

1

2



3

4

5 Liberty Identity Assurance Framework – 6 Read Me First

7 **Version:** 1.0

8 **Editor:**

9 Peter Alterman, Federal PKI Policy Authority
10 Joan Brennan, IEEE-ISTO
11 James A. Gross, Wells Fargo
12 Rob Lockhart, IEEE-ISTO
13 Richard Trevorah, tScheme Limited
14 Frank Villavicencio, Citi

15 **Contributors:**

16 Bob Pinheiro, Robert Pinheiro Consulting LLC
17 David Wasley, Int2
18 Richard Wilsher, The Zygma Partnership
19 Stephen P. Sill, General Services Administration

20 **Abstract:**

21 This document relates to the Liberty Identity Assurance Framework [[IAF](#)] which has been
22 developed within the Liberty Alliance Identity Assurance Expert Group (IAEG) and
23 corresponding public special interest groups with input from members of the global
24 financial services, government, healthcare, IT, and telecommunications sectors.

25 This document is intended to enable non-IAEG members to understand and familiarize
26 themselves with the IAF and thus be a starting point for industry professionals who want
27 to learn more and possibly conform to the IAF.

28 **Filename:** liberty-identity-assurance-framework_-_read-me-first-v1.0.pdf

29

Notice:

30 This document has been prepared by Sponsors of the Liberty Alliance. Permission is
31 hereby granted to use the document solely for the purpose educating the public. No rights
32 are granted to prepare derivative works of this Liberty Alliance Publication. Entities
33 seeking permission to reproduce portions of this document for other uses must contact the
34 Liberty Alliance to determine whether an appropriate license for such use is available.
35 Those who are interested in additional Liberty Publications are advised to review the
36 Liberty Alliance Project's website (<http://www.projectliberty.org/>) for more information.

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

56 All rights reserved.

57

58 Liberty Alliance Project
59 Licensing Administrator
60 c/o IEEE-ISTO
61 445 Hoes Lane
62 Piscataway, NJ 08855-1331, USA
63 info@projectliberty.org

64	Contents	
65		
66	1 Introduction	4
67	1.1 Intended Audience	4
68	1.2 Overview.....	4
69	2 Understanding The Liberty Identity Assurance Framework	6
70	2.1 Assurance Level Criteria.....	6
71	2.2 Service and Credential Assessment Criteria	6
72	2.3 Accreditation and Certification Model	7
73	2.4 Associated Business Rules.....	7
74	3 References	8
75	3.1 Informative.....	8
76		

77 **1 Introduction**

78 This document relates to the Liberty Identity Assurance Framework [[IAF](#)] which has been
79 developed within the Liberty Alliance Identity Assurance Expert Group (IAEG) and
80 corresponding public special interest groups with input from members of the global
81 financial services, government, healthcare, IT, and telecommunications sectors.

82 This document is intended to enable non-IAEG members to understand and familiarize
83 themselves with the IAF and thus be a starting point for industry professionals who want
84 to learn more and possibly conform to the IAF.

85 **1.1 Intended Audience**

86 The intended audience for this document encompasses users of electronic identity
87 credentials, entities that rely upon these electronic credentials, credential service
88 providers who issue these electronic credentials, and assessors who review the business
89 processes of credential service providers. This audience typically includes managers and
90 decision makers responsible for developing strategies for managing access to online
91 resources based on trustworthy identification of potential users, as well as providers of
92 trustworthy online identity credentials.

93 Other audiences might include potential subjects of online identity services and IT
94 auditors who may be asked to evaluate online identity service providers.

95 The reader should have a basic understanding of technical and practical issues regarding
96 identity and online identity credentials as discussed in such forums, documents, and
97 specifications as the EAP Trust Framework [[EAPTrustFramework](#)], the US E-
98 Authentication Federation Credential Assessment Framework ([CAF](#)), and the
99 [[CABForum](#)].

