlement of the CSP concerned.

1244 **3.6.2.2.1 In-Person Public Verification**

1245 If the specific service offers in-person identity proofing to applicants with whom it has no  
1246 previous relationship, then it must comply with the criteria in this section.

1247 The enterprise or specified service must:

---

<sup>1</sup> For an identity proofing service that is within the management scope of a credential management service provider, this should be the credential management service's definitive policy; for a stand-alone identity proofing service, the policy may be either that of a client who has 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.

1248 **AL2\_ID\_IPV#010** **Required evidence**

1249 Ensure that the applicant is in possession of a primary Government Picture ID document  
1250 that bears a photographic image of the holder.

1251 **AL2\_ID\_IPV#020** **Evidence checks**

1252 Ensure that the presented document:

- 1253 a) appears to be a genuine document properly issued by the claimed issuing  
1254 authority and valid at the time of application;  
1255 b) bears a photographic image of the holder that matches that of the applicant;  
1256 c) states an address at which the applicant can be contacted.  
1257

1258 **3.6.2.2 Remote Public Verification**

1259 If the specific service offers remote identity proofing to applicants with whom it has no  
1260 previous relationship, then it must comply with the criteria in this section.

1261 An enterprise or specified service must:

1262 **AL2\_ID\_RPV#010** **Required evidence**

1263 Ensure that the applicant submits the references of and attests to current possession of a  
1264 primary Government Picture ID document, and provides additional verifiable personal  
1265 information that at a minimum must include:

- 1266 a) a name that matches the referenced photo-ID;  
1267 b) date of birth;  
1268 c) current address or personal telephone number;  
1269 d) the issuer, account number, and expiration date of a current credit card.

1270 Additional information may be requested so as to ensure a unique identity, and alternative  
1271 information may be sought where the enterprise can show that it leads to at least the same  
1272 degree of certitude when verified.

1273 **AL2\_ID\_RPV#020** **Evidence checks**

1274 Electronically verify by a record check against the provided identity references with the  
1275 specified issuing authorities/institutions or through similar databases:

- 1276 a) the existence of such records with matching name and reference numbers;  
1277 b) corroboration of date of birth, current address of record, and other personal  
1278 information sufficient to ensure a unique identity.

1279 Additional checks may be performed so as to establish the uniqueness of the claimed  
1280 identity, and alternative checks may be performed where the enterprise can show that they  
1281 lead to at least the same degree of certitude.



1282

1283 **3.6.2.2.3 Current Relationship Verification**

1284 If the specific service offers identity proofing to applicants with whom it has a current  
1285 relationship, then it must comply with the criteria in this section.

1286 The enterprise or specified service must:

1287 **AL2\_ID\_CRV#010 Required evidence**

1288 Ensure that it has previously exchanged a shared secret (e.g., a PIN or password) that  
1289 meets entropy requirements for the AL with the applicant.

1290 **AL2\_ID\_CRV#020 Evidence checks**

1291 Ensure that it has:

- 1292 a) only issued the shared secret after originally establishing the applicant's identity  
1293 with a degree of rigor equivalent to that required under either the AL2 (or higher)  
1294 requirements for in-person or remote public verification  
1295 b) an ongoing business relationship sufficient to satisfy the enterprise of the  
1296 applicant's continued personal possession of the shared secret.  
1297

1298 **3.6.2.2.4 Affiliation Verification**

1299 If the specific service offers identity proofing to applicants on the basis of some form of  
1300 affiliation, then it must comply with the criteria in this section for the purposes of  
1301 establishing that affiliation, in addition to the previously stated requirements for the  
1302 verification of the individual's identity.

1303 The enterprise or specified service must:

1304 **AL2\_ID\_AFV#010 Required evidence**

1305 Ensure that the applicant possesses:

- 1306 a) identification from the organization with which it is claiming affiliation;  
1307 b) agreement from the organization that the applicant may be issued a credential  
1308 indicating that an affiliation exists.

1309 **AL2\_ID\_AFV#020 Evidence checks**

1310 Ensure that the presented documents:

- 1311 a) each appear to be a genuine document properly issued by the claimed issuing  
1312 authorities and valid at the time of application;  
1313 b) refer to an existing organization with a contact address;

- 1314 c) indicate that the applicant has some form of recognizable affiliation with the  
1315 organization;  
1316 d) appear to grant the applicant an entitlement to obtain a credential indicating its  
1317 affiliation with the organization.  
1318

1319 **3.6.2.2.5 Secondary Verification**

1320 In each of the above cases, the enterprise or specified service must:

1321 **AL2\_ID\_SCV#010 Secondary checks**

1322 Have in place additional measures (e.g., require additional documentary evidence, delay  
1323 completion while out-of-band checks are undertaken) to deal with any anomalous  
1324 circumstances that can be reasonably anticipated (e.g., a legitimate and recent change of  
1325 address that has yet to be established as the address of record).

1326

1327 **3.6.2.3 Verification Records**

1328 The specific service must retain records of the identity proofing (verification) that it  
1329 undertakes.

1330 An enterprise or specified service must:

1331 **AL2\_ID\_VRC#010 Verification Records for Personal Applicants**

1332 Log, taking account of all applicable legislative and policy obligations, a record of the  
1333 facts of the verification process. At a minimum, records of identity information must  
1334 include:

- 1335 a) the applicant's full name as shown on the government-issued ID;  
1336 b) the applicant's date of birth;  
1337 c) the applicant's current address of record;  
1338 d) the subscriber's current telephone or email address of record;  
1339 e) type, issuing authority, and reference number(s) of all documents checked in the  
1340 identity proofing process;  
1341 f) where required, a telephone or email address for related contact and/or delivery of  
1342 credentials/notifications;  
1343 g) any pseudonym used by the applicant in lieu of the verified identity;  
1344 h) date and time of verification.

1345 **AL2\_ID\_VRC#020 Verification Records for Affiliated Applicants**

1346 In addition to the foregoing, log, taking account of all applicable legislative and policy  
1347 obligations, a record of the additional facts of the verification process. At a minimum,  
1348 records of identity information must include:

- 1349 a) the subscriber's full name;  
1350 b) the subscriber's current address of record;  
1351 c) the subscriber's current telephone or email address of record;  
1352 d) the subscriber's acknowledgement for issuing the subject with a credential;  
1353 e) type, issuing authority, and reference number(s) of all documents checked in the  
1354 identity proofing process.

1355 **AL2\_ID\_VRC#030 Record Retention**

1356 Either retain, securely, the record of the verification process for the duration of the  
1357 subscriber account plus 7.5 years, or submit same record to a client CSP that has  
1358 undertaken to retain the record for the requisite period or longer.

1359 **3.6.3 Assurance Level 3**

1360 **3.6.3.1 Policy**

1361 The specific service must show that it applies identity proofing policies and procedures  
1362 and that it retains appropriate records of identity proofing activities and evidence.

1363 The enterprise or specified service must:

1364 **AL3\_ID\_POL#010 Unique service identity**

1365 Ensure that a unique identity is attributed to the specific service, such that credentials  
1366 issued by it can be distinguishable from those issued by other services, including services  
1367 operated by the same enterprise.

1368 **AL3\_ID\_POL#020 Unique subject identity**

1369 Ensure that each applicant's identity is unique within the service's community of subjects  
1370 and uniquely associable with tokens and/or credentials issued to that identity.

1371 **AL3\_ID\_POL#030 Published Proofing Policy**

1372 Publish the Identity Proofing Policy under which it verifies the identity of applicants<sup>2</sup> in  
1373 form, language, and media accessible to the declared community of Users.

---

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

1374 **AL3\_ID\_POL#040 Adherence to Proofing Policy**

1375 Perform all identity proofing strictly in accordance with its published Identity Proofing  
1376 Policy, applying the procedures and processes set out in its Identity Proofing Practice  
1377 Statement.

1378

1379 **3.6.3.2 Identity Verification**

1380 The specific service must offer at least one of the following classes of identity proofing  
1381 services and may offer any additional services it chooses, subject to the nature and the  
1382 entitlement of the CSP concerned.

1383 **3.6.3.2.1 In-Person Public Verification**

1384 A specific service that offers identity proofing to applicants with whom it has no previous  
1385 relationship must comply with the criteria in this section.

1386 The enterprise or specified service must:

1387 **AL3\_ID\_IPV#010 Required evidence**

1388 Ensure that the applicant is in possession of a primary Government Picture ID document  
1389 that bears a photographic image of the holder.

1390 **AL3\_ID\_IPV#020 Evidence checks**

1391 Ensure that the presented document:

- 1392 a) appears to be a genuine document properly issued by the claimed issuing  
1393 authority and valid at the time of application;
- 1394 b) bears a photographic image of the holder that matches that of the applicant;
- 1395 c) states an address at which the applicant can be contacted;
- 1396 d) is electronically verified by a record check with the specified issuing authority or  
1397 through similar databases that:
- 1398 i) establishes the existence of such records with matching name and  
1399 reference numbers;
- 1400 ii) corroborates date of birth, current address of record, and other personal  
1401 information sufficient to ensure a unique identity.
- 1402

1403 **3.6.3.2.2 Remote Public Verification**

1404 A specific service that offers remote identity proofing to applicants with whom it has no  
1405 previous relationship must comply with the criteria in this section.

1406 The enterprise or specified service must:

1407 **AL3\_ID\_RPV#010** **Required evidence**

1408 Ensure that the applicant submits details of and attests to current possession of:

- 1409 a) a primary Government Picture ID document, and either  
1410 i) an account number issued by a regulated financial institution, or  
1411 ii) a source of personal information relating to the applicant.

1412 **AL3\_ID\_RPV#020** **Evidence checks**

1413 Electronically verify by a record check against the provided identity references with the  
1414 specified issuing authorities/institutions or through similar databases:

- 1415 a) the existence of such records with matching name and reference numbers;  
1416 b) corroboration of date of birth, current address of record or personal telephone  
1417 number, and other personal information sufficient to ensure a unique identity;  
1418 c) dynamic verification of personal information previously provided by or likely to  
1419 be known only by the applicant.  
1420

1421 **3.6.3.2.3 Affiliation Verification**

1422 A specific service that offers identity proofing to applicants on the basis of some form of  
1423 affiliation must comply with the criteria in this section to establish that affiliation and  
1424 with the previously stated requirements to verify the individual's identity.

1425 The enterprise or specified service must:

1426 **AL3\_ID\_AFV#010** **Required evidence**

1427 Ensure that the applicant possesses:

- 1428 a) identification from the organization with which it is claiming affiliation;  
1429 b) agreement from the organization that the applicant may be issued a credential  
1430 indicating that an affiliation exists.

1431 **AL3\_ID\_AFV#020** **Evidence checks**

1432 Ensure that the presented documents:

- 1433 a) each appear to be a genuine document properly issued by the claimed issuing  
1434 authorities and valid at the time of application;  
1435 b) refer to an existing organization with a contact address;  
1436 c) indicate that the applicant has some form of recognizable affiliation with the  
1437 organization;  
1438 d) appear to grant the applicant an entitlement to obtain a credential indicating an  
1439 affiliation with the organization.  
1440

1441 **3.6.3.2.4 Secondary Verification**

1442 In each of the above cases, the enterprise or specified service must also meet the  
1443 following criteria:

1444 **AL3\_ID\_SCV#010 Secondary checks**

1445 Have in place additional measures (e.g., require additional documentary evidence, delay  
1446 completion while out-of-band checks are undertaken) to deal with any anomalous  
1447 circumstance that can reasonably be anticipated (e.g., a legitimate and recent change of  
1448 address that has yet to be established as the address of record).

1449 **3.6.3.3 Verification Records**

1450 The specific service must retain records of the identity proofing (verification) that it  
1451 undertakes.

1452 The enterprise or specified service must:

1453 **AL3\_ID\_VRC#010 Verification Records**

1454 Log, taking account of all applicable legislative and policy obligations, a record of the  
1455 facts of the verification process. At a minimum, records of identity information must  
1456 include:

- 1457 a) the applicant's full name as stated on the primary documents;
- 1458 b) the applicant's date and place of birth (as declared, but not necessarily verified);
- 1459 c) the applicant's current address of record;
- 1460 d) the subscriber's current telephone or email address of record;
- 1461 e) type, issuing authority, and reference number(s) of all documents checked in the  
1462 identity proofing process;
- 1463 f) any pseudonym used by the applicant in lieu of the verified identity;
- 1464 g) date and time of verification;
- 1465 h) identity of the registrar;
- 1466 i) identity of the CSP providing the verification service or the location at which the  
1467 (in-house) verification was performed.

1468 **AL3\_ID\_VRC#020 Verification Records for Affiliated Applicants**

1469 In addition to the foregoing, log, taking account of all applicable legislative and policy  
1470 obligations, a record of the additional facts of the verification process. At a minimum,  
1471 records of identity information must include:

- 1472 a) the subscriber's full name;
- 1473 b) the subscriber's current address of record;
- 1474 c) the subscriber's current telephone or email address of record;
- 1475 d) the subscriber's acknowledgement of issuing the subject with a credential;

- 1476 e) type, issuing authority, and reference number(s) of all documents checked in the  
1477 identity proofing process;  
1478 f) where required, a telephone or email address for related contact and/or delivery of  
1479 credentials/notifications.

1480 **AL3\_ID\_VRC#030 Record Retention**

1481 Either retain, securely, the record of the verification/revocation process for the duration of  
1482 the subscriber account plus 7.5 years, or submit the same record to a client CSP that has  
1483 undertaken to retain the record for the requisite period or longer.

1484 **3.6.4 Assurance Level 4**

1485 Identity proofing at Assurance Level 4 requires the physical presence of the applicant in  
1486 front of the registration officer with photo ID or other readily verifiable biometric identity  
1487 information, as well as the requirements set out by the following criteria.

1488 **3.6.4.1 Policy**

1489 The specific service must show that it applies identity proofing policies and procedures  
1490 and that it retains appropriate records of identity proofing activities and evidence.

1491 The enterprise or specified service must:

1492 **AL4\_ID\_POL#010 Unique service identity**

1493 Ensure that a unique identity is attributed to the specific service, such that credentials  
1494 issued by it can be distinguishable from those issued by other services, including services  
1495 operated by the same enterprise.

1496 **AL4\_ID\_POL#020 Unique subject identity**

1497 Ensure that each applicant's identity is unique within the service's community of subjects  
1498 and uniquely associable with tokens and/or credentials issued to that identity.

1499 **AL4\_ID\_POL#030 Published Proofing Policy**

1500 Publish the Identity Proofing Policy under which it verifies the identity of applicants<sup>3</sup> in  
1501 form, language, and media accessible to the declared community of users.

---

<sup>3</sup> For an identity proofing service that is within the management scope of a credential management service provider, this should be the credential management service's definitive policy; for a stand-alone identity proofing service, the policy may be either that of a client which has defined one through contract, the ID service's own policy or a separate policy that explains how the client's policies will be complied with.

1502 **AL4\_ID\_POL#040 Adherence to Proofing Policy**

1503 Perform all identity proofing strictly in accordance with its published Identity Proofing  
1504 Policy, applying the procedures and processes set out in its Identity Proofing Practice  
1505 Statement.

1506

1507 **3.6.4.2 Identity Verification**

1508 The specific service may offer only face-to-face identity proofing service. Remote  
1509 verification is not allowed at this level.

1510 The enterprise or specified service must:

1511 **3.6.4.2.1 In-Person Public Verification**

1512 **AL4\_ID\_IPV#010 Required evidence**

1513 Ensure that the applicant is in possession of:

- 1514 a) a primary Government Picture ID document that bears a photographic image of  
1515 the holder and either  
1516 i) secondary Government Picture ID or an account number issued by a  
1517 regulated financial institution, or  
1518 ii) two items confirming name, and address or telephone number, such as:  
1519 utility bill, professional license or membership, or other evidence of  
1520 equivalent standing.

1521 **AL4\_ID\_IPV#030 Evidence checks – primary ID**

1522 Ensure that the presented document:

- 1523 a) appears to be a genuine document properly issued by the claimed issuing  
1524 authority and valid at the time of application;  
1525 b) bears a photographic image of the holder which matches that of the applicant;  
1526 c) states an address at which the applicant can be contacted;  
1527 d) is electronically verified by a record check with the specified issuing authority or  
1528 through similar databases that:  
1529 i) establishes the existence of such records with matching name and  
1530 reference numbers;  
1531 ii) corroborates date of birth, current address of record, and other personal  
1532 information sufficient to ensure a unique identity.

1533 **AL4\_ID\_IPV#040 Evidence checks – secondary ID**

1534 Ensure that the presented document meets the following conditions:

- 1535 1) If it is secondary Government Picture ID,



- 1536 a) appears to be a genuine document properly issued by the claimed issuing  
1537 authority and valid at the time of application,  
1538 b) bears a photographic image of the holder which matches that of the  
1539 applicant,  
1540 c) states an address at which the applicant can be contacted.  
1541 2) If it is a financial institution account number,  
1542 a) is verified by a record check with the specified issuing authority or  
1543 through similar databases that:  
1544 i) establishes the existence of such records with matching name and  
1545 reference numbers,  
1546 ii) corroborates date of birth, current address of record, and other  
1547 personal information sufficient to ensure a unique identity.  
1548 3) If it is two utility bills or equivalent documents,  
1549 a) each appears to be a genuine document properly issued by the claimed  
1550 issuing authority,  
1551 b) corroborates current address of record or telephone number sufficient to  
1552 ensure a unique identity.

1553 **AL4\_ID\_IPV#050 Applicant knowledge checks**

1554 Where the applicant is unable to satisfy any of the above requirements, that the applicant  
1555 can provide a Social Security Number (SSN) that matches the claimed identity.

