

1

2



3

4 Identity Assurance Framework: 5 Assurance Levels

6

7

8 **Version:** 2.0

9 **Date:** 2010-04-24

10 **Editor:** Britta Glade

11

12 **Contributors:**

13 The full list of contributors can be referenced here:

14 <http://kantarainitiative.org/confluence/display/idassurance/IAF+2.0+Contributors>

15

16 **Abstract:**

17 The Kantara Initiative Identity Assurance Work Group (IAWG) was formed to foster
18 adoption of identity trust services. The primary deliverable of the IAWG is the Identity
19 Assurance Framework (IAF), which is comprised of many different documents that detail
20 the levels of assurance and the certification program that bring the Framework to the
21 marketplace. The IAF is comprised of a set of documents that includes an Overview
22 publication, the IAF [Glossary](#), a summary [Assurance Levels](#) document, and an [Assurance](#)
23 [Assessment Scheme \(AAS\)](#), which encompasses the associated assessment and
24 certification program, as well as several subordinate documents, among them the [Service](#)
25 [Assessment Criteria \(SAC\)](#), which establishes baseline criteria for general organizational
26 conformity, identity proofing services, credential strength, and credential management
27 services against which all CSPs will be evaluated. This document overviews the four
28 Levels of Assurance, on which the IAF is based, as posited by the U.S. Federal
29 Government and described in OMB M-04-04 [[M-04-04](#)] and NIST Special Publication
30 800-63 [[NIST800-63](#)]. These are further described in this document.

31

32 **Filename:** Kantara IAF-1200-Levels of Assurance.doc

33

34

Notice:

35 This document has been prepared by Participants of Kantara Initiative. Permission is
36 hereby granted to use the document solely for the purpose of implementing the
37 Specification. No rights are granted to prepare derivative works of this Specification.
38 Entities seeking permission to reproduce portions of this document for other uses must
39 contact Kantara Initiative to determine whether an appropriate license for such use is
40 available.

41

42 Implementation or use of certain elements of this document may require licenses under
43 third party intellectual property rights, including without limitation, patent rights. The
44 Participants of and any other contributors to the Specification are not and shall not be
45 held responsible in any manner for identifying or failing to identify any or all such third
46 party intellectual property rights. This Specification is provided "AS IS," and no
47 Participant in Kantara Initiative makes any warranty of any kind, expressed or implied,
48 including any implied warranties of merchantability, non-infringement of third party
49 intellectual property rights, and fitness for a particular purpose. Implementers of this
50 Specification are advised to review Kantara Initiative's website
51 (<http://www.kantarainitiative.org/>) for information concerning any Necessary Claims
52 Disclosure Notices that have been received by the Kantara Initiative Board of Trustees.

53

54 The content of this document is copyright of Kantara Initiative. © 2010 Kantara
55 Initiative.

56

57 **Contents**

58

59 **1 INTRODUCTION4**

60 **2 ASSURANCE LEVELS5**

61 **2.1 Assurance Level Policy Overview5**

62 **2.2 Description of the Four Assurance Levels6**

63 **2.2.1 Assurance Level 17**

64 **2.2.2 Assurance Level 27**

65 **2.2.3 Assurance Level 38**

66 **2.2.4 Assurance Level 48**

67

68

69

70 1 INTRODUCTION

71 Kantara Initiative formed the Identity Assurance Work Group (IAWG) to foster adoption
72 of consistently managed identity trust services. Utilizing initial contributions from the
73 e-Authentication Partnership (EAP), the US E-Authentication Federation, and Liberty
74 Alliance, the IAWG's objective is to create a Framework of baseline policies
75 requirements (criteria) and rules against which identity trust services can be assessed and
76 evaluated. The goal is to facilitate trusted identity federation and to promote uniformity
77 and interoperability amongst identity service providers, with a specific focus on the level
78 of trust, or assurance, associated with identity assertions. The primary deliverable of
79 IAWG is the Identity Assurance Framework (IAF).

80 The IAF leverages the EAP Trust Framework [[EAPTrustFramework](#)] and the US
81 E-Authentication Federation Credential Assessment Framework ([[CAF](#)]) as baselines in
82 forming the criteria for a harmonized, best-of-breed, industry-recognized identity
83 assurance standard. The IAF is a Framework supporting mutual acceptance, validation,
84 and life cycle maintenance across identity federations. The IAF is comprised of a set of
85 documents which includes an [Overview](#) publication, the IAF [Glossary](#), a summary
86 Assurance Levels document, and an [Assurance Assessment Scheme](#) (AAS) document,
87 which encompasses the associated assessment and certification program. The present
88 document presents an overview of the Assurance Levels.

89

90 2 ASSURANCE LEVELS

91 2.1 Assurance Level Policy Overview

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

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

- 103 • The extent to which the identity presented by a CSP in an identity assertion can be
104 trusted to actually belong to the entity represented. This factor is generally
105 established through the identity proofing process and identity information
106 management practices.
- 107 • The extent to which the electronic credential presented to a CSP by an individual
108 can be trusted to be a proxy for the entity named in it and not someone else
109 (known as identity binding). This factor is directly related to the integrity and
110 reliability of the technology associated with the credential itself, the processes by
111 which the credential and its verification token are issued, managed, and verified,
112 and the system and security measures followed by the credential service provider
113 responsible for this service.