100 **1.2 Overview**

101 In order to conduct any sort of business in an online world, entities (which include
102 people, organizations, applications, machines, etc.) need to be able to identify themselves
103 remotely and reliably. However, in most cases, it is not sufficient for the typical
104 electronic credential (usually a basic userID/password pair or a digital certificate) to
105 simply make the assertion that “I am who I say I am ... believe me.” A relying party
106 needs to be able to know to some degree that the presented electronic identity credential
107 truly represents the individual referred to in the credential. In the case of self-issued
108 credentials, this is generally difficult. However, most electronic identity credentials are
109 issued by Credential Service Providers (CSPs), often referred to as identity providers
110 (IdPs): your workplace network administrator, your social networking service or online
111 game administrator, a government entity, or a trusted third party. You may have multiple
112 credentials from multiple providers ... most people do.

113 There are four main roles involved in making this online exchange trustworthy:

- 114 1. Entities who are the subjects of identity credentials issued by a CSP, variously
115 referred to as “subjects” or “credential holders,”
- 116 2. CSPs who are providers of identity services and issuers of electronic identity
117 credentials,
- 118 3. Auditors or assessors who review the business processes and operating procedures
119 that CSPs follow, and
- 120 4. Entities that rely upon the credentials issued by CSPs, referred to as “relying
121 parties.”

122 Different CSPs follow different policies, rules, and procedures for issuing electronic
123 identity credentials. In the business world, the more trustworthy the credential, the more
124 stringent are the rules governing identity proofing, credential management, and the kinds
125 of credentials issued. But while different CSPs follow their own rules, more and more
126 end users (i.e., subjects) and relying parties (e.g., online services) wish to trust existing
127 credentials and not issue yet another set of credentials for use to access one service. This
128 is where the concept of identity federation becomes important. Federated identity
129 provides CSPs, subjects, and relying parties with a common set of identity trust
130 conventions that transcend individual identity service providers, users, or networks, so
131 that a relying party will know it can trust a credential issued by CSP-1 at a level of
132 assurance comparable to a common standard, which will also be agreed upon by CSP-2,
133 CSP-3, and CSP-4. In this context, an assurance level describes the degree to which a
134 relying party in an electronic exchange can, after performing certain tests to authenticate
135 (validate) the origin of the exchange, be confident that the identity information being
136 presented by a CSP actually represents the entity referred to in it and that it is the
137 represented entity which is actually engaging in the exchange.

138 Identity federation offers many advantages to organizations, including recognized cost
139 and time savings, ability to assure and monitor privacy and security, auditability to meet
140 increasing global compliance demands, and the ability to minimize use and retention of
141 personally identifiable information (PII). The opportunity, and its potential benefits, have
142 been well-documented by early federated identity deployers and users, who recognized
143 identity federation as a logical approach that unlocks a myriad of electronic business and
144 online interactive opportunities which appeal to the end user’s need for simplicity and
145 high level of service.

146 The [\[IAF\]](#) provides a means to enable relying parties to understand the trustworthiness of
147 electronic identity credentials by other parties at commonly agreed levels of assurance.
148 The IAF specifies the verification and proofing checks that CSPs carry out on entities, the
149 way that CSPs run their services, and how the CSPs, themselves, are assessed to verify
150 they are operating their services in conformance with their proclaimed level(s) of
151 assurance and the stated terms of service.

152 **2 Understanding The Liberty Identity Assurance** 153 **Framework**

154 The [\[IAF\]](#) is a standardized approach that defines processes and procedures for CSPs,
155 relying parties, and operators of federated identity networks (Federation Operators) to
156 trust each other’s credentials at known levels of assurance. The main components of the
157 IAF are:

- 158 1. Assurance Level Criteria;
- 159 2. Service and Credential Assessment Criteria;
- 160 3. Accreditation and Certification Model, and;
- 161 4. Associated Business Rules.

162 **2.1 Assurance Level Criteria**

163 Assurance levels are the levels of trust associated with a credential as measured by the
164 associated technology, processes, and policy and practice statements. The IAF defers to
165 the guidance provided by the U.S. National Institute of Standards and Technology (NIST)
166 Special Publication 800-63 version 1.0.2 [\[NIST800-63\]](#) which outlines four (4) levels of
167 assurance, ranging in confidence level from low to very high. The level of assurance
168 provided is measured by the strength and rigor of the identity verification and proofing
169 process, the credential’s strength, and the management processes the CSP applies to it.
170 The IAF then goes on to describe the service assessment criteria at each assurance level.