1556

1557 **3.6.4.2.2 Affiliation Verification**

1558 A specific service that offers identity proofing to applicants on the basis of some form of  
1559 affiliation must comply with the criteria in this section to establish that affiliation, in  
1560 addition to complying with the previously stated requirements for verifying the  
1561 individual's identity.

1562 The enterprise or specified service must:

1563 **AL4\_ID\_AFV#010 Required evidence**

1564 Ensure that the applicant possesses:

- 1565 a) identification from the organization with which the applicant is claiming  
1566 affiliation;  
1567 b) agreement from the organization that the applicant may be issued a credential  
1568 indicating that an affiliation exists.

1569 **AL4\_ID\_AFV#020 Evidence checks**

1570 Ensure that the presented documents:

- 1571 a) each appear to be a genuine document properly issued by the claimed issuing  
1572 authorities and valid at the time of application;  
1573 b) refer to an existing organization with a contact address;  
1574 c) indicate that the applicant has some form of recognizable affiliation with the  
1575 organization;  
1576 d) appear to grant the applicant an entitlement to obtain a credential indicating an  
1577 affiliation with the organization.  
1578

1579 **3.6.4.2.3 Secondary Verification**

1580 In each of the above cases, the enterprise or specified service must also meet the  
1581 following criteria:

1582 **AL4\_ID\_SCV#010 Secondary checks**

1583 Have in place additional measures (e.g., require additional documentary evidence, delay  
1584 completion while out-of-band checks are undertaken) to deal with any anomalous  
1585 circumstances that can reasonably be anticipated (e.g., a legitimate and recent change of  
1586 address that has yet to be established as the address of record).

1587

1588 **3.6.4.3 Verification Records**

1589 The specific service must retain records of the identity proofing (verification) that it  
1590 undertakes.

1591 The enterprise or specified service must:

1592 **AL4\_ID\_VRC#010 Verification Records for Personal Applicants**

1593 Log, taking account of all applicable legislative and policy obligations, a record of the  
1594 facts of the verification process. At a minimum, records of identity information must  
1595 include:

- 1596 a) the applicant's full name,  
1597 b) the applicant's date and place of birth (as declared, but not necessarily verified),  
1598 c) the applicant's current address of record,  
1599 d) the type, issuing authority, and reference number(s) of all documents checked in  
1600 the identity proofing process,  
1601 e) a telephone or email address for related contact and/or delivery of  
1602 credentials/notifications,  
1603 f) any pseudonym used by the applicant in lieu of the verified identity,  
1604 g) a biometric record of the applicant (e.g., a photograph, fingerprint, voice  
1605 recording),  
1606 h) date and time of verification issued by a trusted time-source,

- 1607 i) the signature of the applicant,
- 1608 j) identity of the registrar,
- 1609 k) identity of the CSP providing the verification service or the location at which the
- 1610 (in-house) verification was performed.

1611 **AL4\_ID\_VRC#020 Verification Records for Affiliated Applicants**

1612 In addition to the foregoing, log, taking account of all applicable legislative and policy  
 1613 obligations, a record of the additional facts of the verification process. At a minimum,  
 1614 records of identity information must include:

- 1615 a) the subscriber's full name,
- 1616 b) the subscriber's current address of record,
- 1617 c) the subscriber's current telephone or email address of record,
- 1618 d) the subscriber's authorization for issuing the subject a credential,
- 1619 e) type, issuing authority, and reference number(s) of all documents checked in the
- 1620 identity proofing process,
- 1621 f) a biometric record of each required representative of the affiliating organization
- 1622 (e.g., a photograph, fingerprint, voice recording), as determined by that
- 1623 organization's governance rules/charter.

1624 **AL4\_ID\_VRC#030 Record Retention**

1625 Either retain, securely, the record of the verification/revocation process for the duration of  
 1626 the subscriber account plus 10.5 years, or submit the record to a client CSP that has  
 1627 undertaken to retain the record for the requisite period or longer.

1628 **3.6.5 Compliance Tables**

1629 Use the following tables to correlate criteria for a particular AL and the evidence offered  
 1630 to support compliance.

1631 CSPs preparing for an assessment can use the table appropriate to the level at which they  
 1632 are seeking approval to correlate evidence with criteria or to justify non-applicability  
 1633 (e.g., "specific service types not offered"). Assessors can use the tables to record  
 1634 assessment steps and their determination of compliance or failure.

1635 **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	

1636

**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	

1637

1638

**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	

1639

1640

**Table 3-4. ID-SAC - AL4 compliance**

<b>Clause</b>	<b>Description</b>	<b>Compliance</b>
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	

1641

## 1642 **3.7 Credential Management Service Assessment Criteria**

1643 The Service Assessment Criteria in this section establish requirements for the functional  
1644 conformity of credential management services and their providers at all ALs defined in  
1645 Section 2. These criteria are generally referred to elsewhere within IAEG documentation  
1646 as CM-SAC.

1647 The criteria are divided into five parts. Each part deals with a specific functional aspect  
1648 of the overall credential management process.

1649 This SAC must be used in conjunction with the Common Organizational SAC (CO-  
1650 SAC), described in Section 3.5, and, in addition, must either:

- 1651 • explicitly include the criteria of the Identity Proofing SAC ([ID-SAC]) described  
1652 in Section 3.6, or
- 1653 • rely upon the criteria of the ID-SAC [ID-SAC] being fulfilled by the use of an  
1654 IAEG-approved ID-proofing service.

1655 Note: Some of the SAC-identifying numbers are not used in all of the ALs. In such cases,  
1656 the particular SAC number has been reserved where not used and skipped.

### 1657 **3.7.1 Part A--Credential Operating Environment**

1658 The criteria in this part deal with the overall operational environment in which the  
1659 credential life-cycle management is conducted. The credential management service  
1660 assessment criteria must be used in conjunction with the common organizational criteria  
1661 described in Section 3.5. In addition, they must either explicitly include the identity  
1662 proofing service assessment criteria described in Section 3.6 or rely upon those criteria  
1663 being fulfilled by the use of an IAEG-approved identity proofing service.

1664 These criteria describe requirements for the overall operational environment in which  
1665 credential lifecycle management is conducted. The common organizational criteria  
1666 describe broad requirements. The criteria in this section describe implementation  
1667 specifics. Implementation depends on the AL. The procedures and processes required to  
1668 create a secure environment for management of credentials and the particular  
1669 technologies that are considered strong enough to meet the assurance requirements differ  
1670 considerably from level to level.

#### 1671 **3.7.1.1 Assurance Level 1**

1672 These criteria apply to PINs and passwords.

##### 1673 **3.7.1.1.1 Credential Policy and Practices**

1674 These criteria apply to the policy and practices under which credentials are managed.

1675 An enterprise and its specified service must:

1676 **AL1\_CM\_CPP#010**            **Credential Policy and Practice Statement**

1677 No stipulation.

1678

1679 **3.7.1.1.2 Security Controls**

1680 An enterprise and its specified service must:

1681 **AL1\_CM\_CTR#010**            **Secret revelation**

1682 No stipulation.

1683 **AL1\_CM\_CTR#020**            **Protocol threat risk assessment and controls**

1684 Account for the following protocol threats and apply appropriate controls:

- 1685 a) password guessing,
- 1686 b) message replay.

1687 **AL1\_CM\_CTR#030**            **System threat risk assessment and controls**

1688 Account for the following system threats and apply appropriate controls:

- 1689 a) the introduction of malicious code,
- 1690 b) compromised authentication arising from insider action,
- 1691 c) out-of-band attacks by other users and system operators (e.g., shoulder-surfing),
- 1692 d) spoofing of system elements/applications,
- 1693 e) malfeasance on the part of subscribers and subjects.

1694

1695 **3.7.1.1.3 Storage of Long-term Secrets**

1696 An enterprise and its specified service must:

1697 **AL1\_CM\_STS#010**            **Stored Secrets**

1698 *Not* store secrets (such as passwords) as plain text and apply discretionary access controls  
1699 that limit access to administrators and those applications that require access.

1700

1701 **3.7.1.1.4 Security-relevant Event (Audit) Records**

1702 No stipulation.

1703 **3.7.1.1.5 Subject Options**

1704 An enterprise and its specified service must:

1705 **AL1\_CM\_OPN#010**            **Changeable PIN/Password**

1706 Permit subjects to change their PINs/passwords.

1707

1708 **3.7.1.2 Assurance Level 2**

1709 These criteria apply to passwords.

1710 **3.7.1.2.1 Credential Policy and Practices**

1711 These criteria apply to the policy and practices under which credentials are managed.

1712 An enterprise and its specified service must:

1713 **AL2\_CM\_CPP#010**            **Credential Policy and Practice Statement**

1714 Include in its service definition a description of the policy against which it issues  
1715 credentials and the corresponding practices it applies in their management. At a  
1716 minimum, the Credential Policy and Practice Statement must specify:

- 1717 a) if applicable, any OIDs related to the Practice and Policy Statement;
- 1718 b) how users may subscribe to the service/apply for credentials and how users'  
1719 credentials will be delivered to them;
- 1720 c) how subscribers acknowledge receipt of tokens and credentials and what  
1721 obligations they accept in so doing (including whether they consent to publication  
1722 of their details in credential status directories);
- 1723 d) how credentials may be renewed, modified, revoked, and suspended, including  
1724 how requestors are authenticated or their identity re-proven;
- 1725 e) what actions a subscriber must take to terminate a subscription.

1726 **AL2\_CM\_CPP#030**            **Management Authority**

1727 Have a nominated management body with authority and responsibility for approving the  
1728 Credential Policy and Practice Statement and for its implementation.

1729

1730 **3.7.1.2.2 Security Controls**

1731 An enterprise and its specified service must:

1732 **AL2\_CM\_CTR#010**            **Secret revelation**

1733 Use communication and authentication protocols that minimize the duration of any clear-  
1734 text disclosure of long-term secrets, even when disclosed to trusted parties.



1735 **AL2\_CM\_CTR#020 Protocol threat risk assessment and controls**

1736 Account for the following protocol threats in its risk assessment and apply controls that  
1737 reduce them to acceptable risk levels:

- 1738 a) password guessing,
- 1739 b) message replay,
- 1740 c) eavesdropping.

1741 **AL2\_CM\_CTR#030 System threat risk assessment and controls**

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

- 1744 a) the introduction of malicious code;
- 1745 b) compromised authentication arising from insider action;
- 1746 c) out-of-band attacks by both users and system operators (e.g., the ubiquitous  
1747 shoulder-surfing);
- 1748 d) spoofing of system elements/applications;
- 1749 e) malfeasance on the part of subscribers and subjects;
- 1750 f) intrusions leading to information theft.

1751 **AL2\_CM\_CTR#040 Specified Service's Key Management**

1752 Specify and observe procedures and processes for the generation, storage, and destruction  
1753 of its own cryptographic keys used for securing the specific service's assertions and other  
1754 publicized information. At a minimum, these should address:

- 1755 a) the physical security of the environment;
- 1756 b) access control procedures limiting access to the minimum number of authorized  
1757 personnel;
- 1758 c) public-key publication mechanisms;
- 1759 d) application of controls deemed necessary as a result of the service's risk  
1760 assessment;
- 1761 e) destruction of expired or compromised private keys in a manner that prohibits  
1762 their retrieval, or their archival in a manner that prohibits their reuse.

1763

1764 **3.7.1.2.3 Storage of Long-term Secrets**

1765 An enterprise and its specified service must:

1766 **AL2\_CM\_STS#010 Stored Secrets**

1767 *Not* store secrets (such as passwords) as plain text and apply discretionary access controls  
1768 that limit access to administrators and to those applications requiring access.

1769

1770 **3.7.1.2.4 Security-Relevant Event (Audit) Records**

1771 These criteria describe the need to provide an auditable log of all events that are pertinent  
1772 to the correct and secure operation of the service. The common organizational criteria  
1773 applying to provision of an auditable log of all events pertinent to the correct and secure  
1774 operation of the service must also be considered carefully. These criteria carry  
1775 implications for credential management operations.

1776 **3.7.1.2.5 Subject Options**

1777 An enterprise and its specified service must:

1778 **AL2\_CM\_OPN#010 Changeable PIN/Password**

1779 Permit subjects to change their passwords, but employ reasonable practices with respect  
1780 to password resets and repeated password failures.

1781

1782 **3.7.1.3 Assurance Level 3**

1783 These criteria apply to one-time password devices and soft crypto applications protected  
1784 by passwords or biometric controls.

1785 **3.7.1.3.1 Credential Policy and Practices**

1786 These criteria apply to the policy and practices under which credentials are managed.

1787 An enterprise and its specified service must:

1788 **AL3\_CM\_CPP#010 Credential Policy and Practice Statement**

1789 Include in its service definition a full description of the policy against which it issues  
1790 credentials and the corresponding practices it applies in their issuance. At a minimum,  
1791 the Credential Policy and Practice Statement must specify:

- 1792 a) if applicable, any OIDs related to the Credential Policy and Practice Statement;  
1793 b) how users may subscribe to the service/apply for credentials and how the users'  
1794 credentials will be delivered to them;  
1795 c) how subscribers acknowledge receipt of tokens and credentials and what  
1796 obligations they accept in so doing (including whether they consent to publication  
1797 of their details in credential status directories);  
1798 d) how credentials may be renewed, modified, revoked, and suspended, including  
1799 how requestors are authenticated or their identity -proven;  
1800 e) what actions a subscriber must take to terminate a subscription.

1801 **AL3\_CM\_CPP#030 Management Authority**

1802 Have a nominated management body with authority and responsibility for approving the  
1803 Credential Policy and Practice Statement, and for its implementation.

1804

1805 **3.7.1.3.2 Security Controls**

1806 **AL3\_CM\_CTR#020 Protocol threat risk assessment and controls**

1807 Account for the following protocol threats in its risk assessment and apply controls that  
1808 reduce them to acceptable risk levels:

- 1809 a) password guessing,
- 1810 b) message replay,
- 1811 c) eavesdropping,
- 1812 d) relying party (verifier) impersonation,
- 1813 e) man-in-the-middle attack.

1814 **AL3\_CM\_CTR#030 System threat risk assessment and controls**

1815 Account for the following system threats in its risk assessment and apply controls that  
1816 reduce them to acceptable risk levels:

- 1817 a) the introduction of malicious code;
- 1818 b) compromised authentication arising from insider action;
- 1819 c) out-of-band attacks by both users and system operators (e.g., the ubiquitous  
1820 shoulder-surfing);
- 1821 d) spoofing of system elements/applications;
- 1822 e) malfeasance on the part of subscribers and subjects;
- 1823 f) intrusions leading to information theft.

1824 **AL3\_CM\_CTR#040 Specified Service's Key Management**

1825 Specify and observe procedures and processes for the generation, storage, and destruction  
1826 of its own cryptographic keys used for securing the specific service's assertions and other  
1827 publicized information. At a minimum, these should address:

- 1828 a) the physical security of the environment;
- 1829 b) access control procedures limiting access to the minimum number of authorized  
1830 personnel;
- 1831 c) public-key publication mechanisms;
- 1832 d) application of controls deemed necessary as a result of the service's risk  
1833 assessment;
- 1834 e) destruction of expired or compromised private keys in a manner that prohibits  
1835 their retrieval **or** their archival in a manner that prohibits their reuse.

1836

1837 **3.7.1.3.3 Storage of Long-term Secrets**

1838 An enterprise and its specified service must:

1839 **AL3\_CM\_STS#010 Stored Secrets**

1840 *Not* store secrets (such as passwords) as plain text and apply discretionary access controls  
1841 that limit access to administrators and to those applications that require access.

1842 **AL3\_CM\_STS#020 Stored Secret Encryption**

1843 Encrypt such shared secret files so that:

- 1844 a) the encryption key for the shared secret file is encrypted under a key held in a
- 1845 FIPS 140-2 [FIPS140-2] Level 2 or higher validated hardware cryptographic
- 1846 module or any FIPS 140-2 Level 3 or 4 cryptographic module;
- 1847 b) the shared secret file is decrypted only as immediately required for an
- 1848 authentication operation;
- 1849 c) shared secrets are protected as a key within the boundary of a FIPS 140-2 Level 2
- 1850 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or
- 1851 4 cryptographic module and are not exported from the module in plain text;
- 1852 d) shared secrets are split by an "*n from m*" cryptographic secret sharing method.

1853

1854 **3.7.1.3.4 Security-relevant Event (Audit) Records**

1855 These criteria describe the need to provide an auditable log of all events that are pertinent  
1856 to the correct and secure operation of the service. The common organizational criteria  
1857 applying to the recording of all security-related events must also be considered carefully.  
1858 These criteria carry implications for credential management operations.

1859 In the specific context of a certificate management service, an enterprise and its specified  
1860 service must:

1861 **AL3\_CM\_SER#010 Security event logging**

1862 Ensure that such audit records include:

- 1863 a) the identity of the point of registration (irrespective of whether internal or
- 1864 outsourced);
- 1865 b) generation of the subscriber's keys or the evidence that the subscriber was in
- 1866 possession of both parts of their own key-pair;
- 1867 c) generation of the subscriber's certificate;
- 1868 d) dissemination of the subscriber's certificate;
- 1869 e) any revocation or suspension associated with the subscriber's certificate.

1870

1871 **3.7.1.3.5 Subject options**

1872 An enterprise and its specified service must:

1873 **AL3\_CM\_OPN#010 Changeable PIN/Password**

1874 Permit subjects to change the password used to activate their credentials.

1875

1876 **3.7.1.4 Assurance Level 4**

1877 These criteria apply exclusively to cryptographic technology deployed through a Public  
1878 Key Infrastructure. This technology requires hardware tokens protected by password or  
1879 biometric controls. No other forms of credential are permitted at AL4.

1880 **3.7.1.4.1 Certification Policy and Practices**

1881 These criteria apply to the policy and practices under which certificates are managed.

1882 An enterprise and its specified service must:

1883 **AL4\_CM\_CPP#020 Certificate Policy/Certification Practice Statement**

1884 Include in its service definition its full Certificate Policy and the corresponding  
1885 Certification and Practice Statement. The Certificate Policy and Certification Practice  
1886 Statement must conform to IETF RFC 3647 (2003-11) [[RFC 3647](#)] in their content and  
1887 scope or be demonstrably consistent with the content or scope of that RFC. At a  
1888 minimum, the Certificate Policy must specify:

- 1889 a) applicable OIDs for each certificate type issued;
- 1890 b) how users may subscribe to the service/apply for certificates, and how certificates  
1891 will be issued to them;
- 1892 c) if users present their own keys, how they will be required to demonstrate  
1893 possession of the private key;
- 1894 d) if users' keys are generated for them, how the private keys will be delivered to  
1895 them;
- 1896 e) how subscribers acknowledge receipt of tokens and credentials and what  
1897 obligations they accept in so doing (including whether they consent to publication  
1898 of their details in certificate status directories);
- 1899 f) how certificates may be renewed, re-keyed, modified, revoked, and suspended,  
1900 including how requestors are authenticated or their identity proven;
- 1901 g) what actions a subscriber must take to terminate their subscription.

1902 **AL4\_CM\_CPP#030 Management Authority**

1903 Have a nominated or appointed high-level management body with authority and  
1904 responsibility for approving the Certificate Policy and Certification Practice Statement,  
1905 including ultimate responsibility for its proper implementation.

1906

1907 **3.7.1.4.2 Security Controls**

1908 An enterprise and its specified service must:

1909 **AL4\_CM\_CTR#020 Protocol threat risk assessment and controls**

1910 Account for the following protocol threats in its risk assessment and apply controls that  
1911 reduce them to acceptable risk levels:

- 1912 a) man-in-the-middle attack,
- 1913 b) session hijacking.

1914 **AL4\_CM\_CTR#030 System threat risk assessment and controls**

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

- 1917 a) the introduction of malicious code;
- 1918 b) compromised authentication arising from insider action;
- 1919 c) out-of-band attacks by both users and system operators (e.g., the ubiquitous  
1920 shoulder-surfing);
- 1921 d) spoofing of system elements/applications;
- 1922 e) malfeasance on the part of subscribers and subjects;
- 1923 f) intrusions leading to information theft.

1924 **AL4\_CM\_CTR#040 Specified Service's Key Management**

1925 Specify and observe procedures and processes for the generation, storage, and destruction  
1926 of its own cryptographic keys used for securing the specific service's assertions and other  
1927 publicized information. At a minimum, these should address:

- 1928 a) the physical security of the environment;
- 1929 b) access control procedures limiting access to the minimum number of authorized  
1930 personnel;
- 1931 c) public-key publication mechanisms;
- 1932 d) application of controls deemed necessary as a result of the service's risk  
1933 assessment;
- 1934 e) destruction of expired or compromised private keys in a manner that prohibits  
1935 their retrieval, or their archival in a manner which prohibits their reuse;

1936

1937 **3.7.1.4.3 Storage of Long-term Secrets**

1938 The enterprise and its specified service must meet the following criteria:

1939 **AL4\_CM\_STS#010 Stored Secrets**

1940 *Not* store secrets (such as private keys) as plain text and must apply discretionary access  
1941 controls that limit access to trusted administrators.

1942 **AL4\_CM\_STS#020 Stored Secret Encryption**

1943 Encrypt such secret files so that:

- 1944 a) the encryption key for the secret file is encrypted under a key held in a FIPS 140-  
1945 2 [FIPS140-2] Level 2 or higher validated hardware cryptographic module or any  
1946 FIPS 140-2 Level 3 or 4 cryptographic module;
- 1947 b) the secret file is decrypted only as immediately required for a key recovery  
1948 operation;
- 1949 c) secrets are protected as a key within the boundary of a FIPS 140-2 Level 2 or  
1950 higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4  
1951 cryptographic module and are not exported from the module in plaintext;
- 1952 d) escrowed secrets are split by an "*n from m*" cryptographic secret storing method.  
1953

1954 **3.7.1.4.4 Security-relevant Event (Audit) Records**

1955 These criteria describe the need to provide an auditable log of all events that are pertinent  
1956 to the correct and secure operation of the service. The common organizational criteria  
1957 relating to the recording of all security-related events must also be considered carefully.

1958 These criteria carry implications for credential management operations.

1959 An enterprise and its specified service must:

1960 **AL4\_CM\_SER#010 Security event logging**

1961 Ensure that such audit records include:

- 1962 a) the identity of the point of registration (whether internal or outsourced);
- 1963 b) generation of the subscriber's keys or evidence that the subscriber was in  
1964 possession of both parts of the key-pair;
- 1965 c) generation of the subscriber's certificate;
- 1966 d) dissemination of the subscriber's certificate;
- 1967 e) any revocation or suspension associated with the subscriber's certificate.  
1968

1969 **3.7.1.4.5 Subject Options**

1970 An enterprise and its specified service must:

1971 **AL4\_CM\_OPN#010**            **Changeable PIN/Password**

1972 Permit subjects to change the passwords used to activate their credentials.

1973 **3.7.2 Part B--Credential Issuing**

1974 These criteria apply to the verification of the identity of the subject of a credential and  
1975 with token strength and credential delivery mechanisms. They address requirements  
1976 levied by the use of various technologies to achieve the appropriate AL<sup>4</sup>. These criteria  
1977 include by reference all applicable criteria in Section 3.6.

1978 **3.7.2.1 Assurance Level 1**

1979 **3.7.2.1.1 Identity Proofing**

1980 These criteria determine how the enterprise shows compliance with the criteria for  
1981 fulfilling identity proofing functions.

1982 The enterprise and its specified service must:

1983 **AL1\_CM\_IDP#010**            **Self-managed Identity Proofing**

1984 If the enterprise assumes direct responsibility for identity proofing functions, show, by  
1985 direct inclusion, compliance with all applicable identity proofing service assessment  
1986 criteria<sup>5</sup> ([ID-SAC]) for AL1 or higher.

1987 **AL1\_CM\_IDP#020**            **IAEG-approved outsourced service**

1988 If the enterprise outsources responsibility for identity proofing functions and uses a  
1989 service already operating under an IAEG Identity Proofing Approval, show that the  
1990 service in question has been approved at AL1 or higher.

1991 **AL1\_CM\_IDP#030**            **Non IAEG-approved outsourced service**

1992 If the enterprise outsources responsibility for identity proofing functions, ensure that each  
1993 provider of such a service demonstrates compliance with all applicable identity proofing  
1994 service assessment criteria for AL1 or higher, and that the enterprise, itself, has in place  
1995 controls to ensure the continued fulfillment of those criteria by the provider to which the  
1996 functions have been outsourced.

---

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

<sup>5</sup> 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.



- 1997 **AL1\_CM\_IDP#040**            **Revision to subscriber information**
- 1998 Provide a means for subscribers to amend their stored information after registration.
- 1999
- 2000 **3.7.2.1.2 Credential Creation**
- 2001 These criteria address the requirements for creation of credentials that can only be used at
- 2002 AL1. Any credentials/tokens that comply with the criteria stipulated for AL2 and higher
- 2003 are acceptable at AL1.
- 2004 An enterprise and its specified service must:
- 2005 **AL1\_CM\_CRN\_#010**            **Authenticated Request**
- 2006 Only accept a request to generate a credential and bind it to an identity if the source of the
- 2007 request can be authenticated as being authorized to perform identity proofing at AL1 or
- 2008 higher.
- 2009 **AL1\_CM\_CRN\_#020**            **Unique identity**
- 2010 Ensure that the identity (e.g., UserID) to which a credential is to be bound is unique
- 2011 within the specified service's intended community.
- 2012 **AL1\_CM\_CRN\_#030**            **Token uniqueness**
- 2013 Allow the subscriber to select a unique token (e.g., UserID combined with PIN/password)
- 2014 that must be validated to be unique within the specified service's intended community and
- 2015 assigned uniquely to a single identity subject.
- 2016
- 2017 **3.7.2.2 Assurance Level 2**
- 2018 **3.7.2.2.1 Identity Proofing**
- 2019 These criteria determine how the enterprise shows compliance with the criteria for
- 2020 fulfilling identity proofing functions.
- 2021 The enterprise and its specified service must:
- 2022 **AL2\_CM\_IDP#010**            **Self-managed Identity Proofing**
- 2023 If the enterprise assumes direct responsibility for identity proofing functions, show, by
- 2024 direct inclusion, compliance with all applicable identity proofing service assessment
- 2025 criteria for AL2 or higher.

2026 **AL2\_CM\_IDP#020** **IAEG-approved outsourced service**

2027 If the enterprise outsources responsibility for identity proofing functions and uses a  
2028 service already operating under an IAEG Identity Proofing Approval, show that the  
2029 service in question has been approved at AL2 or higher and that its approval has at least 6  
2030 months of remaining validity.

2031 **AL2\_CM\_IDP#030** **Non IAEG-approved outsourced service**

2032 If the enterprise outsources responsibility for identity proofing functions, ensure that each  
2033 provider of such a service demonstrates compliance with all applicable identity proofing  
2034 service assessment criteria for AL2 or higher, and that the enterprise, itself, has in place  
2035 controls to ensure the continued fulfillment of those criteria by the provider to which the  
2036 functions have been outsourced.

2037 **AL2\_CM\_IDP#040** **Revision to subscriber information**

2038 Provide a means for subscribers to securely amend their stored information after  
2039 registration, either by re-proving their identity, as in the initial registration process, or by  
2040 using their credentials to authenticate their revision.

2041

2042 **3.7.2.2.2 Credential Creation**

2043 These criteria define the requirements for creation of credentials whose highest use is at  
2044 AL2. Credentials/tokens that comply with the criteria stipulated at AL3 and higher are  
2045 also acceptable at AL2 and below.

2046 Note, however, authentication can only be provided at the assurance level at which the  
2047 identity is proven.

2048 An enterprise and its specified service must:

2049 **AL2\_CM\_CRN\_#010** **Authenticated Request**

2050 Only accept a request to generate a credential and bind it to an identity if the source of the  
2051 request can be authenticated as being authorized to perform identity proofing at AL2 or  
2052 higher.

2053 **AL2\_CM\_CRN\_#020** **Unique identity**

2054 Ensure that the identity (e.g., UserID) to which a credential is to be bound is unique  
2055 within the specified service's intended community.

- 2056 **AL2\_CM\_CRN\_#030**      **Token uniqueness**
- 2057 Allow the subscriber to select a unique token (e.g., UserID combined with PIN/password)  
2058 that must be validated to be unique within the specified service's intended community and  
2059 assigned uniquely to a single identity.
- 2060 **AL2\_CM\_CRN\_#040**      **Password strength**
- 2061 Only allow passwords that, over the life of the password, have resistance to an on-line  
2062 guessing attack against a selected user/password of at least 1 in  $2^{14}$  (16,384), accounting  
2063 for state-of-the-art attack strategies.
- 2064 **AL2\_CM\_CRN\_#050**      **One-time password strength**
- 2065 Only allow password tokens that, over the life of the password, have a resistance to  
2066 guessing of 1 in  $2^{14}$  (16,384), accounting for state-of-the-art attack strategies.
- 2067 **AL2\_CM\_CRN\_#060**      **Software cryptographic token strength**
- 2068 Refer to Section [3.7.2.3](#).
- 2069 **AL2\_CM\_CRN\_#070**      **Hardware token strength**
- 2070 Refer to Section [3.7.2.3](#).
- 2071 **AL2\_CM\_CRN\_#080**      **Binding of key**
- 2072 No stipulation.
- 2073 **AL2\_CM\_CRN\_#090**      **Nature of subject**
- 2074 Record the nature of the subject of the credential (which must correspond to the manner  
2075 of identity proofing performed), i.e., physical person, a named person acting on behalf of  
2076 a corporation or other legal entity, corporation or legal entity, or corporate machine entity,  
2077 in a manner that can be unequivocally associated with the credential and the identity that  
2078 it asserts.
- 2079 **3.7.2.2.3 Credential Delivery**
- 2080 An enterprise and its specified service must:
- 2081 **AL2\_CM\_CRD\_#010**      **Confirm subject's details**
- 2082 Confirm the subject's contact details and notify the subject of the credential's issuance by:
- 2083 a)      sending notice to the address of record confirmed during identity proofing or

- 2084 b) issuing the credential(s) in a manner that confirms the address of record supplied  
2085 by the applicant during identity proofing or  
2086 c) issuing the credential(s) in a manner that confirms the ability of the applicant to  
2087 receive telephone communications at a telephone number or email at an email  
2088 address supplied by the applicant during identity proofing.  
2089

2090 **3.7.2.3 Assurance Level 3**

2091 **3.7.2.3.1 Identity Proofing**

2092 These criteria in this section determine how the enterprise shows compliance with the  
2093 criteria for fulfilling identity proofing functions.

2094 The enterprise and its specified service must:

2095 **AL3\_CM\_IDP#010 Self-managed Identity Proofing**

2096 If the enterprise assumes direct responsibility for identity proofing functions, show, by  
2097 direct inclusion, compliance with all applicable identity proofing service assessment  
2098 criteria for AL3 or AL4.

2099 **AL3\_CM\_IDP#020 IAEG-approved outsourced service**

2100 If the enterprise outsources responsibility for identity proofing functions and uses a  
2101 service already operating under an IAEG Identity Proofing Approval, show that the  
2102 service in question has been approved at AL3 or AL4 and that its approval has at least 6  
2103 months of remaining validity.

2104 **AL3\_CM\_IDP#030 Non IAEG-approved outsourced service**

2105 *Not* use any non-IAEG-approved outsourced services for identity proofing.

2106 **AL3\_CM\_IDP#040 Revision to subscriber information**

2107 Provide a means for subscribers to securely amend their stored information after  
2108 registration, either by re-proving their identity as in the initial registration process or by  
2109 using their credentials to authenticate their revision. Successful revision must, where  
2110 necessary, instigate the re-issuance of the credential.

2111

2112 **3.7.2.3.2 Credential Creation**

2113 These criteria define the requirements for creation of credentials whose highest use is  
2114 AL3. Any credentials/tokens that comply with the criteria stipulated at AL4 are also  
2115 acceptable at AL3 and below.

2116 Note, however, that a token and credential created according to these criteria may not  
2117 necessarily provide that level of assurance for the claimed identity of the subscriber.  
2118 Authentication can only be provided at the assurance level at which the identity is proven.  
2119 An enterprise and its specified service must:

2120 **AL3\_CM\_CRN\_#010      Authenticated Request**

2121 Only accept a request to generate a credential and bind it to an identity if the source of the  
2122 request can be authenticated as being authorized to perform identity proofing at AL3 or  
2123 higher.

2124 **AL3\_CM\_CRN\_#020      Unique identity**

2125 Ensure that the identity (e.g., UserID) to which a credential is to be bound is unique  
2126 within the specified service's intended community, accounting fully for identities  
2127 previously used and that are now cancelled.

2128 **AL3\_CM\_CRN\_#030      Token uniqueness**

2129 Allow the subscriber to select a unique token (e.g., UserID combined with PIN/password)  
2130 that must be validated to be unique within the specified service's intended community and  
2131 assigned uniquely to a single identity.

2132 **AL3\_CM\_CRN\_#040      PIN/Password strength**

2133 Must not use PIN/password tokens.

2134 **AL3\_CM\_CRN\_#050      One-time password strength**

2135 Only allow one-time password tokens that:

- 2136 a) depend on a symmetric key stored on a personal hardware device evaluated
- 2137 against FIPS 140-2 [FIPS140-2] Level 1 or higher;
- 2138 b) permit at least 10<sup>6</sup> possible password values;
- 2139 c) require password or biometric activation by the subscriber.

2140 **AL3\_CM\_CRN\_#060      Software cryptographic token strength**

2141 Ensure that software cryptographic keys stored on general-purpose devices:

- 2142 a) are protected by a key and cryptographic protocol that are evaluated against FIPS
- 2143 140-2 Level 2;
- 2144 b) require password or biometric activation by the subscriber or employ a password
- 2145 protocol when being used for authentication.

2146 **AL3\_CM\_CRN\_#070**      **Hardware token strength**

2147 Ensure that hardware tokens used to store cryptographic keys:

- 2148 a)      employ a cryptographic module that is evaluated against FIPS 140-2 Level 1 or
- 2149          higher;
- 2150 b)      require password or biometric activation by the subscriber or also employ a
- 2151          password when being used for authentication.

2152 **AL3\_CM\_CRN\_#080**      **Binding of key**

2153 If the specified service generates the subject's key pair, that the key generation process  
2154 securely and uniquely binds that process to the certificate generation and maintains at all  
2155 times the secrecy of the private key, until it is accepted by the subject.

2156 **AL3\_CM\_CRN\_#090**      **Nature of subject**

2157 Record the nature of the subject of the credential (which must correspond to the manner  
2158 of identity proofing performed), i.e., private person, a named person acting on behalf of a  
2159 corporation or other legal entity, corporation or legal entity, or corporate machine entity,  
2160 in a manner that can be unequivocally associated with the credential and the identity that  
2161 it asserts.

2162

2163 **3.7.2.3.3 Subject Key Pair Generation**

2164 An enterprise and its specified service must:

2165 **AL3\_CM\_SKP\_#010**      **Key generation by Specified Service**

2166 If the specified service generates the subject's keys:

- 2167 a)      use a FIPS-approved [FIPS] algorithm that is recognized as being fit for the
- 2168          purposes of the service;
- 2169 b)      only create keys of a key length and for use with a FIPS-approved public key
- 2170          algorithm recognized as being fit for the purposes of the service;
- 2171 c)      generate and store the keys securely until delivery to and acceptance by the
- 2172          subject;
- 2173 d)      deliver the subject's private key in a manner that ensures that the privacy of the
- 2174          key is not compromised and only the subject has access to the private key.

2175 **AL3\_CM\_SKP\_#020**      **Key generation by Subject**

2176 If the subject generates and presents its own keys, obtain the subject's written  
2177 confirmation that it has:

- 2178 a) used a FIPS-approved algorithm that is recognized as being fit for the purposes of  
2179 the service;  
2180 b) created keys of a key length and for use with a FIPS-approved public key  
2181 algorithm recognized as being fit for the purposes of the service.  
2182

2183 **3.7.2.3.4 Credential Delivery**

2184 An enterprise and its specified service must:

2185 **AL3\_CM\_CRD\_#010 Confirm subject's details**

2186 Confirm the subject's contact details and notify the subject of the credential's issuance by:

- 2187 a) sending notice to the address of record confirmed during identity proofing, and  
2188 either  
2189 i) issuing the credential(s) in a manner that confirms the address of record  
2190 supplied by the applicant during identity proofing; or  
2191 ii) issuing the credential(s) in a manner that confirms the ability of the  
2192 applicant to receive telephone communications at a phone number  
2193 supplied by the applicant during identity proofing while recording the  
2194 applicant's voice.

2195 **AL3\_CM\_CRD\_#020 Subject's acknowledgement**

2196 Receive acknowledgement of receipt of the credential before it is activated and its  
2197 directory status record is published (and thereby the subscription becomes active or re-  
2198 activated, depending upon the circumstances of issue).

2199

2200 **3.7.2.4 Assurance Level 4**

2201 **3.7.2.4.1 Identity Proofing**

2202 These criteria determine how the enterprise shows compliance with the criteria for  
2203 fulfilling identity proofing functions.

2204 An enterprise and its specified service must:

2205 **AL4\_CM\_IDP#010 Self-managed Identity Proofing**

2206 If the enterprise assumes direct responsibility for identity proofing functions, show, by  
2207 direct inclusion, compliance with all applicable identity proofing service assessment  
2208 criteria for AL4.

- 
- 2209 **AL4\_CM\_IDP#020** **IAEG-approved outsourced service**
- 2210 If the enterprise outsources responsibility for identity proofing functions and uses a  
2211 service already operating under an IAEG Identity Proofing Approval, show that the  
2212 service in question has been approved at AL4 and that its approval has at least 12 months  
2213 of remaining validity.
- 2214 **AL4\_CM\_IDP#030** **Non IAEG-approved outsourced service**
- 2215 Not use any non-IAEG-approved outsourced services for identity proofing unless they  
2216 can be demonstrated to have satisfied equivalently rigorous requirements established  
2217 by another scheme recognized by IAEG.
- 2218 **AL4\_CM\_IDP#040** **Revision to subscriber information**
- 2219 Provide a means for subscribers to securely amend their stored information after  
2220 registration, either by re-proving their identity as in the initial registration process or by  
2221 using their credentials to authenticate their revision. Successful revision must, where  
2222 necessary, instigate the re-issuance of the credential.
- 2223 **3.7.2.4.2 Credential Creation**
- 2224 These criteria define the requirements for creation of credentials whose highest use is  
2225 AL4.
- 2226 Note, however, that a token and credential created according to these criteria may not  
2227 necessarily provide that level of assurance for the claimed identity of the subscriber.  
2228 Authentication can only be provided at the assurance level at which the identity is proven.  
2229 An enterprise and its specified service must:
- 2230 **AL4\_CM\_CRN\_#010** **Authenticated Request**
- 2231 Only accept a request to generate a credential and bind it to an identity if the source of the  
2232 request can be authenticated as being authorized to perform identity proofing at AL4.
- 2233 **AL4\_CM\_CRN\_#020** **Unique identity**
- 2234 Ensure that the identity (e.g., UserID) to which a credential is to be bound is unique  
2235 within the specified service's intended community.
- 2236 **AL4\_CM\_CRN\_#030** **Token uniqueness**
- 2237 Allow the subscriber to select a unique token (e.g., UserID combined with PIN/password)  
2238 that must be validated to be unique within the specified service's intended community and  
2239 assigned uniquely to a single identity.



2240 **AL4\_CM\_CRN\_#040 PIN/Password strength**

2241 *Not* use PIN/password tokens.

2242 **AL4\_CM\_CRN\_#050 One-time password strength**

2243 *Not* use one-time password tokens.

2244 **AL4\_CM\_CRN\_#060 Software cryptographic token strength**

2245 *Not* use software cryptographic tokens.

2246 **AL4\_CM\_CRN\_#070 Hardware token strength**

2247 Ensure that hardware tokens used to store cryptographic keys:

- 2248 a) employ a cryptographic module that is evaluated against FIPS 140-2 [FIPS140-2] Level
- 2249 2 or higher;
- 2250 b) are evaluated against FIPS 140-2 Level 3 or higher for their physical security;
- 2251 c) require password or biometric activation by the subscriber.

2252 **AL4\_CM\_CRN\_#080 Binding of key**

2253 If the specified service generates the subject's key pair, that the key generation process  
2254 securely and uniquely binds that process to the certificate generation and maintains at all  
2255 times the secrecy of the private key, until it is accepted by the subject.

2256 **AL3\_CM\_CRN\_#090 Nature of subject**

2257 Record the nature of the subject of the credential, i.e., private person, a named person  
2258 acting on behalf of a corporation or other legal entity, corporation or legal entity, or  
2259 corporate machine entity, in a manner that can be unequivocally associated with the  
2260 credential and the identity that it asserts.

2261

2262 **3.7.2.4.3 Subject Key Pair Generation**

2263 An enterprise and its specified service must:

2264 **AL4\_CM\_SKP\_#010 Key generation by Specified Service**

2265 If the specified service generates the subject's keys:

- 2266 a) use a FIPS-approved [FIPS] algorithm that is recognized as being fit for the
- 2267 purposes of the service;
- 2268 b) only create keys of a key length and for use with a FIPS-approved public key
- 2269 algorithm recognized as being fit for the purposes of the service;

- 2270 c) generate and store the keys securely until delivery to and acceptance by the  
2271 subject;  
2272 d) deliver the subject's private key in a manner that ensures that the privacy of the  
2273 key is not compromised and only the subject has access to the private key.

2274 **AL4\_CM\_SKP\_#020 Key generation by Subject**

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

- 2277 a) used a FIPS-approved algorithm that is recognized as being fit for the purposes of  
2278 the service;  
2279 b) created keys of a key length and for use with a FIPS-approved public key  
2280 algorithm recognized as being fit for the purposes of the service.  
2281

2282 **3.7.2.4.4 Credential Delivery**

2283 An enterprise and its specified service must:

2284 **AL4\_CM\_CRD\_#010 Confirm subject's details**

2285 Confirm the subject's contact details and notify the subject of the credential's issuance by:

- 2286 a) sending notice to the address of record confirmed during identity proofing;  
2287 b) unless the subject presented with a private key, issuing the hardware token to the  
2288 subject in a manner that confirms the address of record supplied by the applicant  
2289 during identity proofing;  
2290 c) issuing the certificate to the subject over a separate channel in a manner that  
2291 confirms either the address of record or the email address supplied by the  
2292 applicant during identity proofing.

2293 **AL4\_CM\_CRD\_#020 Subject's acknowledgement**

2294 Receive acknowledgement of receipt of the hardware token before it is activated and the  
2295 corresponding certificate and its directory status record are published (and thereby the  
2296 subscription becomes active or re-activated, depending upon the circumstances of issue).

2297 **3.7.3 Part C--Credential Revocation**

2298 These criteria deal with credential revocation and the determination of the legitimacy of a  
2299 revocation request.

2300 **3.7.3.1 Assurance Level 1**

2301 An enterprise and its specified service must:

2302 **3.7.3.1.1 Not used**

2303 **3.7.3.1.2 Not used**

2304 **3.7.3.1.3 Secure Revocation Request**

2305 This criterion applies when revocation requests between remote components of a service  
2306 are made over a secured communication.

2307 An enterprise and its specified service must:

2308 **AL1\_ID\_SRR#010 Submit Request**

2309 Submit a request for revocation to the Credential Issuer service (function), using a  
2310 secured network communication, if necessary.

2311

2312 **3.7.3.2 Assurance Level 2**

2313 **3.7.3.2.1 Revocation Procedures**

2314 These criteria address general revocation functions, such as the processes involved and  
2315 the basic requirements for publication.

2316 An enterprise and its specified service must:

2317 **AL2\_CM\_RVP#010 Revocation procedures**

2318 State the conditions under which revocation of an issued credential may occur, the  
2319 processes by which a revocation request may be submitted, the persons and organizations  
2320 from which a revocation request will be accepted, the validation steps that will be applied  
2321 to ensure the validity (identity) of the Revocant, and the response time between a  
2322 revocation request being accepted and the publication of revised certificate status.

2323 **AL2\_CM\_RVP#020 Secure status notification**

2324 Ensure that published credential status notification information can be relied upon in  
2325 terms of the enterprise being its origin (i.e., its authenticity) and its correctness (i.e., its  
2326 integrity).

2327 **AL2\_CM\_RVP#030 Revocation publication**

2328 Ensure that published credential status notification is revised within 72 hours of the  
2329 receipt of a valid revocation request, such that any subsequent attempts to use that  
2330 credential in an authentication shall be unsuccessful.

2331 **AL2\_ID\_RVP#040** **Verify revocation identity**

2332 Establish that the identity for which a revocation request is received is one that was  
2333 issued by the specified service.

2334 **AL2\_ID\_RVP#050** **Revocation Records**

2335 Retain a record of any revocation of a credential that is related to a specific identity  
2336 previously verified, solely in connection to the stated credential. At a minimum, records  
2337 of revocation must include:

- 2338 a) the Revocant's full name;
- 2339 b) the Revocant's current address;
- 2340 c) type, issuing authority, and reference number(s) of all documents checked in the  
2341 identity proofing process for the Revocant;
- 2342 d) the Revocant's authority to revoke (e.g., subscriber themselves, someone acting  
2343 with the subscriber's power of attorney, the credential issuer, law enforcement, or  
2344 other legal due process);
- 2345 e) the subscriber's full name and, where applicable, unique service reference (e.g.,  
2346 certificate serial number, IP address);
- 2347 f) the subscriber's date of birth;
- 2348 g) the subscriber's current address of record;
- 2349 h) the Credential Issuer's identity (if not directly responsible for the identity proofing  
2350 service);
- 2351 i) the identity associated with the credential (whether the subscriber's name or a  
2352 pseudonym);
- 2353 j) the reason for revocation.

2354 **AL2\_ID\_RVP#060** **Record Retention**

2355 Retain, securely, the record of the revocation process for the duration of the subscriber's  
2356 account plus 7.5 years.

2357

2358 **3.7.3.2.2 Verify Revocant's Identity**

2359 The enterprise should not act on a request for revocation without first establishing the  
2360 validity of the request (if it does not, itself, determine the need for revocation).

2361 In order to do so, the enterprise and its specified service must:

2362 **AL2\_ID\_RVR#010** **Verify revocation identity**

2363 Establish that the credential for which a revocation request is received was one that was  
2364 issued by the specified service.

2365 **AL2\_ID\_RVR#020**                    **Revocation reason**

2366 Establish the reason for the revocation request as being sound and well founded, in  
2367 combination with verification of the Revocant, according to AL2\_ID\_RVR#030,  
2368 AL2\_ID\_RVR#040, or AL2\_ID\_RVR#050.

2369 **AL2\_ID\_RVR#030**                    **Verify Subscriber as Revocant**

2370 When the subscriber seeks revocation of the subscriber's own credential, the enterprise  
2371 must:

- 2372 a) if in person, require presentation of a primary Government Picture ID document
- 2373 that must be electronically verified by a record check against the provided identity
- 2374 with the specified issuing authority's records, or
- 2375 b) if remote:
  - 2376 i. electronically verify a signature against records (if available), confirmed
  - 2377 with a call to a telephone number of record, or
  - 2378 ii. authenticate an electronic request as being from the same subscriber,
  - 2379 supported by a credential at Assurance Level 2 or higher.

2380 **AL2\_ID\_RVR#040**                    **ETSP as Revocant**

2381 Where a CSP seeks revocation of a subscriber's credential, the enterprise must establish  
2382 that the request is either:

- 2383 a) from the specified service itself, with authorization as determined by established
- 2384 procedures, or
- 2385 b) from the client Credential Issuer, by authentication of a formalized request over
- 2386 the established secure communications network.

2387 **AL2\_ID\_RVR#050**                    **Verify Legal Representative as Revocant**

2388 Where the request for revocation is made by a law enforcement officer or presentation of  
2389 a legal document, the enterprise must:

- 2390 a) if in person, verify the identity of the person presenting the request, or
- 2391 b) if remote:
  - 2392 i. in paper/facsimile form, verify the origin of the legal document by a
  - 2393 database check or by telephone with the issuing authority, or
  - 2394 ii. authenticate an electronic request as being from a recognized legal office,
  - 2395 supported by a credential at Assurance Level 3 or higher.

2396

2397 **3.7.3.2.3 Secure Revocation Request**

2398 This criterion requires that revocation requests between remote components of the service  
2399 be made with secured communications.

2400 An enterprise and its specified service must:

2401 **AL2\_ID\_SRR#010            Submit Request**

2402 Submit a request for the revocation to the Credential Issuer service (function), using a  
2403 secured network communication if necessary.

2404

2405 **3.7.3.3    Assurance Level 3**

2406 **3.7.3.3.1    Revocation Procedures**

2407 These criteria address general revocation functions, such as the processes involved and  
2408 the basic requirements for publication.

2409 An enterprise and its specified service must:

2410 **AL3\_CM\_RVP#010            Revocation procedures**

2411 State the conditions under which revocation of an issued credential may occur, the  
2412 processes by which a revocation request may be submitted, the persons and organizations  
2413 from which a revocation request will be accepted, the validation steps that will be applied  
2414 to ensure the validity (identity) of the Revocant, and the response time between a  
2415 revocation request being accepted and the publication of revised certificate status.

2416 **AL3\_CM\_RVP#020            Secure status notification**

2417 Ensure that published credential status notification information can be relied upon in  
2418 terms of the enterprise being its origin (i.e., its authenticity) and its correctness (i.e., its  
2419 integrity).

2420 **AL3\_CM\_RVP#030            Revocation publication**

2421 Ensure that published credential status notification is revised within 24 hours of the  
2422 receipt of a valid revocation request, such that any subsequent attempts to use that  
2423 credential in an authentication shall be unsuccessful. The nature of the revocation  
2424 mechanism shall be in accord with the technologies supported by the service.

2425 **AL3\_ID\_RVP#050            Revocation Records**

2426 Retain a record of any revocation of a credential that is related to a specific identity  
2427 previously verified, solely in connection to the stated credential. At a minimum, records  
2428 of revocation must include:

- 2429 a)     the Revocant's full name;
- 2430 b)     the Revocant's current address;

- 2431 c) type, issuing authority, and reference number(s) of all documents checked in the
- 2432 identity proofing process for the Revocant;
- 2433 d) the Revocant's authority to revoke (e.g., subscriber themselves, someone acting
- 2434 with the subscriber's power of attorney, the credential issuer, law enforcement, or
- 2435 other legal due process);
- 2436 e) the subscriber's full name and, where applicable, unique service reference (e.g.,
- 2437 certificate serial number, IP address);
- 2438 f) the subscriber's date of birth;
- 2439 g) the subscriber's current address of record;
- 2440 h) the Credential Issuer's identity (if not directly responsible for the identity proofing
- 2441 service);
- 2442 i) the identity associated with the credential (whether the subscriber's name or a
- 2443 pseudonym);
- 2444 j) the reason for revocation.

2445 **AL3\_ID\_RVP#060 Record Retention**

2446 Retain, securely, the record of the revocation process for the duration of the subscriber's

2447 account plus 7.5 years.

2448

2449 **3.7.3.3.2 Verify Revocant's Identity**

2450 Revocation of a credential requires that the requestor and the nature of the request be

2451 verified as rigorously as the original identity proofing. The enterprise should not act on a

2452 request for revocation without first establishing the validity of the request (if it does not,

2453 itself, determine the need for revocation).

2454 In order to do so, the enterprise and its specified service must:

2455 **AL3\_ID\_RVR#010 Verify revocation identity**

2456 Establish that the credential for which a revocation request is received is one that was

2457 initially issued by the specified service, applying the same process and criteria as would

2458 be applied to an original identity proofing.

2459 **AL3\_ID\_RVR#020 Revocation reason**

2460 Establish the reason for the revocation request as being sound and well founded, in

2461 combination with verification of the Revocant, according to AL3\_ID\_RVR#030,

2462 AL3\_ID\_RVR#040, or AL3\_ID\_RVR#050.

2463 **AL3\_ID\_RVR#030 Verify Subscriber as Revocant**

2464 When the subscriber seeks revocation of the subscriber's own credential:

- 2465 a) if in-person, require presentation of a primary Government Picture ID document  
2466 that must be electronically verified by a record check against the provided identity  
2467 with the specified issuing authority's records, or  
2468 b) if remote:  
2469 i. electronically verify a signature against records (if available), confirmed  
2470 with a call to a telephone number of record, or  
2471 ii. authenticate an electronic request as being from the same subscriber,  
2472 supported by a credential at Assurance Level 3 or higher.

2473 **AL3\_ID\_RVR#040 Verify ETSP as Revocant**

2474 Where a CSP seeks revocation of a subscriber's credential, establish that the request is  
2475 either:

- 2476 a) from the specified service itself, with authorization as determined by established  
2477 procedures, or  
2478 b) from the client Credential Issuer, by authentication of a formalized request over  
2479 the established secure communications network.

2480 **AL3\_ID\_RVR#050 Legal Representative as Revocant**

2481 Where the request for revocation is made by a law enforcement officer or presentation of  
2482 a legal document:

- 2483 a) if in person, verify the identity of the person presenting the request, or  
2484 b) if remote:  
2485 i. in paper/facsimile form, verify the origin of the legal document by a  
2486 database check or by telephone with the issuing authority, or  
2487 ii. authenticate an electronic request as being from a recognized legal office,  
2488 supported by a credential at Assurance Level 3 or higher.  
2489

2490 **3.7.3.3.3 Secure Revocation Request**

2491 This criterion requires that revocation requests between remote components of the service  
2492 be made with secured communications.

2493 An enterprise and its specified service must:

2494 **AL3\_ID\_SRR#010 Submit Request**

2495 Submit a request for the revocation to the Credential Issuer service (function), using a  
2496 secured network communication if necessary.

2497



2498 **3.7.3.4 Assurance Level 4**

2499 **3.7.3.4.1 Revocation Procedures**

2500 These criteria address general revocation functions, such as the processes involved and  
2501 the basic requirements for publication.

2502 An enterprise and its specified service must:

2503 **AL4\_CM\_RVP#010 Revocation procedures**

2504 State the conditions under which revocation of an issued certificate may occur, the  
2505 processes by which a revocation request may be submitted, the persons and organizations  
2506 from which a revocation request will be accepted, the validation steps that will be applied  
2507 to ensure the validity (identity) of the Revocant, and the response time between a  
2508 revocation request being accepted and the publication of revised certificate status.

2509 **AL4\_CM\_RVP#020 Secure status notification**

2510 Ensure that published credential status notification information can be relied upon in  
2511 terms of the enterprise being its origin (i.e., its authenticity) and its correctness (i.e., its  
2512 integrity).

2513 **AL4\_CM\_RVP#030 Revocation publication**

2514 Ensure that published credential status notification is revised within 24 hours of the  
2515 receipt of a valid revocation request, such that any subsequent attempts to use that  
2516 credential in an authentication shall be unsuccessful. The nature of the revocation  
2517 mechanism shall be in accord with the technologies supported by the service.

2518 **AL4\_ID\_RVP#050 Revocation Records**

2519 Retain a record of any revocation of a credential that is related to a specific identity  
2520 previously verified, solely in connection to the stated credential. At a minimum, records  
2521 of revocation must include:

- 2522 a) the Revocant's full name;
- 2523 b) the Revocant's current address;
- 2524 c) type, issuing authority, and reference number(s) of all documents checked in the  
2525 identity proofing process for the Revocant;
- 2526 d) the Revocant's authority to revoke (e.g., subscriber themselves, someone acting  
2527 with the subscriber's power of attorney, the credential issuer, law enforcement, or  
2528 other legal due process);
- 2529 e) the subscriber's full name and, where applicable, unique service reference (e.g.,  
2530 certificate serial number, IP address);
- 2531 f) the subscriber's date of birth;

- 2532 g) the subscriber's current address of record;
- 2533 h) the Credential Issuer's identity (if not directly responsible for the identity proofing
- 2534 service);
- 2535 i) the identity associated with the credential (whether the subscriber's name or a
- 2536 pseudonym);
- 2537 j) the reason for revocation.

2538 **AL4\_ID\_RVP#060 Record Retention**

2539 Retain, securely, the record of the revocation process for the duration of the subscriber's

2540 account plus 7.5 years.

2541

2542 **3.7.3.4.2 Revocation and Re-key**

2543 Revocation of a credential requires that the requestor and the nature of the request be

2544 verified as rigorously as the original identity proofing. The enterprise should not act on a

2545 request for revocation without first establishing the validity of the request (if it does not,

2546 itself, determine the need for revocation).

2547 In order to do so, the enterprise and its specified service must:

2548 **AL4\_ID\_RVR#010 Verify revocation identity**

2549 Establish that the credential for which a revocation request is received is one that was

2550 initially issued by the specified service, applying the same process and criteria as would

2551 apply to an original identity proofing.

2552 **AL4\_ID\_RVR#020 Revocation reason**

2553 Establish the reason for the revocation request as being sound and well founded, in

2554 combination with verification of the Revocant, according to AL4\_CM\_RVR#030,

2555 AL4\_CM\_RVR#040, or AL4\_CM\_RVR#050.

2556 **AL4\_CM\_RVR#030 Verify Subscriber as Revocant**

2557 Where the subscriber seeks revocation of the subscriber's own credential:

- 2558 a) if in person, require presentation of a primary Government Picture ID document
- 2559 that shall be verified by a record check against the provided identity with the
- 2560 specified issuing authority's records, or
- 2561 b) if remote:
  - 2562 i. verify a signature against records (if available), confirmed with a call to a
  - 2563 telephone number of record, or
  - 2564 ii. authenticate an electronic request as being from the same subscriber,
  - 2565 supported by a different credential at Assurance Level 4.

2566 **AL4\_CM\_RVR#040**            **Verify ETSP as Revocant**

2567 Where a CSP seeks revocation of a subscriber's credential, establish that the request is  
2568 either:

- 2569 a) from the specified service itself, with authorization as determined by established  
2570 procedures, or
- 2571 b) from the client Credential Issuer, by authentication of a formalized request over  
2572 the established secure communications network.

2573 **AL4\_CM\_RVR#050**            **Legal Representative as Revocant**

2574 Where the request for revocation is made by a law enforcement officer or presentation of  
2575 a legal document:

- 2576 a) if in person, verify the identity of the person presenting the request, or
- 2577 b) if remote:
  - 2578 i. in paper/facsimile form, verify the origin of the legal document by a  
2579 database check or by telephone with the issuing authority, or
  - 2580 ii. authenticate an electronic request as being from a recognized legal office,  
2581 supported by a different credential at Assurance Level 4.

2582 Re-key of a credential requires that the requestor be verified as the subject with as much  
2583 rigor as was applied to the original identity proofing. The enterprise should not act on a  
2584 request for re-key without first establishing that the requestor is identical to the subject.

2585 In order to do so, the enterprise and its specified service must:

2586 **AL4\_CM\_RKY#010**            **Verify Requestor as Subscriber**

2587 Where the subscriber seeks a re-key for the subscriber's own credential:

- 2588 a) if in-person, require presentation of a primary Government Picture ID document  
2589 that shall be verified by a record check against the provided identity with the  
2590 specified issuing authority's records, or
- 2591 b) if remote:
  - 2592 i. verify a signature against records (if available), confirmed with a call to a  
2593 telephone number of record, or
  - 2594 ii. authenticate an electronic request as being from the same subscriber,  
2595 supported by a different credential at Assurance Level 4.

2596

2597 **3.7.3.4.3 Re-key requests from any other parties must not be accepted**

2598 **3.7.3.4.4 Secure Revocation/Re-key Request**

2599 This criterion requires that revocation requests between remote components of the service  
2600 be made with secured communications.

2601 The enterprise and its specified service must:

2602 **AL4\_ID\_SRR#010            Submit Request**

2603 Submit a request for the revocation to the Credential Issuer service (function), using a  
2604 secured network communication if necessary.

2605 **3.7.4 Part D--Credential Status Management**

2606 These criteria deal with credential status management, such as the receipt of requests for  
2607 new status information arising from a new credential being issued or a revocation or other  
2608 change to the credential that requires notification. They also deal with the provision of  
2609 status information to requesting parties having the right to access such information.

2610 **3.7.4.1 Assurance Level 1**

2611 **3.7.4.1.1 Status Maintenance**

2612 An enterprise and its specified service must:

2613 **AL1\_CM\_CSM#010            Maintain Status Record**

2614 Maintain a record of the status of all credentials issued.

2615 **AL1\_CM\_CSM#040            Status Information Availability**

2616 Provide, with 95% availability, a secure automated mechanism to allow relying parties to  
2617 determine credential status and authenticate the subject's identity.

2618

2619 **3.7.4.2 Assurance Level 2**

2620 **3.7.4.2.1 Status Maintenance**

2621 An enterprise and its specified service must:

2622 **AL2\_CM\_CSM#010            Maintain Status Record**

2623 Maintain a record of the status of all credentials issued.

2624 **AL2\_CM\_CSM#020            Validation of Status Change Requests**

2625 Authenticate all requestors seeking to have a change of status recorded and published and  
2626 validate the requested change before considering processing the request. Such validation  
2627 should include:

- 2628 a) the requesting source as one from which the specified service expects to receive  
2629 such requests;  
2630 b) if the request is not for a new status, the credential or identity as being one for  
2631 which a status is already held.

2632 **AL2\_CM\_CSM#030 Revision to Published Status**

2633 Process authenticated requests for revised status information and have the revised  
2634 information available for access within a period of 72 hours.

2635 **AL2\_CM\_CSM#040 Status Information Availability**

2636 Provide, with 95% availability, a secure automated mechanism to allow relying parties to  
2637 determine credential status and authenticate the subject's identity.

2638 **AL2\_CM\_CSM#050 Inactive Credentials**

2639 Disable any credential that has not been successfully authenticated during a period of 12  
2640 months.

2641

2642 **3.7.4.3 Assurance Level 3**

2643 **3.7.4.3.1 Status Maintenance**

2644 An enterprise and its specified service must:

2645 **AL3\_CM\_CSM#010 Maintain Status Record**

2646 Maintain a record of the status of all credentials issued.

2647 **AL3\_CM\_CSM#020 Validation of Status Change Requests**

2648 Authenticate all requestors seeking to have a change of status recorded and published and  
2649 validate the requested change before considering processing the request. Such validation  
2650 should include:

- 2651 a) the requesting source as one from which the specified service expects to receive  
2652 such requests;  
2653 b) if the request is not for a new status, the credential or identity as being one for  
2654 which a status is already held.

2655 **AL3\_CM\_CSM#030 Revision to Published Status**

2656 Process authenticated requests for revised status information and have the revised  
2657 information available for access within a period of 72 hours.

2658 **AL3\_CM\_CSM#040**            **Status Information Availability**

2659 Provide, with 95% availability, a secure automated mechanism to allow relying parties to  
2660 determine credential status and authenticate the subject's identity.

2661 **AL3\_CM\_CSM#050**            **Inactive Credentials**

2662 Disable any credential that has not been successfully authenticated during a period of 12  
2663 months.

2664

2665 **3.7.4.4**    **Assurance Level 4**

2666 **3.7.4.4.1**   **Status Maintenance**

2667 An enterprise and its specified service must:

2668 **AL4\_CM\_CSM#010**            **Maintain Status Record**

2669 Maintain a record of the status of all credentials issued.

2670 **AL4\_CM\_CSM#020**            **Validation of Status Change Requests**

2671 Authenticate all requestors seeking to have a change of status recorded and published and  
2672 validate the requested change before considering processing the request. Such validation  
2673 should include:

- 2674 a)        the requesting source as one from which the specified service expects to receive  
2675            such requests;
- 2676 b)        if the request is not for a new status, the credential or identity as being one for  
2677            which a status is already held.

2678 **AL4\_CM\_CSM#030**            **Revision to Published Status**

2679 Process authenticated requests for revised status information and have the revised  
2680 information available for access within a period of 72 hours.

2681 **AL4\_CM\_CSM#040**            **Status Information Availability**

2682 Provide, with 95% availability, a secure automated mechanism to allow relying parties to  
2683 determine credential status and authenticate the subject's identity.

2684 **AL4\_CM\_CSM#050**            **Inactive Credentials**

2685 Disable any credential that has not been successfully authenticated during a period of 12  
2686 months.

2687 **3.7.5 Part E--Credential Validation/Authentication**

2688 These criteria apply to credential validation and identity authentication.

2689 **3.7.5.1 Assurance Level 1**

2690 **3.7.5.1.1 Assertion Security**

2691 An enterprise and its specified service must:

2692 **AL1\_CM\_ASS#010 Validation and Assertion Security**

2693 Provide validation of credentials to a relying party using a protocol that:

- 2694 a) requires authentication of the specified service or of the validation source;
- 2695 b) ensures the integrity of the authentication assertion.

2696 **AL1\_CM\_ASS#020 No Post Authentication**

2697 *Not* authenticate credentials that have been revoked.

2698 **AL1\_CM\_ASS#030 Proof of Possession**

2699 Use an authentication protocol that requires the claimant to prove possession and control  
2700 of the authentication token.

2701 **AL1\_CM\_ASS#040 Assertion Lifetime**

2702 No stipulation.

2703

2704 **3.7.5.2 Assurance Level 2**

2705 **3.7.5.2.1 Assertion Security**

2706 An enterprise and its specified service must:

2707 **AL2\_CM\_ASS#010 Validation and Assertion Security**

2708 Provide validation of credentials to a relying party using a protocol that:

- 2709 a) requires authentication of the specified service, itself, or of the validation source;
- 2710 b) ensures the integrity of the authentication assertion.

2711 **AL2\_CM\_ASS#020 No Post Authentication**

2712 *Not* authenticate credentials that have been revoked.

2713 **AL2\_CM\_ASS#030 Proof of Possession**

2714 Use an authentication protocol that requires the claimant to prove possession and control  
2715 of the authentication token.

2716 **AL2\_CM\_ASS#040 Assertion Lifetime**

2717 Generate assertions so as to indicate and effect their expiration 12 hours after their  
2718 creation.

2719

2720 **3.7.5.3 Assurance Level 3**

2721 **3.7.5.3.1 Assertion Security**

2722 An enterprise and its specified service must:

2723 **AL3\_CM\_ASS#010 Validation and Assertion Security**

2724 Provide validation of credentials to a relying party using a protocol that:

- 2725 a) requires authentication of the specified service, itself, or of the validation source;  
2726 b) ensures the integrity of the authentication assertion.

2727 **AL3\_CM\_ASS#020 No Post Authentication**

2728 *Not* authenticate credentials that have been revoked.

2729 **AL3\_CM\_ASS#030 Proof of Possession**

2730 Use an authentication protocol that requires the claimant to prove possession and control  
2731 of the authentication token.

2732 **AL3\_CM\_ASS#040 Assertion Lifetime**

2733 For non-cryptographic credentials, generate assertions that indicate and effect their  
2734 expiration 12 hours after their creation; otherwise, notify the relying party of how often  
2735 the revocation status sources are updated.

2736

2737 **3.7.5.4 Assurance Level 4**

2738 **3.7.5.4.1 Assertion Security**

2739 An enterprise and its specified service must:



2740 **AL4\_CM\_ASS#010 Validation and Assertion Security**

2741 Provide validation of credentials to a relying party using a protocol that:

- 2742 a) requires authentication of the specified service, itself, or of the validation source;
- 2743 b) ensures the integrity of the authentication assertion.

2744 **AL4\_CM\_ASS#020 No Post Authentication**

2745 *Not* authenticate credentials that have been revoked.

2746 **AL4\_CM\_ASS#030 Proof of Possession**

2747 Use an authentication protocol that requires the claimant to prove possession and control  
2748 of the authentication token.

2749 **AL4\_CM\_ASS#040 Assertion Lifetime**

2750 Notify the relying party of how often the revocation status sources are updated.

2751

2752 **3.7.6 Compliance Tables**

2753 Use the following tables to correlate criteria and evidence offered/compliance achieved.  
2754 A table is provided for each assurance level. The tables are linked to their respective  
2755 criteria and vice-versa, to aid referencing between them. Service providers preparing for  
2756 an assessment can use the table appropriate to the level at which they are seeking  
2757 approval to correlate evidence with criteria or to justify non-applicability of criteria (e.g.,  
2758 specific service types not offered): Assessors can use the tables to record the steps they  
2759 take in their assessment and their determination of compliance or failure.

2760

**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	

2761

2762

**Table 3-6 CM-SAC - AL2 Compliance**

<b>Clause</b>	<b>Description</b>	<b>Compliance</b>
<b>Part A - Credential Operating Environment</b>		
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	
<b>Part B – Credential Issuing</b>		
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	
<b>Part C – Credential Revocation</b>		
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	

2763

2764

**Table 3-7 CM-SAC - AL3 Compliance**

<b>Clause</b>	<b>Description</b>	<b>Compliance</b>
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	

2765

2766

**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	

2767



## 2768 **4 Accreditation and Certification Rules**

### 2769 **4.1 Assessor Accreditation**

2770 IAEG certified services can be offered only by a CSP who is IAEG-certified. IAEG  
2771 certification will be granted by a Federation Operator based on an assessment provided  
2772 by an IAEG-accredited assessor. Assessor accreditation requires the following steps.

- 2773 1. An assessor submits an application for accreditation.
- 2774 2. The IAEG evaluates the application according to the criteria set for accreditation.
- 2775 3. The applicant is notified of the IAEG decision.
- 2776 4. In the event of a negative decision, the applicant is offered an appeal.

#### 2777 **4.1.1 Criteria for Assessor Accreditation**

2778 The Board of Directors or any committee or other entity the Board may empower by  
2779 delegation (the Board) may choose to recognize the accreditation of another body in lieu  
2780 of its own accreditation or as a supplement to its own accreditation. The Board shall  
2781 apply the following criteria when determining whether to approve the application of an  
2782 assessor for accreditation.

##### 2783 **4.1.1.1 Expertise With Relevant Standards**

2784 Prior to accreditation, the assessor must demonstrate expertise in the application of at  
2785 least one of the following evaluation standards. In addition, the assessor must  
2786 demonstrate competence in the application of any supplemental evaluation criteria  
2787 formally identified by the IAEG and against which CSPs are to be assessed for  
2788 certification by Federation Operators and other trust providers.

##### 2789 **4.1.1.2 Business Expertise**

2790 The assessor must:

- 2791 • have been in existence for more than 1 month;
- 2792 • be financially solvent and stable and reasonably certain to remain so for the  
2793 foreseeable future;
- 2794 • have sufficient financial resources, either through direct reserves, insurance, or  
2795 otherwise, to absorb the cost resulting from wrongful certification of a CSP upon  
2796 its recommendation for the period of such certification and for 1 year thereafter;
- 2797 • demonstrate excellence, breadth, and depth in the relevant fields of endeavor,  
2798 including electronic authentication, federated identity management, information  
2799 security, and the processes and methods of assessment of such fields;

- 2800 • *not* have any key personnel or personnel directly involved in assessments or  
2801 development and delivery of assessment reports and recommendations to the  
2802 IAEG who have been convicted of a crime.

#### 2803 **4.1.2 Assessment**

2804 Prior to accreditation, assessors may be subject to an on-site evaluation by the IAEG or a  
2805 designee. This assessment is to determine compliance with the current IAEG criteria for  
2806 accreditation and to evaluate expertise, processes and equipment necessary to conduct the  
2807 assessment of CSPs according to IAEG certification criteria and rules. Whether an on-  
2808 site inspection is scheduled or not, the assessor shall provide information as provided for  
2809 in Section 4.1.1.1 and Section 4.1.1.2.

#### 2810 **4.1.3 Accreditation Decision and Appeal**

2811 Within a reasonable time and at the discretion of the IAEG, the IAEG shall make a  
2812 determination of accreditation and communicate that determination to the applicant.

2813 In the event of a negative decision, the assessor may request an appeal of the  
2814 accreditation decision by the IAEG. Such request shall be considered by a three-member  
2815 panel of the IAEG Board of Directors or any committee or other entity the Board may  
2816 empower by delegation, composed of people who have been uninvolved with the decision  
2817 and are impartial.

#### 2818 **4.1.4 Maintaining Accreditation**

2819 After the initial year of accreditation, assessors may be subject to an on-site or remote  
2820 surveillance evaluation. The surveillance assessment shall include review of at least the  
2821 following.

- 2822 • Internal audit reports.
- 2823 • Minutes of management review meetings.
- 2824 • Results of certification assessments, if any.
- 2825 • Any changes in key personnel, facilities and/or major test equipment.
- 2826 • Information on any other significant changes in the quality system of the assessor.

2827 The IAEG, or a designee, may conduct an on-site reassessment or surveillance assessment  
2828 of accredited assessors at a minimum of once every 2 years, for verification of continued  
2829 compliance with IAEG accreditation criteria and rules.

## 2830 **4.2 Certification of Credential Service Provider Offerings**

2831 Only a CSP whose product or line of business is currently IAEG certified can issue or  
2832 otherwise purvey certified credentials or validation of IAEG certified credentials under an  
2833 IAEG brand or IAEG business rules or for use within the IAEG system.

### 2834 **4.2.1 Process of Certification**

2835 The process of certification for each product or line of business for which certification is  
2836 sought by a CSP includes the following steps.

- 2837 1. A CSP seeking certification for a product or line of business begins the formal  
2838 process by reviewing the list of IAEG accredited and approved assessors. The  
2839 CSP selects an assessor for commencing formal assessment, for which there shall  
2840 be a separate contractual arrangement between the applicant and the chosen  
2841 assessor.
- 2842 2. The IAEG accredited assessor selected by the applicant conducts an assessment of  
2843 the CSP product or line of business. At the conclusion of the assessment process,  
2844 the assessor and the CSP separately submit their respective materials upon request  
2845 by Federation Operators.
- 2846 3. The assessor submits the assessment report and its recommendation regarding  
2847 certification upon request to Federation Operators.
- 2848 4. The CSP submits an application for certification to the Federation Operator,  
2849 including agreement to the IAEG business rules, as well as specification of each  
2850 line of offerings for which certification is sought, and the assurance level (AL) at  
2851 which each certification is sought.
- 2852 5. After receiving the assessment and application materials from the assessor and  
2853 CSP, respectively, the Federation Operator evaluates the relevant information and  
2854 makes a decision on certification.
- 2855 6. The requestor communicates its decision on certification to the CSP, the assessor  
2856 and the IAEG.
- 2857 7. In the event of a negative decision, the CSP is afforded an appeal.
- 2858 8. In the event of a positive decision, the CSP's certified product or line of business  
2859 is added to the IAEG Certified CSP offering list.

#### 2860 **4.2.1.1 Application**

2861 The IAEG shall provide an application form for certification as an IAEG CSP both on the  
2862 IAEG web site and in paper form. The application shall include contact information; an  
2863 agreement to abide by the IAEG rules and any other applicable IAEG requirements  
2864 identified in the application, such as a license agreement or other terms and conditions;  
2865 and an IAEG appeal request form to request review of the final certification

2866 determination. In addition, the application shall require the applicant to specify the  
2867 precise scope of each line of business for which certification is sought, the AL at which  
2868 each certification is sought, and any existing applicable accreditation, certification or  
2869 similar approvals granted to each specified line of business.

#### 2870 **4.2.1.2 Initial Evaluation**

2871 Upon receipt of an application for certification, the IAEG shall review the contents and  
2872 audit report.

#### 2873 **4.2.1.3 Assessment**

2874 Prior to certification, CSPs may be subject to an on-site assessment by the assessor. The  
2875 assessment shall determine compliance with the current IAEG Service Assessment  
2876 Criteria.

2877 An IAEG accredited assessor will conduct an on-site reassessment or surveillance  
2878 assessment of a CSP at least 1 year after certification and, at a minimum, once every 2  
2879 years thereafter, for verification of continued compliance with IAEG certification  
2880 requirements.

### 2881 **4.2.2 Criteria for Certification of CSP Line of BUSINESS**

#### 2882 **4.2.2.1 Standard Evaluation Criteria Used by Assessor**

2883 For each line of business for which certification is sought, the practices, operations,  
2884 organization, personnel and other relevant aspects of a CSP must be assessed against one  
2885 of the following evaluation standards:

2886

2887 **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

2888

2889 When multiple offerings share one or more assessment criteria, the criteria need only be  
2890 considered once per assessment. Such criteria may include management organization,  
2891 physical security, or personnel who are common to each line of business for which  
2892 certification is sought. In addition, criteria that have been previously assessed positively  
2893 by an adequate assessor and assessment process and that are equivalent to IAEG criteria  
2894 may be relied upon for purposes of an IAEG assessment. Whether such criteria are  
2895 deemed adequate and equivalent must be decided by the IAEG Board. Such  
2896 determination by the Board may be triggered by a request by a previously assessed

2897 applicant CSP, an accredited assessor or on the initiative of the Board itself. Such  
2898 determinations may be published from time to time as assessment guidance by the IAEG.

#### 2899 **4.2.2.2 Supplemental Criteria Used by Assessor**

2900 The criteria applied by assessors are identified in the IAEG Service Assessment Criteria  
2901 (Section 3).

#### 2902 **4.2.3 Certification Decision**

##### 2903 **4.2.3.1 Assessor Delivers Report and Recommendation**

2904 Upon conclusion of the assessment, for each line of business for which certification has  
2905 been sought, the assessor shall deliver to the Federation Operator a final assessment  
2906 report, including a recommendation on whether to certify the assessed CSP.

##### 2907 **4.2.3.2 Federation Operator Makes Certification Decision**

2908 Upon receipt of each assessment report and recommendation on certification from the  
2909 assessor, the Federation Operator shall determine within a reasonable time whether to  
2910 deny certification to the CSP, certify the CSP, or take such other action as may be  
2911 appropriate, including requesting further information, contractual agreements, or provable  
2912 action from the CSP by a certain date.

2913 The decision of the Federation Operator shall be communicated to both the CSP and the  
2914 assessor within a reasonable time, to be set by the IAEG Board. The assessor will then  
2915 communicate the decision to the IAEG.

#### 2916 **4.2.4 Appeals Process**

2917 Upon receipt of the decision on certification by a Liberty-accredited Federation Operator,  
2918 a CSP may request an appeal of that decision. Upon receiving the Appeal Request from a  
2919 CSP and within a reasonable period of time, to be set by the IAEG Board, the IAEG shall  
2920 appoint a three-member review panel from among IAEG Board of Directors or any  
2921 committee or other entity the Board may empower by delegation, comprised of people  
2922 who have been uninvolved with the decision at issue and are impartial. Said panel shall  
2923 consider the request and make a final determination. The panel may make its  
2924 determination based solely upon the information presented in the appeal request,  
2925 including any attachments, or it may request additional information from one or more  
2926 parties or schedule a hearing to permit the affected parties to further clarify and present  
2927 their positions.

#### 2928 **4.2.5 Maintaining Certification**

2929 The CSP must notify the assessor, the Federation Operator and the IAEG of any material  
2930 change that may lower the assurance level of the certified product or line of business 60

2931 days before the change is performed or immediately upon the incidence of any unplanned  
2932 change. The IAEG, in consultation with the assessor, will determine whether the changes  
2933 are sufficient to require re-assessment. The re-assessment, if required, need only cover  
2934 those elements that have changed.

2935 Annual renewal agreements are required for a certification to remain in effect. The CSP  
2936 warrants continued compliance with the criteria of the assessment in this agreement and  
2937 provides annual audit results. An independent third party must audit any certified product  
2938 or line of business assessed at AL2 or higher every 2 years. Other audits may be internal.  
2939 The IAEG, in consultation with the assessor, may require a partial reassessment if the  
2940 scope of the audits does not include all applicable criteria.

### 2941 **4.3 Process for Handling Non-Compliance**

2942 The following process for handling non-compliance applies both to accredited assessors  
2943 and to certified CSPs, unless otherwise noted.

#### 2944 **4.3.1 Compliance Determination**

2945 Upon receipt by the IAEG of credible information that an assessor or CSP is not in  
2946 compliance with the requirements for accreditation or certification, the IAEG Board or  
2947 staff or a committee at Board discretion shall determine whether the assessor or CSP is in  
2948 fact in material non-compliance with IAEG requirements and shall communicate the  
2949 determination to the affected parties. The Board of Directors shall establish further  
2950 criteria, as needed, detailing conduct or circumstances constituting material non-  
2951 compliance with IAEG rules or standards.

#### 2952 **4.3.2 Period to Cure**

2953 An assessor or CSP found to be in material non-compliance shall be afforded an  
2954 opportunity and period of time to remedy the non-compliance, provided such period does  
2955 not unduly jeopardize the integrity of the IAEG System or the rights or property of  
2956 another party.

#### 2957 **4.3.3 Administrative Recourse**

2958 Based on review of all available data and in light of all the relevant circumstances, the  
2959 IAEG Board of Directors may take administrative recourse against any signatory  
2960 determined to be in material non-compliance with these business rules, to include, as  
2961 needed, any of the following remedies.

2962 **4.3.3.1 Warning**

2963 The non-complying party may be given a warning. The warning may be confidential or  
2964 may be publicized within the IAEG or publicized more broadly, at the discretion of the  
2965 IAEG Board of Directors.

2966 **4.3.3.2 Non-compliance Fees**

2967 The non-complying party may be subject to a schedule of fees, to be specified by the  
2968 IAEG Board of Directors. The fees may increase according to the length of time before  
2969 the party comes back into compliance.

2970 **4.3.3.3 Suspension**

2971 The non-complying party may have its participation in the IAEG System suspended,  
2972 including the suspension of accreditation, pending coming back into compliance.

2973 **4.3.3.4 Termination**

2974 The non-complying party may have its participation in the IAEG System terminated,  
2975 including the termination of accreditation.

2976 **4.4 Acceptable Public Statements Regarding IAEG**  
2977 **Accreditation and Certification**

2978 It is acceptable for a party to indicate that it is an "IAEG Accredited Assessor" or an  
2979 "IAEG Certified Credential Service Provider" for any period during which such statement  
2980 is true. However, no party may make any public claim, whether to media outlets, in bids  
2981 and other proposals, in marketing materials or otherwise, regarding its status as an  
2982 applicant for accreditation or certification, nor can it claim that it is in the process of  
2983 achieving such status.

## 2984 **5 Business Rules**

### 2985 **5.1 Scope**

2986 Signatories to these business rules agree that these rules govern the use and validation of  
2987 Liberty Alliance IAEG certified credentials, the certification of such credentials and the  
2988 accreditation of those who assess issuers of such credentials. These business rules are  
2989 intended to cover use of credentials for purposes of authentication and not specifically for  
2990 the application of a legal signature, which may be subject to other rules depending upon  
2991 the parties and transactions involved. The IAEG will employ a phased approach to  
2992 establishing business rules and assessment criteria for identity trust service providers,  
2993 starting with identity service providers then rolling out to include relying parties and  
2994 federations.

2995 The IAEG will provide a framework of assessment criteria as a guideline for the  
2996 certification of credentials issued by a CSP. The IAEG is responsible for the accreditation  
2997 of assessors who evaluate CSPs for purposes of IAEG certification of credentials.  
2998 Federations and/or Federation Operators will utilize the assessors' evaluations to provide  
2999 certification statements with respect to the individual CSPs. A certification statement  
3000 made by a federation or federation operator regarding a CSP's compliance with IAEG  
3001 certification criteria may be accepted by other federations in consideration of that CSP.

3002 The foregoing does not prohibit use of an IAEG credential under a different brand,  
3003 certification, or set of rules, provided that the credential is clearly being used as a non-  
3004 IAEG credential.

3005 Claimants are not direct signatories to these business rules. Claimants may have  
3006 contracts with each CSP issuing an IAEG credential to the claimant. The claimant can be  
3007 a person, the electronic agent of a person, or any legal entity, including a corporation.  
3008 Any issues or conflicts arising from use of IAEG-certified credentials will be directed to  
3009 the Federation Operator for resolution.

### 3010 **5.2 Participation**

3011 Before becoming eligible to become a participant in these rules, a CSP must successfully  
3012 complete an assessment by an IAEG-accredited assessor and be awarded IAEG  
3013 certification for one or more lines of credentials issued by that CSP. A relying party may  
3014 become bound by these business rules by agreeing to accept and rely on credentials  
3015 issued by one or more IAEG-certified CSPs. A CSP need not be a member of the IAEG  
3016 non-profit corporation in order to become certified to these business rules.



---

## 3017 **5.3 Roles and Obligations**

### 3018 **5.3.1 IAEG**

#### 3019 **5.3.1.1 Promulgation and Amendment of Business Rules and Other Documents**

3020 The IAEG shall formalize and may periodically amend these business rules. The IAEG  
3021 shall also formalize and may periodically amend a set of documents governing the  
3022 accreditation of assessors of IAEG CSPs and the certification criteria of IAEG  
3023 credentials. The IAEG reserves the right, at its discretion, to formalize and periodically  
3024 amend such other materials, including policies or guidelines, participation agreements,  
3025 handbooks or other documents relevant to the IAEG. Notice of all amendments shall be  
3026 given by IAEG by electronic mail to the contact person(s) identified by each signatory for  
3027 such purpose and by posting to the IAEG web site. All amendments shall be effective as  
3028 of the date specified in such notice. If a signatory objects in writing to an amendment  
3029 within 30 days after notice of the amendment is given by IAEG, such objection shall be  
3030 deemed to be a notice of termination of such signatory's participation in IAEG under  
3031 Section 5.2.

#### 3032 **5.3.1.2 Assessor Accreditation and CSP Certification Requirements**

3033 The IAEG is responsible for accreditation of assessors in the IAEG System. The IAEG  
3034 shall formalize and may periodically amend requirements for certification of credentials  
3035 issued by a CSP and the accreditation of assessors of CSPs.

#### 3036 **5.3.1.3 IAEG Providers List**

3037 The IAEG will maintain and update as needed a list of current accredited assessors and  
3038 IAEG-certified CSPs. To the extent allowable, the IAEG will publish this list as a service  
3039 to the industry.

#### 3040 **5.3.1.4 Contact Information**

3041 Current contact information for the IAEG can be found at <http://www.projectliberty.org>.

### 3042 **5.3.2 CSP Obligations**

#### 3043 **5.3.2.1 CSP Certification**

3044 A CSP is obliged to obtain certification of one or more lines of credentials as a  
3045 prerequisite for participation in the IAEG System. Certification of CSPs will be  
3046 determined by federations and/or Federation Operators based on their review of a report  
3047 provided by an IAEG-accredited assessor upon request.

#### 3048 **5.3.2.2 CSP Participation**

3049 A CSP is obliged to abide by the criteria set forth in this document in order to achieve and  
3050 maintain IAEG certification status.

3051 **5.3.2.3 Continued Compliance with Certification Requirements**

3052 Each approved and certified CSP must comply with all certification requirements during  
3053 the period of time for which credentials issued by the CSP are certified.

3054 **5.3.2.4 Use of IAEG Trademark**

3055 A CSP may not use or display the IAEG or Liberty Alliance trademark in association with  
3056 the issuance, validation or other servicing of an IAEG credential or otherwise use or  
3057 display the IAEG or Liberty trademark on or associated with any service, product,  
3058 literature or other information unless such use has been approved by the IAEG and/or  
3059 Liberty Alliance and the trademark is used in accordance with the applicable agreement  
3060 with the IAEG.

3061 **5.3.2.5 Records of IAEG Related Disputes**

3062 A CSP is required to investigate any complaint raised to the CSP from a relying party  
3063 regarding an IAEG credential. The CSP is also required to keep auditable records of its  
3064 investigation and decisions regarding any complaint.

3065 **5.3.2.6 Validation**

3066 Each CSP must make available a method of validation for each IAEG credential it issues  
3067 or is otherwise responsible for validating. Such method must be accessible and reliable.

3068 **5.3.2.7 Privacy Practices**

3069 Each CSP must be able to verify that it is complying with applicable privacy practices, as  
3070 stated in Section 5.3.5.4 of these business rules.

3071 **5.3.2.8 Relying Party Agreements**

3072 It is advised that each approved CSP shall have in place an agreement governing the  
3073 rights and obligations between it and any relying party using, validating or otherwise  
3074 relying upon IAEG-certified credentials issued by that CSP. As an example, such  
3075 agreement may include a clause for conflict resolution upon which the Federation  
3076 Operator can rely in the event a conflict arises. Such agreement may contain such  
3077 additional terms as the parties may agree to.

3078 **5.3.3 Relying Party Obligations**

3079 **5.3.3.1 Relying Party Agreements**

3080 It is advised that a relying party have in place an agreement with a CSP governing the  
3081 practices as well as the rights and obligations between it and the CSP providing the  
3082 IAEG-certified credential. A relying party may also have in place an agreement that  
3083 governs these practices directly with a federation and/or Federation Operator.

3084 **5.3.3.2 Reasonable Reliance and Level of Assurance**

3085 A relying party is expected through its normal course of business to determine for, itself,  
3086 the appropriate level of assurance of the IAEG credential needed for a particular  
3087 application, transaction or other session. A relying party is expected to establish that a  
3088 credential is in fact issued by an IAEG-certified CSP in order for the relying party's  
3089 reliance upon the asserted identity of the claimant to be deemed reasonable under these  
3090 business rules. A relying party is expected to successfully validate an IAEG credential in  
3091 order for its reliance upon the asserted identity of the claimant to be deemed reasonable  
3092 under these business rules. Any use by or validation of an IAEG credential by a party  
3093 that has not entered into an agreement with the CSP that issued the credential shall be at  
3094 the sole risk of that party, for which the CSP shall have no liability whatsoever.

3095 **5.3.3.3 Use of IAEG Trademark**

3096 A relying party may not use or display the IAEG or Liberty Alliance trademark in  
3097 association with the acceptance, validation or other use of an IAEG credential or  
3098 otherwise use or display the IAEG or Liberty trademark on or associated with any  
3099 service, product, literature or other information unless such use has been approved by the  
3100 IAEG and/or Liberty Alliance.

3101 **5.3.4 Assessor Obligations**

3102 **5.3.4.1 Assessor Accreditation**

3103 An assessor is not eligible for approval by the IAEG to conduct an assessment for  
3104 purposes of IAEG certification of a CSP or otherwise participate as an assessor in the  
3105 IAEG System unless that assessor has been and remains accredited by the IAEG.

3106 **5.3.4.2 Assessor Agreement**

3107 An assessor is obliged to execute an IAEG assessor agreement as a prerequisite to being  
3108 approved by the IAEG.

3109 **5.3.4.3 Continued Compliance with Accreditation Requirements**

3110 In accordance with the requirements of the IAEG accreditation and certification rules and  
3111 any applicable service assessment criteria, approved and accredited assessors must  
3112 remain in compliance with all accreditation requirements for the period of time for which  
3113 they are accredited.

3114 **5.3.4.4 Use of IAEG Trademark**

3115 An assessor may not use or display the IAEG or Liberty Alliance trademark in association  
3116 with an assessment or otherwise use or display the IAEG or Liberty trademark on or  
3117 associated with any service, product, literature or other information unless such use has  
3118 been approved by the IAEG and/or Liberty Alliance and the trademark is used in  
3119 accordance with the applicable agreement with the IAEG.

3120 **5.3.5 General Obligations**

3121 **5.3.5.1 Record Keeping**

3122 Every signatory wishing to avail itself of IAEG resolution of disputes under the terms of  
3123 these business rules is obliged to keep records sufficient to preserve evidence of the facts  
3124 related to a particular dispute.

3125 **5.3.5.2 System Security and Reliability**

3126 Every signatory agrees to safeguard the security and reliability of the IAEG System.  
3127 Specifically, every signatory agrees that the IAEG reserves the right to suspend use of the  
3128 IAEG System, in whole or in part, and the participation of any party or parties to the  
3129 system without notice and at the sole discretion of the IAEG to protect the integrity and  
3130 efficacy of the IAEG System or the rights or property of any party. Agreement to access,  
3131 use or rely upon the IAEG System is subject to such terms and conditions as the IAEG  
3132 may provide in these business rules, related participation agreements or otherwise.

3133 **5.3.5.3 Third Party Processors**

3134 Any IAEG-certified or -accredited party that is a participating in these rules and uses a  
3135 third-party processor to perform any processing, transactions or other obligations related  
3136 to participation in the IAEG System either must take full responsibility for assuring that  
3137 actions of the third-party processor are in compliance with all applicable terms of these  
3138 business rules or assure that the third party, itself, becomes a direct signatory of these  
3139 business rules.

3140 **5.3.5.4 Claimant Privacy**

3141 Every participant in these business rules must assure that each claimant for which the  
3142 participating organization collects or otherwise uses personally identifiable information  
3143 has granted informed consent with regard to the sharing of any personally identifiable  
3144 information about the claimant by the participant with any other party, whether such  
3145 information is contained in a credential, other identity assertion or otherwise. The  
3146 informed consent of the individual must be obtained before personally identifiable  
3147 information is used for enrollment, authentication or any subsequent uses. Claimants  
3148 must be provided with a clear statement about the collection and use of personally  
3149 identifiable information upon which to make informed decisions. Participants must  
3150 collect only the information necessary to complete the intended authentication function.

3151 Informed consent, for the purposes of this section, is an agreement made by a claimant  
3152 with the legal capacity to do so who is so situated as to be able to exercise free power of  
3153 choice without the intervention of any element of force, fraud, deceit, duress, over-  
3154 reaching, or other form of constraint or coercion and who is given sufficient information  
3155 about the subject matter and elements of the transaction involved as to enable him or her  
3156 to make an informed and enlightened decision.

3157 Nothing in these business rules shall be construed to authorize or permit the sharing of  
3158 any personally identifiable information about an end user other than the information  
3159 contained in a certificate or other identity assertion. Such information can be shared only  
3160 with an approved relying party to whom the end user has presented credentials or  
3161 attempted to access services with an identity assertion operating under the IAEG. If any  
3162 other personally identifiable information about a claimant is shared with any party  
3163 operating within the IAEG System or any other party, the required consent terms listed in  
3164 this section of these business rules must be affirmatively assented to by the claimant.

## 3165 **5.4 Enforcement and Recourse**

### 3166 **5.4.1 Breach of Accreditation or Certification Requirements**

#### 3167 **5.4.1.1 Compliance Determination**

3168 Upon receipt by the IAEG of credible information that any IAEG-certified or -accredited  
3169 party is not in compliance with the requirements for accreditation or certification, the  
3170 IAEG Board or staff or a committee at Board discretion shall make a determination on  
3171 whether the party is in fact in material non-compliance with IAEG requirements and shall  
3172 communicate the determination to the affected parties. The Board of Directors shall  
3173 establish further criteria, as needed, detailing conduct or circumstances constituting  
3174 material non-compliance with IAEG rules or standards.

3175 Upon receipt of credible information that a CSP is not in compliance with the  
3176 requirements for certification, a Federation Operator may make the determination on  
3177 whether the CSP is in fact in material non-compliance with IAEG requirements and shall  
3178 communicate the determination to affected parties.

#### 3179 **5.4.1.2 Period to Cure**

3180 An IAEG-certified or -accredited party found to be in material non-compliance shall be  
3181 afforded an opportunity and period of time to remedy that material non-compliance,  
3182 provided such period does not unduly jeopardize the integrity of the IAEG System or the  
3183 rights or property of another party.

### 3184 **5.4.2 Monetary Recourse**

3185 A CSP may be liable solely under the terms of an existing agreement with a relying party  
3186 for losses suffered by the relying party where the cause is attributable to conduct by the  
3187 CSP that was carried out in material non-compliance with these business rules or with  
3188 certification requirements. Conflict resolution will be directed to the appropriate  
3189 Federation Operator.

3190 A CSP may offer credentials at a band of monetary recourse set independently from levels  
3191 of assurance. A CSP shall disclose the monetary recourse it will or will not make

3192 available with respect to IAEG credentials and any applicable terms or limitations  
3193 governing the recourse according to Table 5-1.

3194

<b>Table 5-1. Bands and Amounts of Monetary Recourse</b>	
<b>Band</b>	<b>Amount</b>
1. No recourse	Zero monetary recourse
2. By agreement	By agreement of the parties

3195

#### 3196 **5.4.2.1 Safe Harbors**

##### 3197 **5.4.2.1.1 Losses Arising From Authorization or Unreasonable Reliance**

3198 In no event shall liability or other recourse specified herein be triggered by unreasonable  
3199 reliance on a credential by a relying party or by losses resulting from authorization errors  
3200 that have not been caused by errors in authentication of identity of a claimant by means  
3201 of an IAEG credential.

##### 3202 **5.4.2.1.2 Conduct in Accordance with Business Rules**

3203 Under these business rules, an approved CSP is not liable for losses suffered by a relying  
3204 party where the cause is attributable to conduct by the CSP that was carried out in  
3205 accordance with these business rules.

#### 3206 **5.4.2.2 Request for Monetary Recourse**

3207 All requests for monetary recourse and the dispositions of all requests must be directed to  
3208 the appropriate Federation Operator or trust provider by each relying party and CSP  
3209 involved.

#### 3210 **5.4.2.3 Reporting to the IAEG**

3211 All disputes and monetary requests involving IAEG-certified CSPs will be reported to the  
3212 IAEG by the Federation Operator or trust provider involved.

#### 3213 **5.4.3 Administrative Recourse**

3214 Based on review of all available data and in light of all relevant circumstances, the IAEG  
3215 Board of Directors may take administrative recourse against any participant determined  
3216 to be in material non-compliance with these business rules, to include, as needed, any of  
3217 the following remedies.

3218 **5.4.3.1 Warning**

3219 The non-complying party may be given a warning. The warning may be confidential or  
3220 may be publicized within the IAEG or publicized more broadly, at the discretion of the  
3221 IAEG Board of Directors.

3222 **5.4.3.2 Credential Revocation**

3223 The non-complying party may be required to revoke one or more IAEG credentials.

3224 **5.4.3.3 Non-compliance Fees**

3225 The non-complying party may be subject to a schedule of fees, to be specified by the  
3226 IAEG Board of Directors. The fees may increase according to the length of time before  
3227 the party comes back into compliance.

3228 **5.4.3.4 Suspension**

3229 The non-complying party may have its participation in the IAEG System suspended,  
3230 including the suspension of accreditation or certification, pending coming back into  
3231 compliance.

3232 **5.4.3.5 Termination**

3233 The non-complying party may have its participation in the IAEG System terminated,  
3234 including the termination of accreditation or certification.

3235 **5.5 General Terms**

3236 **5.5.1 Governing Law**

3237 These business rules and any related materials governing the IAEG shall be construed  
3238 and adjudicated according to the laws of the state of Delaware.

3239 **5.5.2 Disclaimer**

3240 No signatory may disclaim the warranty of merchantability and fitness for a particular  
3241 purpose with respect to the provision of any service or product to any other signatory  
3242 under these business rules.

3243 **5.5.3 Assignment and Succession**

3244 No signatory may sell, rent, lease, sublicense, assign, grant a security interest in or  
3245 otherwise transfer any right and/or obligation contained in these business rules or the  
3246 participation agreement executed by that signatory without the express written consent of  
3247 the IAEG.

3248 **5.5.4 Hold Harmless**

3249 All signatories to these business rules agree to hold the IAEG harmless for any losses or  
3250 other liability arising out of or in relation to the issuance, use, acceptance, validation, or  
3251 other reliance upon an IAEG credential or otherwise arising out of or in relation to  
3252 participation in the IAEG System or other conduct subject to these business rules.

3253 **5.5.5 Severability**

3254 If any provision, set of provisions or part of a provision of these business rules is held to  
3255 be unenforceable or otherwise invalid in whole or in part, the remaining provisions shall  
3256 remain in full force and effect and shall be construed to the maximum extent practicable  
3257 as a consistent and reasonable entire agreement.

3258 **5.6 Interpretation**

3259 The terms of these business rules shall be interpreted by the IAEG so as to avoid conflict  
3260 or inconsistencies between the various provisions and between these business rules,  
3261 applicable participation agreements and other relevant IAEG materials.



## 3262 **6 IAEG Glossary**

- 3263 *Accreditation.* The process used to achieve formal recognition that an organization has  
3264 agreed to the IAEG operating rules and is competent to perform assessments using  
3265 the Service Assessment Criteria.
- 3266 *AL.* See *assurance level*
- 3267 *Applicant.* An individual or person acting as a proxy for a machine or corporate entity  
3268 who is the subject of an identity proofing process.
- 3269 *Approval.* The process by which the IAEG Board accepts the compliance of a certified  
3270 service and the ETSP responsible for that service commits to upholding the IAEG  
3271 Rules.
- 3272 *Approved encryption.* Any cryptographic algorithm or method specified in a FIPS or a  
3273 NIST recommendation. Refer to <http://csrc.nist.gov/cryptval/>
- 3274 *Approved service.* A certified service which has been granted an approval by the IAEG  
3275 Board.
- 3276 *Assertion.* A statement from a verifier to a relying party that contains identity or other  
3277 information about a subscriber.
- 3278 *Assessment.* A process used to evaluate an electronic trust service and the service  
3279 provider using the requirements specified by one or more Service Assessment  
3280 Criteria for compliance with all applicable requirements.
- 3281 *Assessor.* A person or corporate entity who performs an assessment.
- 3282 *Assurance level (AL).* A degree of certainty that a claimant has presented a credential  
3283 that refers to the claimant's identity. Each assurance level expresses a degree of  
3284 confidence in the process used to establish the identity of the individual to whom  
3285 the credential was issued and a degree of confidence that the individual who uses  
3286 the credential is the individual to whom the credential was issued. The four  
3287 assurance levels are:
- 3288 Level 1: Little or no confidence in the asserted identity's validity  
3289 Level 2: Some confidence in the asserted identity's validity  
3290 Level 3: High confidence in the asserted identity's validity  
3291 Level 4: Very high confidence in the asserted identity's validity
- 3292 *Attack.* An attempt to obtain a subscriber's token or to fool a verifier into believing that  
3293 an unauthorized individual possesses a claimant's token.
- 3294 *Attribute.* A property associated with an individual.
- 3295 *Authentication.* Authentication simply establishes identity, not what that identity is  
3296 authorized to do or what access privileges he or she has.

- 3297 *Authentication protocol.* A well-specified message exchange process that verifies  
3298 possession of a token to remotely authenticate a claimant. Some authentication  
3299 protocols also generate cryptographic keys that are used to protect an entire  
3300 session, so that the data transferred in the session is cryptographically protected.
- 3301 *Authorization.* Process of deciding what an individual ought to be allowed to do.
- 3302 *Bit.* A binary digit: 0 or 1
- 3303 *Brand.* See IAEG Branded Credential.
- 3304 *CAP:* Credential Assessment Profile
- 3305 *Certification.* The IAEG's affirmation that a particular credential service provider can  
3306 provide a particular credential service at a particular assurance level.
- 3307 *Claimant.* A party whose identity is to be verified.
- 3308 *Certification Body.* An organization which has been deemed competent to perform  
3309 assessments of a particular type. Such assessments may be formal evaluations or  
3310 testing and be based upon some defined set of standards or other criteria.
- 3311 *Certified service.* An electronic trust service which has been assessed by an IAEG-  
3312 recognized certification body and found to be compliant with the applicable  
3313 SACs.
- 3314 *Credential.* An object to be verified when presented in an authentication transaction. A  
3315 credential can be bound in some way to the individual to whom it was issued, or it  
3316 can be a bearer credential. Electronic credentials are digital documents that bind  
3317 an identity or an attribute to a subscriber's token.
- 3318 *Credential management.* A service that supports the lifecycle of identity credentials from  
3319 issuance to revocation, including renewal, status checks and authentication  
3320 services.
- 3321 *Credential service.* A type of electronic trust service that supports the verification of  
3322 identities (identity proofing), the issuance of identity related  
3323 assertions/credentials/tokens, and the subsequent management of those credentials  
3324 (for example, renewal, revocation and the provision of related status and  
3325 authentication services).
- 3326 *Credential service provider (CSP).* An electronic trust service provider that operates one  
3327 or more credential services. A CSP can include a Registration Authority.
- 3328 *Credential service.* A reliable, efficient means of disseminating credential information.
- 3329 *CSP.* See *credential service provider*.
- 3330 *Cryptographic token.* A token for which the secret is a cryptographic key.
- 3331 *IAEG.* See *Identity Assurance Expert Group*

- 3332 *IAEG assessor.* An organization that has agreed to the IAEG Rules and that has been  
3333 accredited to conduct assessments of credential service providers.
- 3334 *IAEG-branded credential.* Information indicating the individual identity of a natural  
3335 person, according to a CSP certified by the IAEG to issue, process, validate or  
3336 otherwise purvey such credential.
- 3337 *IAEG credential service provider.* Organization that has agreed to the IAEG Operating  
3338 Rules and other applicable Rules, and that has been Certified to issue, process,  
3339 validate, etc., an IAEG branded credential.
- 3340 *IAEG-recognized assessor.* A body that has been granted an accreditation to perform  
3341 assessments against Service Assessment Criteria, at the specified assurance  
3342 level(s).
- 3343 *IAEG-recognized certification body.* A certification body which has been accredited by,  
3344 or whose qualifications have been otherwise established by, a scheme which the  
3345 IAEG Board has deemed to be appropriate for the purposes of determining an  
3346 ETSP's competence to perform assessments against IAEG's criteria.
- 3347 *Identity Assurance Expert Group (IAEG).* The multi-industry Liberty Alliance  
3348 partnership working on enabling interoperability among public and private  
3349 electronic identity authentication systems.
- 3350 *Electronic credentials.* Digital documents used in authentication that bind an identity or  
3351 an attribute to a subscriber's token.
- 3352 *Electronic Trust service (ETS).* A service that enhances trust and confidence in electronic  
3353 transactions, typically but not necessarily using cryptographic techniques or  
3354 involving confidential material such as PINs and passwords.
- 3355 *Electronic Trust service provider (ETSP).* An entity that provides one or more electronic  
3356 trust services.
- 3357 *ETS.* See electronic trust service.
- 3358 *ETSP.* See electronic trust service provider,
- 3359 *Federated identity management.* A system that allows individuals to use the same user  
3360 name, password, or other personal identification to sign on to the networks of  
3361 more than one enterprise in order to conduct transactions.
- 3362 *Federal Information Processing Standards ([FIPS]) .* Standards and guidelines issued by  
3363 the National Institute of Standards and Technology (NIST) for use government-  
3364 wide. NIST develops FIPS when the Federal government has compelling  
3365 requirements, such as for security and interoperability, for which no industry  
3366 standards or solutions are acceptable.
- 3367 *FIPS.* See Federal Information Processing Standards.
- 3368 *Identification.* Process of using claimed or observed attributes of an individual to infer  
3369 who the individual is.

- 3370 *Identifier*. Something that points to an individual, such as a name, a serial number, or  
3371 some other pointer to the party being identified.
- 3372 *Identity authentication*. Process of establishing an understood level of confidence that an  
3373 identifier refers to an identity. It may or may not be possible to link the  
3374 authenticated identity to an individual.
- 3375 *Identity*. A unique name for single person. Because a person's legal name is not  
3376 necessarily unique, identity must include enough additional information (for  
3377 example, an address or some unique identifier such as an employee or account  
3378 number) to make a unique name.
- 3379 *Identity binding*. The extent to which an electronic credential can be trusted to be a proxy  
3380 for the entity named in it.
- 3381 *Identity Proofing*. The process by which identity related information is validated so as to  
3382 identify a person with a degree of uniqueness and certitude sufficient for the  
3383 purposes for which that identity is to be used.
- 3384 *Identity Proofing policy*. A set of rules that defines identity proofing requirements  
3385 (required evidence, format, manner of presentation, validation), records actions  
3386 required of the registrar, and describes any other salient aspects of the identity  
3387 proofing function that are applicable to a particular community or class of  
3388 applications with common security requirements. An identity proofing policy is  
3389 designed to accomplish a stated assurance level.
- 3390 *Identity Proofing service provider*. An electronic trust service provider which offers, as a  
3391 standalone service, the specific electronic trust service of identity proofing. This  
3392 service provider is sometimes referred to as a Registration Agent/Authority (RA).
- 3393 *Identity Proofing practice statement*. A statement of the practices that an identity  
3394 proofing service provider employs in providing its services in accordance with the  
3395 applicable identity proofing policy.
- 3396 *Issuer*. Somebody or something that supplies or distributes something officially.
- 3397 *Level of assurance*. See assurance level.
- 3398 *Network*. An open communications medium, typically, the Internet, that is used to  
3399 transport messages between the claimant and other parties.
- 3400 *OID*. Object identifier.
- 3401 *Password*. A shared secret character string used in authentication protocols. In many  
3402 cases the claimant is expected to memorize the password.
- 3403 *Practice statement*. A formal statement of the practices followed by an authentication  
3404 entity (e.g., RA, CSP, or verifier) that typically defines the specific steps taken to  
3405 register and verify identities, issue credentials and authenticate claimants.

- 3406 *Public key.* The public part of the asymmetric key pair that is typically used to verify  
3407 signatures or encrypt data.
- 3408 *Public key infrastructure (PKI)* . A set of technical and procedural measures used to  
3409 manage public keys embedded in digital certificates. The keys in such certificates  
3410 can be used to safeguard communication and data exchange over potentially  
3411 unsecure networks.
- 3412 *Registration.* An entry in a register, or somebody or something whose name or  
3413 designation is entered in a register.
- 3414 *Relying party.* An entity that relies upon a subscriber's credentials, typically to process a  
3415 transaction or grant access to information or a system.
- 3416 *Role.* The usual or expected function of somebody or something, or the part somebody or  
3417 something plays in a particular action or event.
- 3418 *SAC.* See Service Assessment Criteria.
- 3419 *Security.* A collection of safeguards that ensures the confidentiality of information,  
3420 protects the integrity of information, ensures the availability of information,  
3421 accounts for use of the system, and protects the system(s) and/or network(s) used  
3422 to process the information.
- 3423 *Service Assessment Criteria (SAC).* A set of requirements levied upon specific  
3424 organizational and other functions performed by electronic trust services and  
3425 service providers. Services and service providers must comply with all applicable  
3426 criteria to qualify for IAEG approval.
- 3427 *Signatory.* A party that opts into and agrees to be bound by the IAEG Rules according to  
3428 the specified procedures.
- 3429 *Specified service.* The electronic trust service which, for the purposes of an IAEG  
3430 assessment, is the subject of criteria set out in a particular SAC, or in an  
3431 application for assessment, in a grant of an approval or other similar usage as may  
3432 be found in various IAEG documentation.
- 3433 *Subject.* An entity that is able to use an electronic trust service subject to agreement with  
3434 an associated subscriber. A subject and a subscriber can be the same entity.
- 3435 *Subscriber.* A party that has entered into an agreement to use an electronic trust service.  
3436 A subscriber and a subject can be the same entity.
- 3437 *Threat.* An adversary that is motivated and capable to violate the security of a target and  
3438 has the capability to mount attacks that will exploit the target's vulnerabilities.
- 3439 *Token.* Something that a claimant possesses and controls (typically a key or password)  
3440 that is used to authenticate the claimant's identity.
- 3441 *Assurance framework.* The body of work that collectively defines the industry-led self-  
3442 regulatory framework for electronic trust services in the United States, as operated

3443 by the IAEG. The trust framework includes descriptions of criteria, rules,  
3444 procedures, processes, and other documents.  
3445 *Verification.* Establishment of the truth or correctness of something by investigation of  
3446 evidence.

## 3447 **7 Publication Acknowledgements**

3448 The IAEG would like to thank the following working group chairs and vice chairs for  
3449 their commitment and dedication to the Liberty Identity Trust Framework.

3450

3451 IAEG Co-Chair: Jane Henessey, Wells Fargo

3452 IAEG Co-Chair: Michael Sessa, PESC

3453

3454 Interim Chair: James Lewis, The Center for Strategic and International Studies

3455 Interim Vice Chair: David Temoshok, U.S. General Services Administration

3456

3457 Business Requirements and Processes Work Group

3458 Chair: Linda G. Elliot, PingID Network

3459 Vice Chair: Thomas Greco, beTRUSTed

3460

3461 Credential Services Assessment Criteria and Levels of Assurance Work Group

3462 Chair: Robert J. Schlecht, Mortgage Bankers Association of America

3463 Vice Chair: Von Harrison, U.S. General Services Administration

3464

3465 Credential Services Assessment Criteria Sub Work

3466 Chair: Nancy Black, HollenGroup

3467 Vice Chair: Richard Wilsher, The Zyigma Partnership

3468

3469 Levels of Assurance Sub Work Group

3470 Chair: Peter Alterman, National Institutes of Health

3471 Vice Chair: Noel Nazario, KPMG LLP

3472

3473 Interoperability Sub Work Group

3474 Chair: William E. Burr, National Institute of Standards and Technology

3475 Vice Chair: Kurt Van Etten, eBay, Inc.

3476

3477 Evaluation, Accreditation and Compliance Work Group

3478 Chair: Gary Glickman, Giesecke & Devrient Cardtech, Inc.

3479 Vice Chair: Cornelia Chebinou, National Association of State Auditors, Comptrollers  
3480 and Treasurers

3481

3482 EAP Governance Work Group

3483 Chair: Paula Arcioni, State of New Jersey, Office of Information Technology

3484 Vice Chair: Roger J. Cochetti, CompTIA

3485

3486 Consultants

3487 Russ Cutler, Confiance Advisors, LLC

- 3488 Yuriy Dzambasow, A&N Associates, Inc.
- 3489 Nathan Faut, KPMG
- 3490 Dan Greenwood, Commonwealth of Massachusetts
- 3491 Rebecca Nielsen, Booz Allen Hamilton
- 3492 Richard Wilsher, The Zygma Partnership
- 3493
- 3494 Members of the various work groups include:
- 3495 Khaja Ahmed, Microsoft Corporation
- 3496 Michael A. Aisenberg, VeriSign, Inc.
- 3497 Peter Alterman, National Institutes of Health
- 3498 Paula Arcioni, State of New Jersey, Office of Information Technology
- 3499 Jonathan Askins, ACXIOM Corporation
- 3500 Asaf Awan, Parkweb Associates
- 3501 Stefano Baroni, SETECS
- 3502 Paul Barrett, Real User Corporation
- 3503 Nancy Black, Hollen Group
- 3504 Debb Blanchard, Enspier Technologies/GDT
- 3505 Warren Blosjo, 3Factor
- 3506 Daniel Blum, Burton Group
- 3507 Iana Bohmer, Northrop Grumman Information Technology
- 3508 Christine Borucke, Electronic Data Systems
- 3509 Kirk Brafford, SSP-Litronic, Inc.
- 3510 Mayi Canales, M Squared Strategies, Inc.
- 3511 Richard Carter, American Association of Motor Vehicles Administration
- 3512 Kim Cartwright, Experian
- 3513 James A. Casey, NeuStar, Inc.
- 3514 Ray Cavanaugh, Entegriy Solutions
- 3515 Chuck Chamberlain, U.S. Postal Service
- 3516 Cornelia Chebinou, National Association of State Auditors, Comptrollers and Treasurers
- 3517 Rebecca Chisolm, Sun Microsystems Federal
- 3518 Roger J. Cochetti, CompTIA
- 3519 Dan Combs, Global Identity Solutions
- 3520 John Cornell, U.S. General Services Administration
- 3521 Sarah Currier, CheckFree Corporation
- 3522 Chris Daly, IBM Corporation
- 3523 Peter Davis, Neustar
- 3524 Kathy DiMaggio, Sigaba Corporation
- 3525 Yuriy Dzambasow, A&N Associates, Inc.
- 3526 Josh Elliott, American Management Systems
- 3527 Clay Epstein, Indentrus LLC
- 3528 Irving R. Gilson, Department of Defense
- 3529 Gary Glickman, Giesecke & Devrient Cardtech, Inc.
- 3530 James A. Gross, Wells Fargo



3531 Kirk R. Hall, GeoTrust  
3532 Von Harrison, U.S. General Services Administration  
3533 Christopher Hankin, Sun Microsystems, Inc.  
3534 Michael Horkey, Global Identity Solutions  
3535 Katherine M. Hollis, Electronic Data Systems  
3536 Robert Housel, National City Corporation  
3537 Burt Kaliski, RSA Security, Inc.  
3538 Shannon Kellog, RSA Security, Inc.  
3539 James Kobielus, Burton Group  
3540 Patrick Lally, SSP-Litronic, Inc.  
3541 Steve Lazerowich, Enspier Technologies/GDT  
3542 Phillip S. Lee, SC Solutions, Inc.  
3543 Peter Lieberwirth, Authentidate  
3544 Rob Lockhart, IEEE-ISTO  
3545 Chris Loudon, Enspier Technologies/GDT  
3546 J. Scott Lowry, Enspier Technologies/GDT  
3547 Lena Kannappan, FuGen Solutions  
3548 Paul Madsen, NTT  
3549 Adele Marsh, PA Higher Education Assistance Agency  
3550 Patty McCarty, Private ID Systems  
3551 Doug McCoy, SAFLINK Corporation  
3552 Ben Miller, InsideID  
3553 Larry Miller, Identrus LLC  
3554 Sead Muftic, SETECS  
3555 Noel Nazario, KPMG LLP  
3556 Michael R. Nelson, IBM Corporation  
3557 Simon Nicholson, Sun Microsystems, Inc.  
3558 Pete Palmer, HIMSS NHII Task Force Advisor, Guidant Corporation  
3559 Stephen Permison, Standards Based Programs  
3560 Bob Pinheiro, Independent Security Researcher  
3561 Alex Popowycz, Fidelity Investments  
3562 Hemma Prafullchandra, FuGen Solutions  
3563 Stephen L. Ranzini, University Bank  
3564 Christiane Reinhold, BearingPoint  
3565 Donald E. Rhodes, American Banker Association  
3566 Jason Roualt, HP  
3567 Randy V. Sabett, Cooley Goodward, LLP  
3568 Ravi Sandhu, NSD Security  
3569 Dean Sarff, Minerals Management Service  
3570 Donald Saxinger, FDIC  
3571 Robert J. Schlecht, Mortgage Bankers Association of America  
3572 Howard Schmidt, eBay, Inc.  
3573 Ari Schwartz, Center for Democracy and Technology

3574 John Shipley, The Shipley Group  
3575 Stephen P. Sill, U.S. General Services Administration  
3576 Helena G. Sims, NACHA – The Electronic Payments Association  
3577 Bill Smith, Sun Microsystems, Inc.  
3578 Tadgh Smith, IBM  
3579 Judith Spencer, U.S. General Services Administration  
3580 William Still, ChoicePoint Public Sector  
3581 Michael M. Talley, University Bancorp  
3582 David Temoshok, U.S. General Services Administration  
3583 Richard Thayer, ComTech, Inc.  
3584 John Ticer, NeuStar, Inc.  
3585 Kevin Trilli, VeriSign, Inc.  
3586 Matthew Tuttle, beTRUSTed  
3587 A. Jerald Varner, U.S. General Services Administration  
3588 Martin Wargon, Wave Systems Corporation  
3589 Richard Wilsher, The Zygma Partnership  
3590 David Weitzel, Mitretek Systems, Inc.  
3591 Michael Wolf, Authentidate  
3592 Gordon R. Woodrow, ClearTran, Inc.  
3593 Steve Worona, EDUCAUSE  
3594 David Wasley, Int2

## 3595 8 References

- 3596 [BSI7799-2] "BS 7799-2:2002 Information security management. Specification with  
3597 guidance for use," BSI Group (September 05, 2002). [http://www.bsi-](http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030049529)  
3598 [global.com/en/Shop/Publication-Detail/?pid=000000000030049529](http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030049529)
- 3599
- 3600 [CAF] Louden, Chris, Spenser, Judy, Burr, Bill, Hawkins, Kevin, Temoshok, David,  
3601 Cornell, John, Wilsher, Richard G, Timchak, Steve, Sill, Stephen, Silver, Dave, Harrison,  
3602 Von, eds., "E-Authentication Credential Assessment Framework (CAF)," E-  
3603 Authentication Initiative, Version 2.0.0 (March 16, 2005).  
3604 <http://www.cio.gov/eauthentication/documents/CAF.pdf>
- 3605
- 3606 [EAP CSAC 04011] "EAP working paper: Identity Proofing Service Assessment Criteria  
3607 (ID-SAC)," Electronic Authentication Partnership, Draft 0.1.3 (July 20, 2004)  
3608 [http://eap.projectliberty.org/docs/Jul2004/EAP\\_CSAC\\_04011\\_0-1-3\\_ID-SAC.doc](http://eap.projectliberty.org/docs/Jul2004/EAP_CSAC_04011_0-1-3_ID-SAC.doc)
- 3609
- 3610 [EAPTrustFramework] "Electronic Authentication Partnership Trust Framework"  
3611 Electronic Authentication Partnership, Version 1.0. (January 6, 2005)  
3612 [http://eap.projectliberty.org/docs/Trust\\_Framework\\_010605\\_final.pdf](http://eap.projectliberty.org/docs/Trust_Framework_010605_final.pdf)
- 3613
- 3614 [FIPS] "Federal Information Processing Standards Publications" Federal Information  
3615 Processing Standards. <http://www.itl.nist.gov/fipspubs/>
- 3616
- 3617 [FIPS140-2] "Security Requirements for Cryptographic Modules" Federal Information  
3618 Processing Standards. (May 25, 2001) [http://csrc.nist.gov/publications/fips/fips140-](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)  
3619 [2/fips1402.pdf](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)
- 3620
- 3621 [ISO/IEC17799] "ISO/IEC 17799:2005 Information technology -- Security techniques --  
3622 Code of practice for information security management" International Organization for  
3623 Standardization.  
3624 [http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=39612](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39612)
- 3625
- 3626 [M-04-04] Bolton, Joshua B., eds., "E-Authentication Guidance for Federal Agencies,"  
3627 Office of Management and Budget, (December 16, 2003).  
3628 <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>
- 3629

- 3630 [NIST800-63] Burr, William E., Dodson, Donna F., Polk, W. Timothy, eds., "Electronic  
3631 Authentication Guideline: : Recommendations of the National Institute of Standards and  
3632 Technology," Version 1.0.2, National Institute of Standards and Technology, (April,  
3633 2006). [http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1\\_0\\_2.pdf](http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf)  
3634
- 3635 [RFC 3647] Chokhani, S., Ford, W., Sabett, R., Merrill, C., Wu, S., eds., "Internet X.509  
3636 Public Key Infrastructure Certificate Policy and Certification Practices Framework," The  
3637 Internet Engineering Task Force (November, 2003). <http://www.ietf.org/rfc/rfc3647.txt>  
3638