114 Managing risk in electronic transactions requires authentication and identity information
115 management processes that provide an appropriate level of assurance of identity. Because
116 different levels of risk are associated with different electronic transactions, IAWG has
117 adopted a multi-level approach to ALs. Each level describes a different degree of
118 certainty in the identity of the claimant.

119 The IAWG ALs enable subscribers and relying parties to select appropriate electronic
120 identity trust services. IAWG uses the ALs to define the [Service Assessment Criteria](#)
121 [\(SAC\)](#) to be applied to electronic identity trust service providers when they are
122 demonstrating compliance through the [Assurance Assessment Scheme \(AAS\)](#)
123 certification and assurance program. Relying parties (RPs) should use the assurance level
124 descriptions to map risk and determine the type of credential issuance and authentication
125 services they require. Credential service providers (CSPs) should use the levels to
126 determine what types of credentialing electronic identity trust services they are capable of
127 providing currently and/or aspire to provide in future service offerings.

128

129 **2.2 Description of the Four Assurance Levels**

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

133

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

134

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

141

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

142

143 The level of assurance provided is measured by the strength and rigor of the identity
144 proofing process, the credential's strength, and the management processes the service
145 provider applies to it. The IAWG has established service assessment criteria at each AL

146 for electronic trust services providing credential management services. These criteria are
147 described in the [Service Assessment Criteria](#) document.

148 CSPs can determine the AL at which their services might qualify by evaluating their
149 overall business processes and technical mechanisms against the [Service Assessment](#)
150 [Criteria](#). The service assessment criteria within each AL are the basis for assessing and
151 approving electronic trust services.

152 **2.2.1 Assurance Level 1**

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

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

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

168 **2.2.2 Assurance Level 2**

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

175 For example, a transaction in which a beneficiary changes an address of record through
176 an insurance provider's web site can be a Level 2 transaction. The site needs some
177 authentication to ensure that the address being changed is the entitled person's address.
178 However, this transaction involves a relatively low (moderate) risk of inconvenience.
179 Since official notices regarding payment amounts, account status, and records of changes
180 are sent to the beneficiary's address of record, the transaction entails moderate risk of
181 unauthorized release of personally sensitive data.

182 **2.2.3 Assurance Level 3**

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

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

196 **2.2.4 Assurance Level 4**

197 AL4 is appropriate for transactions requiring very high confidence in an asserted identity.
198 This level provides the best practical remote-network authentication assurance, based on
199 proof of possession of a key through a cryptographic protocol. Level 4 is similar to Level
200 3 except that only “hard” cryptographic tokens are allowed. High levels of cryptographic
201 assurance are required for all elements of credential and token management. All sensitive
202 data transfers are cryptographically authenticated using keys bound to the authentication
203 process.

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

212 A summary chart with the levels of assurance, examples, and assessment criteria, is below
213 in Table [2-3](#):

214

215

Table 2-3 Identity Assurance Levels Illustrated

Assurance Level	Example	Assessment Criteria – Organization	Assessment Criteria – Identity Proofing	Assessment Criteria – Credential Management
AL 1	Registration to a news website	Minimal Organizational criteria	Minimal criteria - Self assertion	PIN and Password
AL 2	Change of address of record by beneficiary	Moderate organizational criteria	Moderate criteria - Attestation of Govt. ID	Single factor; Prove control of token through authentication protocol
AL 3	Access to an online brokerage account	Stringent organizational criteria	Stringent criteria – stronger attestation and verification of records	Multi-factor auth; Cryptographic protocol; “soft”, “hard”, or “OTP” tokens
AL 4	Dispensation of a controlled drug or \$1mm bank wire	Stringent organizational criteria	More stringent criteria – stronger attestation and verification	Multi-factor auth w/hard tokens only; crypto protocol w/keys bound to auth process

216

217

218

Revision History

219

1. 8May2008 – Identity Assurance Framework Version 1.0 Initial Draft

220

a. Released by Liberty Alliance

221

b. Revision and scoping of Initial Draft release

222

2. 23JUNE 2008 – Identity Assurance Framework Version 1.1 Final Draft

223

a. Released by Liberty Alliance

224

b. Inclusion of comments to Final Draft

225

3. 1OCTOBER2009 – Identity Assurance Framework Version 1.1 Final Draft

226

a. Documents contributed to Kantara Initiative by Liberty Alliance

227

4. XAPRIL2010 – Identity Assurance Framework Version 2.0

228

a. Released by Kantara Initiative

229

b. Significant scope build

230

c. Original Identity Assurance Framework all inclusive document broken in
to a set of documents with specific focus:

231

232

i. Kantara IAF-1000-Overview

233

ii. Kantara IAF-1100-Glossary

234

iii. Kantara IAF-1200-Levels of Assurance

235

iv. Kantara IAF-1300-Assurance Assessment Scheme

236

v. Kantara IAF-1400-Service Assessment Criteria

237

vi. Kantara IAF-1600-Assessor Qualifications and Requirements

238