171 On the relying party side, these same four assurance levels address increasing levels of
172 risk. For each Assurance Level, the IAF defines commensurate risk mitigation measures
173 appropriate for the level of trust that may be assumed in the identity credentials. These
174 four levels have been adopted by the U.K. government, the Government of Canada, and
175 the U.S. Federal Government for categorizing required electronic identity trust levels for
176 providing electronic government services.

177 **2.2 Service and Credential Assessment Criteria**

178 The Service and Credential Assessment Criteria section in the IAF establishes baseline
179 criteria for organizational conformity, identity-proofing services, credential strength, and
180 credential management services against which all CSPs will be evaluated. The IAF also
181 establishes a protocol for publishing updates, as needed, to account for technological
182 advances and preferred practice and policy updates.

183 These criteria set out the requirements that identity services and their CSPs must meet at
184 each assurance level within the IAF in order to receive Liberty accreditation.

185 CSPs can determine the assurance levels at which their services might qualify by
186 evaluating their overall business processes and technical mechanisms against the Service

187 Assessment Criteria. The Service Assessment Criteria within each assurance level are the
188 basis for assessing and approving electronic trust services.

189 **2.3 Accreditation and Certification Model**

190 The [\[IAF\]](#) uses a phased approach to establish criteria for certification and accreditation,
191 initially focusing on CSPs and the accreditation of those who will assess and evaluate
192 them. The goal of this phased approach is to provide, initially, federations and Federation
193 Operators with the means to certify their members for the benefit of inter-federation and
194 to streamline the certification process for the industry. It is anticipated that follow-on
195 phases will target the development of criteria for certification of federations, themselves,
196 as well as best practices guidelines for relying parties.

197 The IAF establishes the requirements that assessors must have in order to perform
198 assessments or audits for Liberty accreditation and defines the rules and requirements for
199 the actual assessments.

200 **2.4 Associated Business Rules**

201 Signatories to these business rules agree that they govern the issuance, use, and validation
202 of credentials issued by IAEG-certified CSPs, the certification of such CSPs, and the
203 accreditation of those who assess CSPs. The Business Rules section of the IAF identifies:
204 how CSPs and relying parties can participate in or be bound by the rules; what the roles
205 and obligations are of the various parties to the rules, i.e., the IAEG, CSPs, relying
206 parties, and assessors; the means of enforcement of and recourse under the rules; and, the
207 general terms of the rules (including Governing Law, severability etc.).

208 **3 References**

209 **3.1 Informative**

- 210 [CABForum] See the CA/Browser Forum website at <http://www.cabforum.org/>
- 211 [CAF] Louden, Chris; Spencer, Judy; Burr, Bill; Hawkins, Kevin; Temoshok, David;
212 Cornell, John; Wilsher, Richard G.; Timchak, Steve; Sill, Stephen; Silver, Dave; Harrison,
213 Von; eds., "E-Authentication Credential Assessment Framework (CAF)," E-
214 Authentication Initiative, Version 2.0.0 (March 16, 2005).
215 <http://www.cio.gov/eauthentication/documents/CAF.pdf>
- 216 [EAPTrustFramework] "Electronic Authentication Partnership Trust Framework"
217 Electronic Authentication Partnership, Version 1.0. (January 6, 2005)
218 http://eap.projectliberty.org/docs/Trust_Framework_010605_final.pdf
- 219 [IAF] Cutler, Russ, eds. "Liberty Identity Assurance Framework," Version 1.1, Liberty
220 Alliance Project (21 June, 2008).
221 [http://www.projectliberty.org/liberty/content/download/4315/28869/file/liberty-identity-
assurance-framework-v1.1.pdf](http://www.projectliberty.org/liberty/content/download/4315/28869/file/liberty-identity-
222 assurance-framework-v1.1.pdf)
- 223 [NIST800-63] Burr, William E., Dodson, Donna F., Polk, W. Timothy, eds., "Electronic
224 Authentication Guideline: : Recommendations of the National Institute of Standards and
225 Technology," Version 1.0.2, National Institute of Standards and Technology, (April,
226 2006). http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf